



FEDERAL REGISTER

Vol. 89

Tuesday,

No. 209

October 29, 2024

Pages 85851–86230

OFFICE OF THE FEDERAL REGISTER



The **FEDERAL REGISTER** (ISSN 0097-6326) is published daily, Monday through Friday, except official holidays, by the Office of the Federal Register, National Archives and Records Administration, under the Federal Register Act (44 U.S.C. Ch. 15) and the regulations of the Administrative Committee of the Federal Register (1 CFR Ch. I). The Superintendent of Documents, U.S. Government Publishing Office, is the exclusive distributor of the official edition. Periodicals postage is paid at Washington, DC.

The **FEDERAL REGISTER** provides a uniform system for making available to the public regulations and legal notices issued by Federal agencies. These include Presidential proclamations and Executive Orders, Federal agency documents having general applicability and legal effect, documents required to be published by act of Congress, and other Federal agency documents of public interest.

Documents are on file for public inspection in the Office of the Federal Register the day before they are published, unless the issuing agency requests earlier filing. For a list of documents currently on file for public inspection, see www.federalregister.gov.

The seal of the National Archives and Records Administration authenticates the **Federal Register** as the official serial publication established under the Federal Register Act. Under 44 U.S.C. 1507, the contents of the **Federal Register** shall be judicially noticed.

The **Federal Register** is published in paper and on 24x microfiche. It is also available online at no charge at www.govinfo.gov, a service of the U.S. Government Publishing Office.

The online edition of the **Federal Register** is issued under the authority of the Administrative Committee of the Federal Register as the official legal equivalent of the paper and microfiche editions (44 U.S.C. 4101 and 1 CFR 5.10). It is updated by 6:00 a.m. each day the **Federal Register** is published and includes both text and graphics from Volume 1, 1 (March 14, 1936) forward. For more information, contact the GPO Customer Contact Center, U.S. Government Publishing Office. Phone 202-512-1800 or 866-512-1800 (toll free). E-mail, gpocusthelp.com.

The annual subscription price for the **Federal Register** paper edition is \$860 plus postage, or \$929, for a combined **Federal Register**, **Federal Register** Index and List of CFR Sections Affected (LSA) subscription; the microfiche edition of the **Federal Register** including the **Federal Register** Index and LSA is \$330, plus postage. Six month subscriptions are available for one-half the annual rate. The prevailing postal rates will be applied to orders according to the delivery method requested. The price of a single copy of the daily **Federal Register**, including postage, is based on the number of pages: \$11 for an issue containing less than 200 pages; \$22 for an issue containing 200 to 400 pages; and \$33 for an issue containing more than 400 pages. Single issues of the microfiche edition may be purchased for \$3 per copy, including postage. Remit check or money order, made payable to the Superintendent of Documents, or charge to your GPO Deposit Account, VISA, MasterCard, American Express, or Discover. Mail to: U.S. Government Publishing Office—New Orders, P.O. Box 979050, St. Louis, MO 63197-9000; or call toll free 1-866-512-1800, DC area 202-512-1800; or go to the U.S. Government Online Bookstore site, see bookstore.gpo.gov.

There are no restrictions on the republication of material appearing in the **Federal Register**.

How To Cite This Publication: Use the volume number and the page number. Example: 89 FR 12345.

Postmaster: Send address changes to the Superintendent of Documents, Federal Register, U.S. Government Publishing Office, Washington, DC 20402, along with the entire mailing label from the last issue received.

SUBSCRIPTIONS AND COPIES

PUBLIC

Subscriptions:

Paper or fiche 202-512-1800
Assistance with public subscriptions 202-512-1806

General online information 202-512-1530; 1-888-293-6498

Single copies/back copies:

Paper or fiche 202-512-1800
Assistance with public single copies 1-866-512-1800
(Toll-Free)

FEDERAL AGENCIES

Subscriptions:

Assistance with Federal agency subscriptions:
Email FRSubscriptions@nara.gov
Phone 202-741-6000

The Federal Register Printing Savings Act of 2017 (Pub. L. 115-120) placed restrictions on distribution of official printed copies of the daily **Federal Register** to members of Congress and Federal offices. Under this Act, the Director of the Government Publishing Office may not provide printed copies of the daily **Federal Register** unless a Member or other Federal office requests a specific issue or a subscription to the print edition. For more information on how to subscribe use the following website link: <https://www.gpo.gov/frsubs>.



Contents

Federal Register

Vol. 89, No. 209

Tuesday, October 29, 2024

Agriculture Department

See Animal and Plant Health Inspection Service

See Forest Service

Alcohol and Tobacco Tax and Trade Bureau

RULES

Establishment of Viticultural Area:

Beverly, WA, 85852–85854

Animal and Plant Health Inspection Service

NOTICES

Imports:

Fresh Sourp Fruit (*Annona muricata*) from Mexico,
85935–85940

Bureau of Safety and Environmental Enforcement

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:

Pollution Prevention and Control, 85985–85986

Children and Families Administration

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals, 85974–85975

Civil Rights Commission

NOTICES

Hearings, Meetings, Proceedings, etc.:

Colorado Advisory Committee, 85941–85942

Hawaii Advisory Committee, 85942

Coast Guard

RULES

Safety Zone:

Neuse River, New Bern, NC, 85855–85857

Special Local Regulation:

Key West World Championship, Key West, FL, 85855

Commerce Department

See International Trade Administration

See National Oceanic and Atmospheric Administration

Comptroller of the Currency

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:

Company-Run Annual Stress Test Reporting Template
and Documentation for Covered Institutions with
Total Consolidated Assets of \$250 Billion or More
under the Dodd-Frank Wall Street Reform and
Consumer Protection Act, 86079–86081

International Regulation, 86081–86082

Corporation for National and Community Service

RULES

Protection of Human Subjects, 85867–85879

Defense Department

PROPOSED RULES

Privacy Act; Implementation, 85892–85895

NOTICES

Arms Sales, 85946–85951, 85955–85962

Designation of Chinese Military Company, 86230

Privacy Act; Systems of Records, 85952–85954

Removal of Designated Chinese Military Companies, 86230

Removal of Designated Chinese Military Companies and

Designation of Chinese Military Company;

Supplemental, 86230

Education Department

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:

National Evaluation of the Pathways to Partnerships
Program, 85962–85963

Environmental Protection Agency

RULES

Air Quality State Implementation Plans; Approvals and
Promulgations:

Wisconsin; State Implementation Plan Alignment
Revision, 85857–85859

Pesticide Tolerance; Exemptions, Petitions, Revocations,
etc.:

Glufosinate-P, 85859–85867

Equal Employment Opportunity Commission

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals, 85963–85965

Federal Aviation Administration

RULES

Airspace Designations and Reporting Points:

Asheville, NC, 85851–85852

PROPOSED RULES

Airworthiness Directives:

Rolls-Royce Deutschland Ltd and Co KG, 85890–85892

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:

Generic Clearance for the Collection of Qualitative

Feedback on Agency Service Delivery, 86075–86076

Federal Communications Commission

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals, 85965–85967

Federal Contract Compliance Programs Office

NOTICES

Request under the Freedom of Information Act:

Federal Contractors' Type 2 Consolidated Employer
Information Reports, 85986–85988

Federal Mediation and Conciliation Service

NOTICES

Privacy Act; Systems of Records, 85967–85969

Federal Railroad Administration

PROPOSED RULES

Procedures for Waivers and Safety-Related Proceedings,
85895–85909

NOTICES

Petition for Waiver of Compliance, 86076–86077

Petition for Waiver of Compliance; Modification, 86076

Federal Reserve System

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals, 85969–85974

Change in Bank Control:

Acquisitions of Shares of a Bank or Bank Holding Company, 85970–85971

Formations of, Acquisitions by, and Mergers of Bank Holding Companies, 85972–85973

Fish and Wildlife Service

PROPOSED RULES

Endangered and Threatened Species:

Removal of Chipola Slabshell and Fat Threeridge from the Federal List of Endangered and Threatened Wildlife, 85909–85934

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

Approval Procedures for Nontoxic Shot and Shot Coatings, 85980–85981

Environmental Assessments; Availability, etc.:

Proposed Multi-Bat Species General Conservation Plan for Routine Development Projects in New York, Pennsylvania, and West Virginia, 85981–85983

Foreign Assets Control Office

NOTICES

Sanctions Action, 86082–86083

Forest Service

NOTICES

Hearings, Meetings, Proceedings, etc.:

Modoc Resource Advisory Committee, 85941

Health and Human Services Department

See Children and Families Administration

See National Institutes of Health

Homeland Security Department

See Coast Guard

NOTICES

Guidance:

Product Security Bad Practices, 85976

Security Requirements for Restricted Transactions under Executive Order 14117, 85976–85980

Interior Department

See Bureau of Safety and Environmental Enforcement

See Fish and Wildlife Service

See Land Management Bureau

See National Park Service

Internal Revenue Service

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals, 86112–86113

Quarterly Publication of Individuals, Who Have Chosen to Expatriate, 86083–86112

International Trade Administration

NOTICES

Antidumping or Countervailing Duty Investigations, Orders, or Reviews:

Prestressed Concrete Steel Wire Strand from Mexico; Correction, 85944

Application for Duty-Free Entry of Scientific Instruments: Massachusetts Institute of Technology, et al., 85942–85943

International Trade Commission

NOTICES

Investigations; Determinations, Modifications, and Rulings, etc.:

Sodium Nitrite from China and Germany, 85986

Justice Department

PROPOSED RULES

Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 86116–86227

Labor Department

See Federal Contract Compliance Programs Office

See Labor Statistics Bureau

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

Mine Mapping and Records of Opening, Closing and Reopening of Mines, 85988

Labor Statistics Bureau

NOTICES

Hearings, Meetings, Proceedings, etc.:

Technical Advisory Committee; Correction, 85989

Land Management Bureau

NOTICES

Record of Decision:

Rhyolite Ridge Lithium-Boron Project, Esmeralda County, NV, 85983

National Aeronautics and Space Administration

NOTICES

Hearings, Meetings, Proceedings, etc.:

Astrophysics Advisory Committee, 85989

National Council on Disability

NOTICES

Meetings; Sunshine Act, 85989–85990

National Highway Traffic Safety Administration

NOTICES

Hearings, Meetings, Proceedings, etc.:

Technical Workshop and Demonstrations, 86077–86079

National Institutes of Health

NOTICES

Hearings, Meetings, Proceedings, etc.:

Center for Scientific Review, 85975–85976

National Labor Relations Board

NOTICES

Performance Review Board Members, 85990

National Oceanic and Atmospheric Administration

RULES

Atlantic Highly Migratory Species:

Sea Turtle Careful Release Equipment and Techniques, 85879–85885

Fisheries of the Northeastern United States:

Framework Adjustment 16 to the Mackerel, Squid, and Butterfish Fishery Management Plan, 85885–85888

NOTICES

Taking or Importing of Marine Mammals:
Atlantic Shores South Project Offshore of New Jersey,
85944–85946

National Park Service**NOTICES**

National Register of Historic Places:
Pending Nominations and Related Actions, 85983–85985

Nuclear Regulatory Commission**PROPOSED RULES**

Draft Regulatory Guide:
Qualification of Fiber-Optic Cables, Connections, and
Optical Fiber Splices for Use in Safety Systems for
Production and Utilization Facilities, 85889–85890

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
General Domestic Licenses for Byproduct Material,
85990–85991
Environmental Assessments; Availability, etc.:
Waste Control Specialists, LLC; Finding of No Significant
Impact, 85991–85994
Licenses; Exemptions, Applications, Amendments etc.:
Involving No Significant Hazards Considerations, 85994–
85999

Securities and Exchange Commission**NOTICES**

Application:
Gemcorp Capital Advisors LLC and Gemcorp
Commodities Alternative Products Fund, 86023–
86024
Self-Regulatory Organizations; Proposed Rule Changes:
Cboe BYX Exchange, Inc., 85999–86003
Cboe BZX Exchange, Inc., 86051–86055
Cboe C2 Exchange, Inc., 86061–86065
Cboe EDGA Exchange, Inc., 86046–86051
Cboe EDGX Exchange, Inc., 86065–86070
Cboe Exchange, Inc., 86019–86023
MIAX Sapphire, LLC, 86024–86046
Nasdaq BX, Inc., 86003–86007
Nasdaq PHLX LLC, 86007–86019
New York Stock Exchange LLC, 86070–86073
NYSE Arca, Inc., 86055–86061
The Options Clearing Corp., 86046

Small Business Administration**NOTICES**

Disaster Declaration:
California, 86073
Georgia; Public Assistance Only, 86073

Trade Representative, Office of United States**NOTICES**

Request for Application:
Indigenous Peoples' Representative on the Observer
Delegation from the United States to the Partnership
Council of the Indigenous Peoples Economic and
Trade Cooperation Arrangement, 86074–86075

Transportation Department

See Federal Aviation Administration
See Federal Railroad Administration
See National Highway Traffic Safety Administration

Treasury Department

See Alcohol and Tobacco Tax and Trade Bureau
See Comptroller of the Currency
See Foreign Assets Control Office
See Internal Revenue Service

Separate Parts In This Issue**Part II**

Justice Department, 86116–86227

Part III

Defense Department, 86230

Reader Aids

Consult the Reader Aids section at the end of this issue for phone numbers, online resources, finding aids, and notice of recently enacted public laws.

To subscribe to the Federal Register Table of Contents electronic mailing list, go to <https://public.govdelivery.com/accounts/USGPOOFR/subscriber/new>, enter your e-mail address, then follow the instructions to join, leave, or manage your subscription.

CFR PARTS AFFECTED IN THIS ISSUE

A cumulative list of the parts affected this month can be found in the Reader Aids section at the end of this issue.

10 CFR	
Proposed Rules:	
50	85889
52	85889
14 CFR	
71	85851
Proposed Rules:	
39	85890
27 CFR	
9	85852
28 CFR	
Proposed Rules:	
202	86116
32 CFR	
Proposed Rules:	
310	85892
33 CFR	
100	85855
165	85855
40 CFR	
52	85857
180	85859
45 CFR	
2584	85867
49 CFR	
Proposed Rules:	
211	85895
50 CFR	
635	85879
648	85886
Proposed Rules:	
17	85909

Rules and Regulations

Federal Register

Vol. 89, No. 209

Tuesday, October 29, 2024

This section of the FEDERAL REGISTER contains regulatory documents having general applicability and legal effect, most of which are keyed to and codified in the Code of Federal Regulations, which is published under 50 titles pursuant to 44 U.S.C. 1510.

The Code of Federal Regulations is sold by the Superintendent of Documents.

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 71

[Docket No. FAA–2023–2254; Airspace Docket No. 23–ASO–51]

RIN 2120–AA66

Amendment of Class E Airspace; Asheville, NC

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: This action amends Class E airspace extending upward from 700 feet above the surface for Mission Hospitals, Asheville, NC, as new instrument approach procedures have been designed for Mission Hospitals. Additionally, this action updates the coordinates for Mission Hospitals and Asheville Regional Airport. Controlled airspace is necessary for the safety and management of instrument flight rules (IFR) operations at this airport.

DATES: Effective 0901 UTC, February 20, 2025. The Director of the Federal Register approves this incorporation by reference action under 1 CFR part 51, subject to the annual revision of FAA Order JO 7400.11 and publication of conforming amendments.

ADDRESSES: A copy of the Notice of Proposed Rulemaking (NPRM), all comments received, this final rule, and all background material may be viewed online at www.regulations.gov using the FAA Docket number. Electronic retrieval help and guidelines are available on the website. It is available 24 hours a day, 365 days a year.

FAA Order JO 7400.11J, Airspace Designations, and Reporting Points, as well as subsequent amendments, can be viewed online at www.faa.gov/air-traffic/publications/. For further information, you can contact the Airspace Policy Group, Federal Aviation Administration, 800 Independence

Avenue SW, Washington, DC 20591; telephone: (202) 267–8783.

FOR FURTHER INFORMATION CONTACT:

Robert Scott Stuart, Operations Support Group, Eastern Service Center, Federal Aviation Administration, 1701 Columbia Avenue, College Park, GA 30337; telephone: (404) 305–5926.

SUPPLEMENTARY INFORMATION:

Authority for This Rulemaking

The FAA's authority to issue rules regarding aviation safety is found in Title 49 of the United States Code. Subtitle I, Section 106 describes the authority of the FAA Administrator. Subtitle VII, Aviation Programs, describes in more detail the scope of the agency's authority. This rulemaking is promulgated under the authority described in Subtitle VII, Part A, Subpart I, Section 40103. Under that section, the FAA is charged with prescribing regulations to assign the use of airspace necessary to ensure the safety of aircraft and the efficient use of airspace. This regulation is within the scope of that authority, as it amends Class E airspace extending upward from 700 feet above the surface for Mission Hospitals, Asheville, NC.

History

The FAA published a notice of proposed rulemaking for Docket No. FAA 2023–2254 in the **Federal Register** (89 FR 63114; August 2, 2024), proposing to amend Class E airspace extending upward from 700 feet above the surface for Mission Hospitals, Asheville, NC. Interested parties were invited to participate in this rulemaking effort by submitting written comments on the proposal to the FAA. One comment was received in favor of the proposal.

Incorporation by Reference

Class E airspace is published in paragraph 6005 of FAA Order JO 7400.11, Airspace Designations and Reporting Points, which is incorporated by reference in 14 CFR 71.1 on an annual basis. This document amends the current version of that order, FAA Order JO 7400.11J, dated July 31, 2024, and effective September 15, 2024. FAA Order JO 7400.11J is publicly available as listed in the **ADDRESSES** section of this document. These amendments will be published in the next update to FAA Order JO 7400.11. FAA Order JO

7400.11J lists Class A, B, C, D, and E airspace areas, air traffic service routes, and reporting points.

The Rule

This amendment to 14 CFR part 71 amends Class E airspace for Mission Hospitals, Asheville, NC, by relocating the center point of the Class E airspace extending upward from 700 feet above the surface within a 6-mile radius of Mission Hospitals. Additionally, this action deletes the Point In Space Coordinates for St. Josephs-Mission Hospital and uses Mission Hospitals as a reference to accommodate Class E airspace requirements. This action also updates coordinates for Asheville Regional Airport. Controlled airspace is necessary for the safety and management of instrument flight rules (IFR) operations in the area.

Regulatory Notices and Analyses

The FAA has determined that this regulation only involves an established body of technical regulations for which frequent and routine amendments are necessary to keep them operationally current. It, therefore: (1) is not a “significant regulatory action” under Executive Order 12866; (2) is not a “significant rule” under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979); and (3) does not warrant preparation of a Regulatory Evaluation as the anticipated impact is so minimal. Since this is a routine matter that will only affect air traffic procedures and air navigation, it is certified that this proposed rule, when promulgated, will not have a significant economic impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

Environmental Review

The FAA has determined that this action qualifies for categorical exclusion under the National Environmental Policy Act in accordance with FAA Order 1050.1F, “Environmental Impacts: Policies and Procedures,” paragraph 5–6.5a. This airspace action is not expected to cause any potentially significant environmental impacts, and no extraordinary circumstances exist that warrant the preparation of an environmental assessment.

Lists of Subjects in 14 CFR Part 71

Airspace, Incorporation by reference, Navigation (air).

The Amendment

In consideration of the foregoing, the Federal Aviation Administration amends 14 CFR part 71 as follows:

PART 71—DESIGNATION OF CLASS A, B, C, D, AND E AIRSPACE AREAS; AIR TRAFFIC SERVICE ROUTES; AND REPORTING POINTS

■ 1. The authority citation for 14 CFR part 71 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g); 40103, 40113, 40120; E.O. 10854, 24 FR 9565, 3 CFR, 1959–1963 Comp., p. 389.

§ 71.1 [Amended]

■ 2. The incorporation by reference in 14 CFR 71.1 of Federal Aviation Administration Order JO 7400.11J, Airspace Designations and Reporting Points, dated July 31, 2024, and effective September 15, 2024, is amended as follows:

Paragraph 6005 Class E Airspace Areas Extending Upward From 700 Feet or More Above the Surface of the Earth.

* * * * *

ASO NC E5 Asheville, NC [Amended]

Asheville Regional Airport, NC
(Lat. 35°26'10" N, long. 82°32'31" W)
Mission Hospitals, NC
(Lat. 35°34'31" N, long. 82°32'55" W)

That airspace extending upward from 700 feet above the surface within 6 miles each side of Runway 16/34 centerline, extending 17 miles north and 21 miles south of the Asheville Regional Airport, and that airspace within a 6-mile radius of Mission Hospitals.

* * * * *

Issued in College Park, Georgia, on October 23, 2024.

Andree C. Davis,

Manager, Airspace & Procedures Team South, Eastern Service Center, Air Traffic Organization.

[FR Doc. 2024–25072 Filed 10–28–24; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF THE TREASURY**Alcohol and Tobacco Tax and Trade Bureau****27 CFR Part 9**

[Docket No. TTB–2022–0014; T.D. TTB–198; Ref: Notice No. 219, 219A]

RIN 1513–AD00

Establishment of the Beverly, Washington Viticultural Area

AGENCY: Alcohol and Tobacco Tax and Trade Bureau, Treasury.

ACTION: Final rule; Treasury decision.

SUMMARY: The Alcohol and Tobacco Tax and Trade Bureau (TTB) establishes the approximately 2,415-acre “Beverly, Washington” viticultural area (AVA) in Grant County, Washington. The Beverly, Washington AVA is located entirely within the established Columbia Valley AVA. TTB designates viticultural areas to allow vintners to better describe the origin of their wines and to allow consumers to better identify wines they may purchase.

DATES: This final rule is effective November 29, 2024.

FOR FURTHER INFORMATION CONTACT:

Mimi Torello, Regulations and Rulings Division, Alcohol and Tobacco Tax and Trade Bureau, 1310 G Street NW, Box 12, Washington, DC 20005; phone 202–453–1039, ext. 432.

SUPPLEMENTARY INFORMATION:**Background on Viticultural Areas****TTB Authority**

Section 105(e) of the Federal Alcohol Administration Act (FAA Act), 27 U.S.C. 205(e), authorizes the Secretary of the Treasury to prescribe regulations for the labeling of wine, distilled spirits, and malt beverages. The FAA Act provides that these regulations should, among other things, prohibit consumer deception and the use of misleading statements on labels and ensure that labels provide the consumer with adequate information as to the identity and quality of the product. The Alcohol and Tobacco Tax and Trade Bureau (TTB) administers the FAA Act pursuant to section 1111(d) of the Homeland Security Act of 2002, codified at 6 U.S.C. 531(d). In addition, the Secretary has delegated certain administration and enforcement of these authorities to TTB through Treasury Order 120–01.

Part 4 of the TTB regulations (27 CFR part 4) authorizes TTB to establish definitive viticultural areas and regulate the use of their names as appellations of

origin on wine labels and in wine advertisements. Part 9 of the TTB regulations (27 CFR part 9) sets forth standards for the preparation and submission to TTB of petitions for the establishment or modification of American viticultural areas (AVAs) and lists the approved AVAs.

Definition

Section 4.25(e)(1)(i) of the TTB regulations (27 CFR 4.25(e)(1)(i)) defines a viticultural area for American wine as a delimited grape-growing region having distinguishing features as described in part 9 of the regulations and, once approved, a name and a delineated boundary codified in part 9 of the regulations. These designations allow vintners and consumers to attribute a given quality, reputation, or other characteristic of a wine made from grapes grown in an area to the wine’s geographic origin. The establishment of AVAs allows vintners to describe more accurately the origin of their wines to consumers and helps consumers to identify wines they may purchase. Establishment of an AVA is neither an approval nor an endorsement by TTB of the wine produced in that area.

Requirements

Section 4.25(e)(2) of the TTB regulations (27 CFR 4.25(e)(2)) outlines the procedure for proposing an AVA and allows any interested party to petition TTB to establish a grape-growing region as an AVA. Section 9.12 of the TTB regulations (27 CFR 9.12) prescribes standards for petitions to establish or modify AVAs. Petitions to establish an AVA must include the following:

- Evidence that the area within the proposed AVA boundary is nationally or locally known by the AVA name specified in the petition;
- An explanation of the basis for defining the boundary of the proposed AVA;
- A narrative description of the features of the proposed AVA affecting viticulture, such as climate, geology, soils, physical features, and elevation, that make the proposed AVA distinctive and distinguish it from adjacent areas outside the proposed AVA boundary;
- If the proposed AVA is to be established within, or overlapping, an existing AVA, an explanation that both identifies the attributes of the proposed AVA that are consistent with the existing AVA and explains how the proposed AVA is sufficiently distinct from the existing AVA and therefore appropriate for separate recognition; and

- The appropriate United States Geological Survey (USGS) map(s) showing the location of the proposed AVA, with the boundary of the proposed AVA clearly drawn thereon; and

- A detailed narrative description of the proposed AVA boundary based on USGS map markings.

Notice of Proposed Rulemakings and Comments Received

TTB received a petition on behalf of Zirkle Fruit Company and local vineyard owners and winemakers proposing to establish the “Wanapum Village” AVA in Grant County, Washington. TTB proposed the establishment of the AVA in Notice No. 219, which published in the **Federal Register** on November 28, 2022 (87 FR 72927). In the notice, TTB summarized the evidence from the petition regarding the name, boundary, and distinguishing features for the proposed AVA. The notice also included information from the petition comparing the distinguishing features of the proposed AVA to the surrounding areas. For a detailed description of the evidence relating to the name, boundary, and distinguishing features of the proposed AVA, and for a detailed comparison of the distinguishing features of the proposed AVA to the surrounding areas, see Notice No. 219. The comment period closed on January 27, 2023. TTB received no comments in response to Notice No. 219.

However, after the comment period closed, TTB received a request from the original petitioner asking to change the name of the proposed AVA from “Wanapum Village” to “Beverly, Washington.” The petitioner stated that members of the Wanapum tribe expressed concerns about the use of their name for an AVA. The petitioner included sufficient name evidence to support the proposed name change.

As a result of the request, TTB published Notice No. 219A in the **Federal Register** on October 5, 2023 (88 FR 69113), proposing to change the name of the proposed Wanapum Village AVA to “Beverly, Washington.” No other changes to the proposed AVA were included in Notice No. 219A. The comment period closed December 4, 2023. TTB received one comment in response to Notice No. 219A. The anonymous public comment expressed support for use of the name “Beverly, Washington” for the AVA, based both on respect for the Wanapum tribe regarding use of their name and “Beverly” being a common name used in the local community to describe the region.

TTB Determination

After careful review of the petition and comment, TTB finds that the evidence provided by the petitioner supports the establishment of the Beverly, Washington AVA. Accordingly, under the authority of the FAA Act, section 1111(d) of the Homeland Security Act of 2002, and parts 4 and 9 of the TTB regulations, TTB establishes the “Beverly, Washington” AVA in Grant County, effective 30 days from the publication date of this document.

TTB has also determined that the Beverly, Washington AVA will remain part of the established Columbia Valley AVA. As discussed in Notice No. 219, the Beverly, Washington AVA shares some of the general viticultural features of the larger Columbia Valley AVA, such as elevations being below 2,000 feet and annual growing degree day (GDD) accumulations¹ that did not fall below 2,800. However, the Beverly, Washington AVA has some distinctive features, namely its soils. Within the Beverly, Washington AVA, soils are primarily formed from sand and gravel deposited by water and are classified as sand and stony loamy sand. By contrast, T.D. ATF–190, which established the Columbia Valley AVA, described the soils of the Columbia Valley AVA as fine-grained soils derived from wind-deposited silts and fine sand.

The Beverly, Washington Viticultural Area

Distinguishing features of the Beverly, Washington AVA include low, rolling hills with gentle to moderate slopes at an elevation of 515 to 950 feet. Soils are derived from ice-age flood deposits of sand and gravel mixed with wind-deposited sand and are excessively to somewhat excessively well-drained. The four main soil series dominating the Beverly, Washington AVA are the Burbank, Winchester, Schwana, and Quincy series. According to the petition, soils within the AVA are coarse soils, which are less susceptible to erosion than soils formed in silt and fine sand; therefore, cover crops are not currently used in the AVA. Also, coarse-textured soils without cover crops warm faster than fine-grained soils. Such warmer soils promote earlier onset of phenological states in grapes, such as bud break and veraison.

¹ See Albert J. Winkler, *General Viticulture* (Berkeley: University of California Press, 1974), pages 61–64. In the Winkler climate classification system, annual heat accumulation during the growing season, measured in annual GDDs, defines climatic regions. One GDD accumulates for each degree Fahrenheit (F) that a day’s mean temperature is above 50 degrees F, the minimum temperature required for grapevine growth.

Climate in the Beverly, Washington AVA is warm and windy with a higher average growing season temperature, and higher GDD accumulations than most of the surrounding regions. The average growing season temperatures for the AVA range from 65.8 degrees Fahrenheit to 71.8 degrees Fahrenheit, with an average maximum temperature ranging from 78.2 degrees Fahrenheit to 85.9 degrees Fahrenheit. GDD accumulations within the AVA range from 2,816 to 3,593. Wind speeds within the AVA are also high, with average wind speeds ranging from 7.1 miles per hour to 7.8 miles per hour. Maximum wind speeds can reach 28.2 miles per hour. According to the petition, warm temperatures and high GDD accumulations within the Beverly, Washington AVA allow vineyard owners to plant warmer-climate cultivars that require more heat to ripen. Additionally, cooler climate grape varieties planted in the AVA will ripen faster and accumulate more sugars than the same varieties planted in cooler regions. High winds within the AVA can reduce mildew pressure on the vines and promote development of smaller grapes with thicker skins.

To the west of the Beverly, Washington AVA is the Columbia River floodplain with elevations between 500 and 530 feet. Regions to the north and east of the AVA, which include the established Royal Slope AVA (27 CFR 9.271), have finer-grained soils, lower temperatures, and are less windy. The topography of the regions to the north and east of the AVA consists of a single gentle slope with elevations up to 1,756 feet. The soils within the Royal Slope AVA also differ from those of the Beverly, Washington AVA and consist of fewer medium-to coarse-grained soils.

To the immediate south of the Beverly, Washington AVA is a rugged 1,500-foot deep, 1.5-mile-wide cliff-walled canyon known as Sentinel Gap. This region has soils that are defined as “rubble land-rock outcrop complex,” making this particular area unsuitable for viticulture. Regions farther to the south, including the established Wahluke Slope AVA (27 CFR 9.192), are gently sloping and have soils similar to the Beverly, Washington AVA. Data suggests that temperatures in the established Wahluke Slope AVA are more varied than in the Beverly, Washington AVA, with some locations reporting similar temperatures and GDD accumulations, while other locations reported higher or lower temperatures and GDD accumulations. However, the average and maximum wind speeds in the Beverly, Washington AVA are

generally higher than in the Wahluke Slope AVA.

Boundary Description

See the narrative description of the boundary of the Beverly, Washington AVA in the regulatory text published at the end of this final rule.

Maps

The petitioner provided the required maps, and they are listed below in the regulatory text. The Beverly, Washington AVA boundary may also be viewed on the AVA Map Explorer on the TTB website, at <https://www.ttb.gov/wine/ava-map-explorer>.

Impact on Current Wine Labels

Part 4 of the TTB regulations prohibits any label reference on a wine that indicates or implies an origin other than the wine's true place of origin. For a wine to be labeled with an AVA name or with a brand name that includes an AVA name, at least 85 percent of the wine must be derived from grapes grown within the area represented by that name, and the wine must meet the other conditions listed in 27 CFR 4.25(e)(3). If the wine is not eligible for labeling with an AVA name and that name appears in the brand name, then the label is not in compliance and the bottler must change the brand name and obtain approval of a new label. Similarly, if the AVA name appears in another reference on the label in a misleading manner, the bottler would have to obtain approval of a new label. Different rules apply if a wine has a brand name containing an AVA name that was used as a brand name on a label approved before July 7, 1986. See 27 CFR 4.39(i)(2) for details.

With the establishment of the Beverly, Washington AVA, its name, "Beverly, Washington," will be recognized as a name of viticultural significance under § 4.39(i)(3) of the TTB regulations (27 CFR 4.39(i)(3)). The text of the regulations clarifies this point. Consequently, wine bottlers using the name "Beverly, Washington" in a brand name, including a trademark, or in another label reference to the origin of the wine, will have to ensure that the product is eligible to use the AVA name as an appellation of origin.

The establishment of the Beverly, Washington AVA will not affect any existing AVA. The establishment of the AVA will allow vintners to use "Beverly, Washington" or "Columbia Valley" as an appellation of origin for wines made primarily from grapes grown within the AVA if the wines meet the eligibility requirements for the appellation.

Regulatory Flexibility Act

TTB certifies that this regulation will not have a significant economic impact on a substantial number of small entities. The regulation imposes no new reporting, recordkeeping, or other administrative requirement. Any benefit derived from the use of an AVA name would be the result of a proprietor's efforts and consumer acceptance of wines from that area. Therefore, no regulatory flexibility analysis is required.

Executive Order 12866

It has been determined that this final rule is not a significant regulatory action as defined by Executive Order 12866 of September 30, 1993, as amended. Therefore, no regulatory assessment is required.

Drafting Information

Mimi Torello of the Regulations and Rulings Division drafted this final rule.

List of Subjects in 27 CFR Part 9

Wine.

The Regulatory Amendment

For the reasons discussed in the preamble, TTB amends title 27, chapter I, part 9, Code of Federal Regulations, as follows:

PART 9—AMERICAN VITICULTURAL AREAS

- 1. The authority citation for part 9 continues to read as follows:

Authority: 27 U.S.C. 205.

Subpart C—Approved American Viticultural Areas

- 2. Add § 9.297 to subpart C to read as follows:

§ 9.297 Beverly, Washington.

(a) *Name*. The name of the viticultural area described in this section is "Beverly, Washington". For purposes of part 4 of this chapter, "Beverly, Washington" is a term of viticultural significance.

(b) *Approved maps*. The one United States Geological Survey (USGS) 1:24,000 scale topographic map used to determine the boundary of the viticultural area is titled Beverly, Washington (2017).

(c) *Boundary*. The Beverly, Washington viticultural area is located in Grant County, Washington. The boundary of the Beverly, Washington viticultural area is described as follows:

(1) The beginning point is on the Beverly, Washington map at the intersection of State Highway 243 and

southern boundary of section 34 just north of the town of Schwana. From the beginning point, proceed northwest along Highway 243 to its intersection with an unnamed local road on the north side of Wanapum Village, near the center of section 21; then

(2) Proceed east in a straight line for 2,450 feet to the 600-foot elevation contour; then

(3) Proceed southeasterly along the 600-foot elevation contour for approximately 1,500 feet to its intersection with an unnamed local road in section 22; then

(4) Proceed northeasterly along the unnamed local road for approximately 3,000 feet to its intersection with another unnamed local road; then

(5) Proceed north-northeast in a straight line for approximately 500 feet to the intersection of Beverly Burke Road and an unnamed local road; then

(6) Proceed northeasterly along Beverly Burke Road to the point where it becomes concurrent with the northern boundary of section 22, and continue east along Beverly Burke Road to its intersection with the eastern boundary of section 22; then

(7) Proceed south along the eastern boundary of section 22 for one mile to its intersection with the northern boundary of section 26; then

(8) Proceed east along the northern boundary of section 26 for one mile to its intersection with the eastern boundary of section 26; then

(9) Proceed south along the eastern boundary of section 26 to its intersection with the 540-foot elevation contour; then

(10) Proceed southwesterly along the 540-foot elevation contour to its intersection with the southern boundary of section 26; then

(11) Proceed west along the southern boundary of section 26 to its intersection with the eastern boundary of section 34; then

(12) Proceed south along the eastern boundary of section 34 for 1 mile to its intersection with the southern boundary of section 34; then

(13) Proceed west along the southern boundary of section 34 for 0.5 mile to the beginning point.

Signed: October 22, 2024.

Mary G. Ryan,
Administrator.

Approved: October 23, 2024.

Aviva R. Aron-Dine,
Deputy Assistant Secretary, Tax Policy.

[FR Doc. 2024-25076 Filed 10-28-24; 8:45 am]

BILLING CODE 4810-31-P

DEPARTMENT OF HOMELAND SECURITY**Coast Guard****33 CFR Part 100****[Docket No. USCG–2024–0892]****Special Local Regulation; Key West World Championship, Key West, FL****AGENCY:** Coast Guard, DHS.**ACTION:** Notification of enforcement of regulation.

SUMMARY: The Coast Guard will enforce a special local regulation for the Key West World Championship high-speed boat race on November 6, 8, and 10, 2024, to provide for the safety of life on navigable waterways during this event. Our regulation for marine events within the Seventh Coast Guard District identifies the regulated area for this event in Key West, FL. During the enforcement period, no person or vessel may enter, transit through, anchor in, or remain within the regulated area without permission from the Captain of the Port Key West or a designated representative.

DATES: The regulations in 33 CFR 100.701 will be enforced for the Key West World Championship high-speed boat race regulated area in paragraph (b), item no. 4 in table 1 to § 100.701, daily from 10 a.m. until 4 p.m., on November 6, 8, and 10, 2024.

FOR FURTHER INFORMATION CONTACT: If you have questions about this notification of enforcement, call or email Lieutenant Hailye Wilson, Sector Key West Waterways Management Division, Coast Guard; telephone 305–292–8768, email *Hailye.M.Wilson@uscg.mil*.

SUPPLEMENTARY INFORMATION: The Coast Guard will enforce special local regulations in for the Key West World Championship high speed boat race area identified in table 1 to § 100.701, paragraph (b), item No. 4, on November 6, 8, and 10, 2024. This action is being taken to provide for the safety of life on navigable waterways during this event. Our regulation for recurring marine events, Sector Key West, § 100.701, table 1 paragraph (b), Item 4, specifies the location of the regulated area for the Key West World Championship high-speed boat race, which encompasses a portion of the Atlantic Ocean in Key West, Florida. During the enforcement periods, as reflected in § 100.701(c), all persons and vessels, except those persons and vessels participating in the high-speed boat race, are prohibited from entering, transiting through,

anchoring in, or remaining within the regulated area without obtaining permission from the Captain of the Port Key West or a designated representative.

In addition to this notice of enforcement in the **Federal Register**, the Coast Guard plans to provide notification of this enforcement period via the Local Notice to Mariners, marine information broadcasts, or both.

Dated: October 23, 2024.

Jason D. Ingram,*Captain, U.S. Coast Guard, Captain of the Port Key West.*

[FR Doc. 2024–25029 Filed 10–28–24; 8:45 am]

BILLING CODE 9110–04–P**DEPARTMENT OF HOMELAND SECURITY****Coast Guard****33 CFR Part 165****[Docket Number USCG–2024–0849]****RIN 1625–AA00****Safety Zone, Neuse River, New Bern, NC****AGENCY:** Coast Guard, DHS.**ACTION:** Temporary final rule.

SUMMARY: The Coast Guard is establishing a temporary safety zone on the navigable waters of the Neuse River in New Bern, North Carolina adjacent to the New Bern downtown waterfront and Union Point Park. This action is necessary to provide for the safety of life on these waters during an aerobatic air show on November 30, 2024. This rule prohibits persons and vessels from being in the safety zone unless authorized by the Captain of the Port (COTP) North Carolina or a designated representative.

DATES: This rule is effective from November 30, 2024, from 3 p.m. through 7 p.m.

ADDRESSES: To view documents mentioned in this preamble as being available in the docket, go to <https://www.regulations.gov>, type USCG–2024–0849 in the search box and click “Search.” Next, in the Document Type column, select “Supporting & Related Material.”

FOR FURTHER INFORMATION CONTACT: If you have questions on this rule, call or email Petty Officer Eric Gordon, Waterways Management Division, U.S. Coast Guard; telephone 571–608–8783, email *NCMarineevents@uscg.mil*.

SUPPLEMENTARY INFORMATION:**I. Table of Abbreviations**

CFR Code of Federal Regulations

COTP Captain of the Port
DHS Department of Homeland Security
FR Federal Register
NPRM Notice of proposed rulemaking
§ Section
U.S.C. United States Code

II. Background Information and Regulatory History

The Coast Guard is issuing this temporary rule without prior notice and opportunity to comment pursuant to authority under section 4(a) of the Administrative Procedure Act (APA) (5 U.S.C. 553(b)). This provision authorizes an agency to issue a rule without prior notice and opportunity to comment when the agency for good cause finds that those procedures are “impracticable, unnecessary, or contrary to the public interest.” Under 5 U.S.C. 553(b)(B), the Coast Guard finds that good cause exists for not publishing a notice of proposed rulemaking (NPRM) with respect to this rule because it would be impracticable to publish an NPRM and consider comments without delaying promulgation of the rule beyond November 30, 2024, the date of the air show, and it would be contrary to the public interest to delay promulgation of the rule until after the event occurs. The rule needs to be in effect by November 30, 2024, to protect persons and vessels from the hazards associated with this event. Such hazards include the possibility of an aircraft striking a vessel on the surface below the flight zone.

Under 5 U.S.C. 553(d)(3), the Coast Guard finds that good cause exists for making this rule effective less than 30 days after publication in the **Federal Register**. Delaying the effective date of this rule would be impracticable to publish this rule 30 days prior to the date of the event, and contrary to the public interest to delay publication past that date because the rule must be in place to protect persons and vessels from the hazards associated with this event on November 30, 2024.

III. Legal Authority and Need for Rule

The Coast Guard is issuing this rule under authority in 46 U.S.C. 70034. The Captain of the Port North Carolina (COTP) has determined that potential hazards associated with the Downtown New Bern Airshow, scheduled for 3:00 p.m. through 7:00 p.m. on November 30, 2024, is a safety concern for mariners during the time that aircraft perform aerobatic maneuvers directly above the Neuse River. This rule is necessary to protect personnel, vessels, and the marine environment from the hazards associated with the airshow above this position of the Neuse River.

IV. Discussion of the Rule

This rule establishes a temporary safety zone on a portion of the Neuse River on November 30, 2024, from 3:00 p.m. to 7:00 p.m. The rule will be enforced for the duration of the event. The date and times of enforcement will be broadcast locally over VHF–FM marine radio. The safety zone will include all navigable waters of the Neuse River in New Bern, North Carolina inside an area starting from approximate positions: latitude 35°06'55" N, longitude 077°02'04" W, then east to latitude 35°07'06" N, longitude 077°01'27" W, then southeast to latitude 35°06'49" N, longitude 077°01'12" W, then south to latitude 35°06'08" N, longitude 077°01'18" W, then west to latitude 35°06'02" N, longitude 077°01'57" W, then north to latitude 35°06'32" N, longitude 077°01'54" W, then north to the point of origin then north to the point of origin, for a total area of approximately 1 mile square.

The airshow will consist of three separate performances and will last a total approximately 4 hours. All aircraft will remain at least 500 feet above the ground. Public spectators will be allowed to view the event from the waterway, however, for safety reasons, the aircraft will not perform if there are any vessels inside the safety zone. The duration of this safety zone is intended to protect participants and spectators on the navigable waters of the Neuse River during the airshow. Vessels may transit the area, so long as they remain outside the safety zone. No vessel or person will be permitted to enter the safety zone without obtaining permission from the COTP North Carolina or a designated representative.

V. Regulatory Analyses

We developed this rule after considering numerous statutes and Executive orders related to rulemaking. Below we summarize our analyses based on a number of these statutes and Executive orders, and we discuss First Amendment rights of protestors.

A. Regulatory Planning and Review

Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits. This rule has not been designated a “significant regulatory action,” under section 3(f) of Executive Order 12866, as amended by Executive Order 14094 (Modernizing Regulatory Review). Accordingly, this rule has not been

reviewed by the Office of Management and Budget (OMB).

This regulatory action determination is based on the size, location, and duration of the safety zone. Vessel traffic will not be allowed to enter or transit a portion of the Neuse River during the airshow from 3:00 p.m. through 7:00 p.m. November 30, 2024. The Coast Guard will transmit a Broadcast Notice to Mariners via VHF–FM marine channel 16 regarding the enforcement area. This rule allows vessels to request permission to pass through the regulated area.

B. Impact on Small Entities

The regulatory flexibility analysis provisions of the Regulatory Flexibility Act of 1980, 5 U.S.C. 601–612, do not apply to rules not subject to notice and comment. As the Coast Guard has, for good cause, waived notice and comment requirement that would otherwise apply to this rulemaking, the Regulatory Flexibility Act’s provisions do not apply here. Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121), we want to assist small entities in understanding this rule. If the rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please call or email the person listed in the **FOR FURTHER INFORMATION CONTACT** section.

Small businesses may send comments on the actions of Federal employees who enforce, or otherwise determine compliance with, Federal regulations to the Small Business and Agriculture Regulatory Enforcement Ombudsman and the Regional Small Business Regulatory Fairness Boards. The Ombudsman evaluates these actions annually and rates each agency’s responsiveness to small business. If you wish to comment on actions by employees of the Coast Guard, call 1–888–REG–FAIR (1–888–734–3247). The Coast Guard will not retaliate against small entities that question or complain about this rule or any policy or action of the Coast Guard.

C. Collection of Information

This rule will not call for a new collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520).

D. Federalism and Indian Tribal Governments

A rule has implications for federalism under Executive Order 13132, Federalism, if it has a substantial direct effect on the States, on the relationship

between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government. We have analyzed this rule under that Order and have determined that it is consistent with the fundamental federalism principles and preemption requirements described in Executive Order 13132.

Also, this rule does not have Tribal implications under Executive Order 13175, Consultation and Coordination with Indian Tribal Governments, because it does not have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

E. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular, the Act addresses actions that may result in the expenditure by a State, local, or Tribal government, in the aggregate, or by the private sector of \$100,000,000 (adjusted for inflation) or more in any one year. Though this rule will not result in such an expenditure, we do discuss the effects of this rule elsewhere in this preamble.

F. Environment

We have analyzed this rule under Department of Homeland Security Directive 023–01, Rev. 1, associated implementing instructions, and Environmental Planning COMDTINST 5090.1 (series), which guide the Coast Guard in complying with the National Environmental Policy Act of 1969 (42 U.S.C. 4321–4370f), and have determined that this action is one of a category of actions that do not individually or cumulatively have a significant effect on the human environment. This rule involves a safety zone lasting 4 hours that will prohibit entry within a 1 square mile area of the Neuse River on November 30, 2024, from 3 p.m. to 7 p.m. It is categorically excluded from further review under paragraph L60(a) of Appendix A, Table 1 of DHS Instruction Manual 023–01–001–01, Rev. 1. A Record of Environmental Consideration supporting this determination is available in the docket. For instructions on locating the docket, see the **ADDRESSES** section of this preamble.

G. Protest Activities

The Coast Guard respects the First Amendment rights of protesters. Protesters are asked to call or email the

person listed in the **FOR FURTHER INFORMATION CONTACT** section to coordinate protest activities so that your message can be received without jeopardizing the safety or security of people, places, or vessels.

List of Subjects in 33 CFR Part 165

Harbors, Marine safety, Navigation (water), Reporting and recordkeeping requirements, Security measures, Waterways.

For the reasons discussed in the preamble, the Coast Guard amends 33 CFR part 165 as follows:

PART 165—REGULATED NAVIGATION AREAS AND LIMITED ACCESS AREAS

■ 1. The authority citation for part 165 continues to read as follows:

Authority: 46 U.S.C. 70034, 70051, 70124; 33 CFR 1.05–1, 6.04–1, 6.04–6, and 160.5; Department of Homeland Security Delegation No. 00170.1, Revision No. 01.3.

■ 2. Add § 165.T05–0512 to read as follows:

§ 165.T05–0512 Safety Zone; Neuse River, Airshow, New Bern, NC.

(a) *Location.* The following area is a safety zone: all navigable waters of the Neuse River in New Bern, North Carolina, inside an area starting from approximate positions: latitude 35°06'55" N, longitude 077°02'04" W, then east to latitude 35°07'06" N, longitude 077°01'27" W, then southeast to latitude 35°06'49" N, longitude 077°01'12" W, then south to latitude 35°06'08" N, longitude 077°01'18" W, then west to latitude 35°06'02" N, longitude 077°01'57" W, then north to latitude 35°06'32" N, longitude 077°01'54" W, then north to the point of origin, for a total area of approximately 1 mile square.

(b) *Definitions.* As used in this section—

Captain of the Port (COTP) means the Commander, Sector North Carolina.

Designated representative means a Coast Guard Patrol Commander, including a Coast Guard commissioned, warrant, or petty officer designated by the Captain of the Port North Carolina (COTP) for the enforcement of the safety zone.

(c) *Regulations.* (1) The general regulations governing safety zones in § 165.23 apply to the area described in paragraph (a) of this section.

(2) Entry into or remaining in this safety zone is prohibited unless authorized by the COTP North Carolina or the COTP North Carolina's designated representative. Unless permission to remain in the zone has been granted by the COTP North

Carolina or the COTP North Carolina's designated representative, a vessel within this safety zone must immediately depart the zone when this section becomes effective.

(3) The Captain of the Port, North Carolina can be reached through the Coast Guard Sector North Carolina Command Duty Officer, Wilmington, North Carolina, at telephone number 910–343–3882.

(4) The Coast Guard and designated security vessels enforcing the safety zone can be contacted on VHF–FM marine band radio channel 13 (165.65 MHz) and channel 16 (156.8 MHz).

(d) *Enforcement.* The U.S. Coast Guard may be assisted in the patrol and enforcement of the safety zone by Federal, State, and local agencies.

(e) *Enforcement period.* This section will be enforced from 3 p.m. through 7 p.m. on November 30, 2024.

Courtney A. Sergeant,

Commander, U.S. Coast Guard, Alternate Captain of the Port Sector North Carolina.

[FR Doc. 2024–25110 Filed 10–28–24; 8:45 am]

BILLING CODE 9110–04–P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 52

[EPA–R05–OAR–2023–0540; FRL–11835–02–R5]

Air Plan Approval; Wisconsin; SIP Alignment Revision

AGENCY: Environmental Protection Agency (EPA).

ACTION: Final rule.

SUMMARY: The Environmental Protection Agency (EPA) is approving an October 27, 2023, submittal from the Wisconsin Department of Natural Resources (WDNR) to align provisions approved in the Wisconsin State Implementation Plan (SIP) with current Wisconsin administrative rules and statutes. WDNR requested that certain provisions previously approved into the Wisconsin SIP under now obsolete numbering schemes be renumbered to ensure citations in the Wisconsin SIP reflect the current numbering systems of the Wisconsin Administrative Code (WAC) and the Wisconsin Statutes (Wis. Stats.). WDNR also requested that EPA approve rule and statute provisions that have been revised since they were approved into the Wisconsin SIP. Finally, WDNR requested removal of rules and statutes from the Wisconsin SIP that are no longer in effect in Wisconsin. Approval of these changes in the Wisconsin SIP

will not impact the state's air quality or ability to meet Clean Air Act (CAA) requirements. EPA proposed to approve this action on May 16, 2024, and received no comments.

DATES: This final rule is effective on November 29, 2024.

ADDRESSES: EPA has established a docket for this action under Docket ID No. EPA–R05–OAR–2023–0540. All documents in the docket are listed on the www.regulations.gov website. Although listed in the index, some information is not publicly available, *i.e.*, Confidential Business Information (CBI), Proprietary Business Information (PBI), or other information whose disclosure is restricted by statute. Certain other material, such as copyrighted material, is not placed on the internet and will be publicly available only in hard copy form. Publicly available docket materials are available either through www.regulations.gov or at the Environmental Protection Agency, Region 5, Air and Radiation Division, 77 West Jackson Boulevard, Chicago, Illinois 60604. This facility is open from 8:30 a.m. to 4:30 p.m., Monday through Friday, excluding Federal holidays. We recommend that you telephone Christos Panos at (312) 353–8328 before visiting the Region 5 office.

FOR FURTHER INFORMATION CONTACT: Christos Panos, Air and Radiation Division (AR–18J), Environmental Protection Agency, Region 5, 77 West Jackson Boulevard, Chicago, Illinois 60604, (312) 353–8328, panos.christos@epa.gov.

SUPPLEMENTARY INFORMATION: Throughout this document whenever “we,” “us,” or “our” is used, we mean EPA.

I. Background Information

On May 16, 2024 (89 FR 42829), EPA proposed to approve the SIP revision request submitted by Wisconsin on October 27, 2023. The revision includes primarily administrative changes to existing rules and updates to material adopted by reference related to rules in WAC Chapters 400, 415, 417, 431, 436, 445, 447, 492 and 493, and Wis. Stats. Chapters 15, 110, 285 and 299. Also, EPA proposed to approve Wisconsin's request for the removal of previously approved WAC rules and Wis. Stats. identified in Section 4 of the WDNR submittal. Most of the provisions that WDNR has removed are from Wis. Stats. that are obsolete. These provisions are no longer needed or have been replaced by other approved rules in the Wisconsin SIP. An explanation of the CAA requirements, a detailed analysis

of the revisions, and EPA's reasons for proposing approval were provided in the notice of proposed rulemaking (NPRM), and will not be restated here. The public comment period for this proposed rule ended on June 17, 2024. EPA received no comments on the proposal.

II. Final Action

EPA is approving the SIP revision request submitted by Wisconsin on October 27, 2023. As previously stated, the purpose of this SIP revision is to revise the current SIP approved Wisconsin administrative rules and statute provisions so that they are consistent with the current versions of the Wisconsin rules and statutes. This will provide clarity to regulators, sources, and the public as to what has been approved into the Wisconsin SIP. To accomplish this WDNR requested that EPA revise the SIP by (1) replacing citations to rules and statutes that were revised as part of, or after, the Wisconsin renumbering processes, and (2) approving provisions that were simply updated, but not renumbered, with the most current version of these rule or statute provisions. WDNR also requested that EPA remove certain provisions from the Wisconsin SIP that are no longer in effect in Wisconsin. These provisions were either repealed at the state level via rulemaking action, or were not retained in the WAC or Wis. Stats. during the renumbering processes. Therefore EPA is approving into the Wisconsin SIP all of the requested revisions which are contained in the following version of the state rules and statutes:

- Chapters 15, 110, 285 and 299, Updated 21–22 Wis. Stats., published October 4, 2023;
- NR 400, Wisconsin Register, July 2022 No. 799, effective August 1, 2022;
- NR 415, Wisconsin Register, April 2023 No. 808, effective May 1, 2023;
- NR 417, Wisconsin Register, November 1999 No. 526, effective November 1, 1999;
- NR 431, Wisconsin Register, November 2003 No. 574, effective November 1, 2003;
- NR 436, Wisconsin Register, November 1999 No. 526, effective November 1, 1999;
- NR 445, Wisconsin Register, March 2016 No. 723, effective April 1, 2016;
- NR 447, Wisconsin Register, June 2004 No. 582, effective July 1, 2004;
- NR 492, Wisconsin Register, April 2013 No. 688, effective May 1, 2013;
- NR 493, Wisconsin Register, November 1999 No. 527, effective December 1, 1999;

- Chapter Trans 131, Wisconsin Register, July 2023 No. 811, effective August 1, 2023.

III. Incorporation by Reference

In this rule, EPA is finalizing regulatory text that includes incorporation by reference. In accordance with requirements of 1 CFR 51.5, EPA is finalizing the incorporation by reference of the Wisconsin Regulations described in section II. of this preamble and set forth in the amendments to 40 CFR part 52 below. EPA has made, and will continue to make, these documents generally available through www.regulations.gov, and at the EPA Region 5 Office (please contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section of this preamble for more information).

Also in this document, EPA is removing EPA-Approved Wisconsin rules NR 422.02(24) and NR 493.05(5)(title) and EPA-Approved Wisconsin Statutes 144.30(9m), 144.30(9p), 144.30(9r), 144.30(17), 144.30(17m), 144.30(18), 144.30(18m), 144.30(19), 144.30(19m), 144.30(22), 144.30(22m), 144.3712(2), 144.3712(3), 144.395, 144.397(1), 144.399(2), 144.399(3) and 144.402 from the Wisconsin SIP, which is incorporated by reference in accordance with the requirements of 1 CFR part 51.

IV. Statutory and Executive Order Reviews

Under the CAA, the Administrator is required to approve a SIP submission that complies with the provisions of the CAA and applicable Federal regulations. 42 U.S.C. 7410(k); 40 CFR 52.02(a). Thus, in reviewing SIP submissions, EPA's role is to approve state choices, provided that they meet the criteria of the CAA. Accordingly, this action merely approves state law as meeting Federal requirements and does not impose additional requirements beyond those imposed by state law. For that reason, this action:

- Is not a significant regulatory action subject to review by the Office of Management and Budget under Executive Orders 12866 (58 FR 51735, October 4, 1993), and 14094 (88 FR 21879, April 11, 2023);
- Does not impose an information collection burden under the provisions of the Paperwork Reduction Act (44 U.S.C. 3501 *et seq.*);
- Is certified as not having a significant economic impact on a substantial number of small entities under the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*);
- Does not contain any unfunded mandate or significantly or uniquely

affect small governments, as described in the Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4);

- Does not have federalism implications as specified in Executive Order 13132 (64 FR 43255, August 10, 1999);
- Is not subject to Executive Order 13045 (62 FR 19885, April 23, 1997) because it approves a state program;
- Is not a significant regulatory action subject to Executive Order 13211 (66 FR 28355, May 22, 2001); and
- Is not subject to requirements of section 12(d) of the National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 272 note) because application of those requirements would be inconsistent with the CAA.

In addition, the SIP is not approved to apply on any Indian reservation land or in any other area where EPA or an Indian Tribe has demonstrated that a Tribe has jurisdiction. In those areas of Indian country, the rule does not have Tribal implications and will not impose substantial direct costs on Tribal governments or preempt Tribal law as specified by Executive Order 13175 (65 FR 67249, November 9, 2000).

Executive Order 12898 (Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Populations, 59 FR 7629, February 16, 1994) directs Federal agencies to identify and address “disproportionately high and adverse human health or environmental effects” of their actions on minority populations and low-income populations to the greatest extent practicable and permitted by law. EPA defines environmental justice (EJ) as “the fair treatment and meaningful involvement of all people regardless of race, color, national origin, or income with respect to the development, implementation, and enforcement of environmental laws, regulations, and policies.” EPA further defines the term fair treatment to mean that “no group of people should bear a disproportionate burden of environmental harms and risks, including those resulting from the negative environmental consequences of industrial, governmental, and commercial operations or programs and policies.”

WDNR did not evaluate EJ considerations as part of its SIP submittal; the CAA and applicable implementing regulations neither prohibit nor require such an evaluation. EPA did not perform an EJ analysis and did not consider EJ in this action. Consideration of EJ is not required as part of this action, and there is no information in the record inconsistent with the stated goal of E.O. 12898 of

achieving EJ for people of color, low-income populations and Indigenous peoples.

This action is subject to the Congressional Review Act, and EPA will submit a rule report to each House of the Congress and to the Comptroller General of the United States. This action is not a “major rule” as defined by 5 U.S.C. 804(2).

Under section 307(b)(1) of the CAA, petitions for judicial review of this action must be filed in the United States Court of Appeals for the appropriate circuit by December 30, 2024. Filing a petition for reconsideration by the Administrator of this final rule does not affect the finality of this action for the purposes of judicial review nor does it extend the time within which a petition for judicial review may be filed, and shall not postpone the effectiveness of such rule or action. This action may not be challenged later in proceedings to enforce its requirements. (See section 307(b)(2).)

List of Subjects in 40 CFR Part 52

Environmental protection, Air pollution control, Carbon monoxide, Incorporation by reference, Intergovernmental relations, Lead, Nitrogen dioxide, Ozone, Particulate matter, Reporting and recordkeeping requirements, Sulfur oxides, Volatile organic compounds.

Dated: October 23, 2024.

Debra Shore,

Regional Administrator, Region 5.

For the reasons stated in the preamble, title 40 CFR part 52 is amended as follows:

PART 52—APPROVAL AND PROMULGATION OF IMPLEMENTATION PLANS

■ 1. The authority citation for part 52 continues to read as follows:

Authority: 42 U.S.C. 7401 *et seq.*

■ 2. Section 52.2570 is amended by removing and reserving paragraphs (c) (13), (c)(14), (c)(15), (c)(22), (c)(27), (c)(28), (c)(30), (c)(32), (c)(33), (c)(34), (c)(36), (c)(39), (c)(40), (c)(41), (c)(42), (c)(43), (c)(45), (c)(49), (c)(72), (c)(78) and (c)(91), and by adding paragraph (c)(150) to read as follows:

§ 52.2570 Identification of plan.

* * * * *

(c) * * *

(150) On October 27, 2023, WDNR submitted a SIP revision request to align provisions approved in the Wisconsin SIP with current Wisconsin administrative rules and statutes. WDNR requested that certain provisions

previously approved into the Wisconsin SIP under now obsolete numbering schemes be renumbered to ensure citations in the Wisconsin SIP reflect the current numbering systems of the Wisconsin Administrative Code (WAC) and the Wisconsin Statutes (Wis. Stats.). WDNR also requested that EPA approve rule and statute provisions that have been revised since they were approved into the Wisconsin SIP. Finally, WDNR requested removal of rules and statutes from the Wisconsin SIP that are no longer in effect in Wisconsin. The rule and statute provisions that have been revised or removed were previously approved in paragraphs (c) (13), (c)(14), (c)(15), (c)(22), (c)(27), (c)(28), (c)(30), (c)(32), (c)(33), (c)(34), (c)(36), (c)(39), (c)(40), (c)(41), (c)(42), (c)(43), (c)(45), (c)(49), (c)(72), (c)(78) and (c)(91) of this section. Approval of these changes in the Wisconsin SIP will not impact the state’s air quality or ability to meet Clean Air Act requirements.

(i) *Incorporation by reference.* (A) Wisconsin Administrative Code, NR 400, except Note, 400.01, 400.02 (19m), (27m), (107m), (123e), and (123s), 400.03(1)(a) through (cm) and (dm) through (m), and 400.03(4)(jp) and (js), as published in the Wisconsin Register, July 2022 No. 799, effective August 1, 2022.

(B) Wisconsin Administrative Code, NR 415, except 415.01, 415.02(3) and (8), 415.075(1), (2)(a) intro, 1. through 4., 6. and 7., (b) and (c), (3)(a) through (e), (4), (5), and (6), 415.076, and 415.09(2) and (3)(a) through (c), as published in the Wisconsin Register, April 2023 No. 808, effective May 1, 2023.

(C) Wisconsin Administrative Code, NR 417, except Note, 417.01(2), 417.03, 417.05, and 417.07(2)(e) and (f), as published in the Wisconsin Register, November 1999 No. 526, effective November 1, 1999.

(D) Wisconsin Administrative Code, NR 431, only 431.03, 431.04 and 431.05, as published in the Wisconsin Register, November 2003 No. 574, effective November 1, 2003.

(E) Wisconsin Administrative Code, NR 436, except 436.01(2), 436.03(2), and 436.05(5), as published in the Wisconsin Register, November 1999 No. 526, effective November 1, 1999.

(F) Wisconsin Administrative Code, NR 445, only 445.16, as published in the Wisconsin Register, March 2016 No. 723, effective April 1, 2016.

(G) Wisconsin Administrative Code, NR 447, only 447.02 intro, (6), (7), (16), (18) Note, and (31), 447.07 (3) intro, (a) and (d), 447.12 (3)(b) Note, 447.16 (2), and 447.18 intro and (1) Note, as published in the Wisconsin Register,

June 2004 No. 582, effective July 1, 2004.

(H) Wisconsin Administrative Code, NR 492, only 492.03, as published in the Wisconsin Register, April 2013 No. 688, effective May 1, 2013.

(I) Wisconsin Administrative Code, NR 493, except Note and 493.01, as published in the Wisconsin Register, November 1999 No. 527.

(J) Wisconsin Administrative Code, Chapter Trans 131, as published in the Wisconsin Register, July 2023 No. 811, effective August 1, 2023.

(K) Wisconsin Statutes, Chapter 15, only 15.347(8), as revised by Updated 21–22 Wis. Stats., published October 4, 2023.

(L) Wisconsin Statutes, Chapter 110, only 110.20, as revised by Updated 21–22 Wis. Stats., published October 4, 2023.

(M) Wisconsin Statutes, Chapter 285, 285.01 except (17m), (21), (28), (33), (35), (38), (39), (40); 285.11 except (12), (13), (15), (16), (17), (18), (19); 285.13 except (7); 285.17 only (1); 285.19; 285.21 except (4); 285.23 except (6); 285.27 except (2)(d) and (3); 285.30; 285.31 only (5); 285.33 only (1); 285.35; 285.60 except (1)(b)2., (2g), (5m), (6)(b) and (c), (8), (9), (10) and (11); 285.61 except (5)(a) and (b), (10) and (11); 285.62; 285.63 except (11); 285.65; 285.66; 285.68; 285.69 except (1)(c), (1d), (2)(a), (c) intro, (c)2., (d) and (e), (2e), (2m), (3), (5), (6), and (7); 285.79; 285.81 except (1m) and (4); 285.83 except (2); and 285.87 except (2), as revised by Updated 21–22 Wis. Stats., published October 4, 2023.

(N) Wisconsin Statutes, Chapter 299, only 299.95, as revised by Updated 21–22 Wis. Stats., published October 4, 2023.

(ii) [Reserved]

[FR Doc. 2024–25032 Filed 10–28–24; 8:45 am]

BILLING CODE 6560–50–P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 180

[EPA–HQ–OPP–2020–0250; EPA–HQ–OPP–2020–0533; FRL–12339–01–OCSPP]

Glufosinate-P; Pesticide Tolerances

AGENCY: Environmental Protection Agency (EPA).

ACTION: Final rule.

SUMMARY: This regulation establishes tolerances for residues of glufosinate-P in or on multiple commodities, which are identified and discussed later in this document. BASF Corporation and MITSUI Chemicals Crop & Life

Solutions, INC requested these tolerances under the Federal Food, Drug, and Cosmetic Act (FFDCA).

DATES: This regulation is effective October 29, 2024. Objections and requests for hearings must be received on or before December 30, 2024 and must be filed in accordance with the instructions provided in 40 CFR part 178 (see also Unit I.C. of the **SUPPLEMENTARY INFORMATION**).

ADDRESSES: The docket for this action, identified by docket identification (ID) number EPA-HQ-OPP-2020-0250 and EPA-HQ-OPP-2020-0533 is available at <https://www.regulations.gov> or at the Office of Pesticide Programs Regulatory Public Docket (OPP Docket) in the Environmental Protection Agency Docket Center (EPA/DC), West William Jefferson Clinton Bldg., Rm. 3334, 1301 Constitution Ave. NW, Washington, DC 20460-0001. The Public Reading Room is open from 8:30 a.m. to 4:30 p.m., Monday through Friday, excluding legal holidays. The telephone number for the Public Reading Room and the OPP Docket is (202) 566-1744. Please review the visitor instructions and additional information about the docket available at <https://www.epa.gov/dockets>.

FOR FURTHER INFORMATION CONTACT: Charles Smith, Registration Division (7505P), Office of Pesticide Programs, Environmental Protection Agency, 1200 Pennsylvania Ave. NW, Washington, DC 20460-0001; main telephone number: 202-566-2427; email address: RDfrNotices@epa.gov.

SUPPLEMENTARY INFORMATION:

I. General Information

A. Does this action apply to me?

You may be potentially affected by this action if you are an agricultural producer, food manufacturer, or pesticide manufacturer. The following list of North American Industrial Classification System (NAICS) codes is not intended to be exhaustive, but rather provides a guide to help readers determine whether this document applies to them. Potentially affected entities may include:

- Crop production (NAICS code 111).
- Animal production (NAICS code 112).
- Food manufacturing (NAICS code 311).
- Pesticide manufacturing (NAICS code 32532).

B. How can I get electronic access to other related information?

You may access a frequently updated electronic version of EPA's tolerance regulations at 40 CFR part 180 through

the **Federal Register** Office's e-CFR site at <https://www.ecfr.gov/current/title-40>.

C. How can I file an objection or hearing request?

Under FFDCA section 408(g), 21 U.S.C. 346a, any person may file an objection to any aspect of this regulation and may also request a hearing on those objections. You must file your objection or request a hearing on this regulation in accordance with the instructions provided in 40 CFR part 178. To ensure proper receipt by EPA, you must identify docket ID number EPA-HQ-OPP-2020-0250 in the subject line on the first page of your submission. All objections and requests for a hearing must be in writing and must be received by the Hearing Clerk on or before December 30, 2024. Addresses for mail and hand delivery of objections and hearing requests are provided in 40 CFR 178.25(b).

In addition to filing an objection or hearing request with the Hearing Clerk as described in 40 CFR part 178, please submit a copy of the filing (excluding any Confidential Business Information (CBI)) for inclusion in the public docket. Information not marked confidential pursuant to 40 CFR part 2 may be disclosed publicly by EPA without prior notice. Submit the non-CBI copy of your objection or hearing request, identified by docket ID number EPA-HQ-OPP-2020-0250, by one of the following methods:

- **Federal eRulemaking Portal:** <https://www.regulations.gov>. Follow the online instructions for submitting comments. Do not submit electronically any information you consider to be CBI or other information whose disclosure is restricted by statute.

- **Mail:** OPP Docket, Environmental Protection Agency Docket Center (EPA/DC), (28221T), 1200 Pennsylvania Ave. NW, Washington, DC 20460-0001.

- **Hand Delivery:** To make special arrangements for hand delivery or delivery of boxed information, please follow the instructions at <https://www.epa.gov/dockets/where-send-comments-epa-dockets>.

Additional instructions on commenting or visiting the docket, along with more information about dockets generally, is available at <https://www.epa.gov/dockets>.

II. Summary of Petitioned-For Tolerance

In the **Federal Register** of March 24, 2023 (88 FR 17778) (FRL-10579-02-OCSP), EPA issued a document pursuant to FFDCA section 408(d)(3), 21 U.S.C. 346a(d)(3), announcing the filing of a pesticide petition (PP 2F9021) by

BASF Corporation Agricultural Solutions, 26 Davis Drive, P.O. Box 13528, Research Triangle Park, NC 27709. The petition requested that 40 CFR 180.473 be amended by modifying the tolerances for residues of glufosinate to include residues of L-glufosinate ammonium, glufosinate-P-ammonium [(2S)-2-amino-4-(hydroxymethylphosphinyl) butanoic acid -monoammonium salt] as measured by the sum of glufosinate (2-amino-4-(hydroxymethylphosphinyl)butanoic acid) and its metabolites, 2-(acetylamino)-4-(hydroxymethylphosphinyl) butanoic acid, and 3-(hydroxymethylphosphinyl) propanoic acid, expressed as 2-amino-4-(hydroxymethylphosphinyl)butanoic acid equivalents in or on canola, meal at 1.1 parts per million (ppm); cattle, fat at 0.40 ppm; cattle, meat at 0.15 ppm; cattle, meat byproducts at 6.0 ppm; corn, field, forage at 4.0 ppm; corn, field, grain at 0.20 ppm; corn, field, stover at 6.0 ppm; corn, sweet, forage at 1.5 ppm; corn, sweet, kernels plus cob with husks removed at 0.30 ppm; corn, sweet, stover at 6.0 ppm; cotton, gin byproducts at 30 ppm; cotton, seed, subgroup 20C at 15.00 ppm; egg at 0.15 ppm; goat, fat at 0.40 ppm; goat, meat at 0.15 ppm; goat, meat byproducts at 6.0 ppm; grain aspirated fractions at 25.00 ppm; hog, fat at 0.40 ppm; hog, meat at 0.15 ppm; hog, meat byproducts at 6.0 ppm; horse, fat at 0.40 ppm; horse, meat at 0.15 ppm; horse, meat byproducts at 6.0 ppm; milk at 0.15 ppm; poultry, fat at 0.15 ppm; poultry, meat at .15 ppm; poultry, meat byproducts at 0.60 ppm; rapeseed, subgroup 20A at 0.4 ppm; sheep, fat at 0.40 ppm; sheep, meat at 0.15 ppm; sheep, meat byproducts at 6.0 ppm; soybean at 2.0 ppm; soybean, hulls at 10.0 ppm and tolerances for indirect or inadvertent residues on barley, hay at 0.4 ppm; barley, straw at 0.4 ppm; buckwheat, fodder at 0.4 ppm; buckwheat, forage at 0.4 ppm; oat, forage at 0.4 ppm; oat, hay at 0.4 ppm; oat, straw at 0.4 ppm; rye, forage at 0.4 ppm; rye, straw at 0.4 ppm; teosinte at 0.4 ppm; triticale at 0.4 ppm; wheat, forage at 0.4 ppm; wheat, hay at 0.4 ppm; and wheat, straw at 0.4 ppm.

Also, in the **Federal Register** of December 21, 2020 (85 FR 82998) (FRL-10016-93), EPA issued a document pursuant to FFDCA section 408(d)(3), 21 U.S.C. 346a(d)(3), announcing the filing of a pesticide petition (PP 0F8842) by Meiji Seika Pharma Co., Ltd, c/o Landis International, Inc., 3185 Madison Highway, P.O. Box 5126, Valdosta, GA 31603-5126. The petition requested to establish tolerance for residues of L-

glufosinate free acid, (2S)-2-amino-4-[hydroxy(methyl)phosphinoyl]butyric acid, including its metabolites and degradates, 2-(acetylamino)-4-(hydroxymethyl phosphinyl) butanoic acid (NAG), and 3-(hydroxymethylphosphinyl) propanoic acid (MPP), expressed as 2-amino-4-(hydroxymethylphosphinyl)butanoic acid equivalents in or on apple at 0.05 ppm; beet, sugar, molasses at 5.0 ppm; beet, sugar, roots at 0.9 ppm; beet, sugar, tops (leaves) at 1.5 ppm; bushberry subgroup 13B at 0.15 ppm; canola, meal at 1.1 ppm; canola, seed at 0.40 ppm; cattle, fat at 0.40 ppm; cattle, meat at 0.15 ppm; cattle, meat byproducts at 6.0 ppm; corn, field, forage at 4.0 ppm; corn, field, grain at 0.20 ppm; corn, field, stover at 6.0 ppm; corn, sweet, forage at 1.5 ppm; corn, sweet, kernels plus cob with husks removed at 0.30 ppm; corn, sweet, stover at 6.0 ppm; cotton, gin byproducts at 15 ppm; cotton, undelinted seed at 4.0 ppm; egg at 0.15 ppm; fruit, citrus, crop group 10–10 at .15 ppm; fruit, pome, crop group 11–10 at .25 ppm; fruit, stone, crop group 12–12 at 0.30 ppm; goat, fat at 0.40 ppm; goat, meat at 0.15 ppm; goat, meat byproducts at 6.0 ppm; grape at 0.05 ppm; hog, fat at 0.40 ppm; hog, meat at 0.15 ppm; hog, meat byproducts at 6.0 ppm; horse, fat at 0.40 ppm; horse, meat at 0.15 ppm; horse, meat byproducts at 6.0 ppm; milk at 0.15 ppm; nut, tree, crop group 14–12 at 0.50 ppm; olive at 0.50 ppm; potato at 0.80 ppm; potato, chips at 1.6 ppm; potato, granules/flakes at 2.0 ppm; poultry, fat at 0.15 ppm; poultry, meat at .15 ppm; poultry, meat byproducts at 0.60 ppm; sheep, fat at 0.40 ppm; sheep, meat at 0.15 ppm; sheep, meat byproducts at 6.0 ppm; soybean at 2.0 ppm; soybean, hulls at 10.0 ppm.

These documents referenced summaries of the petitions prepared by BASF Corporation Agricultural Solutions and Meiji Seika Pharma Co., Ltd. (now known as MITSUI Chemicals Crop & Life Solutions), the petitioners, which are available in the docket, <https://www.regulations.gov>. One comment was received on the notice of filing for petition *0F8842*. No comments were received on the notice of filing for petition *2F9021*. EPA's response to this comment is discussed in Unit IV.C.

The tolerances EPA is establishing vary from what the petitioners have requested in a few ways, which are explained in greater detail in Unit IV.C. In sum, BASF Corporation Agricultural Solutions and MITSUI Chemicals Crop & Life Solutions have deleted crops from their initial request, the Agency will be establishing tolerances only on those crops as mentioned in Unit V.

Moreover, in order to align with the International Organization for Standardization (ISO) recognized nomenclature, EPA is establishing tolerances for glufosinate-P, which is the current standard name for L-glufosinate free acid. Because applications of glufosinate-P-ammonium (also known as L-glufosinate-ammonium) result in residues of glufosinate-P on crops, EPA is setting the tolerance for glufosinate-P residues, which will cover any residues that remain on food from applications of pesticides with either form of the pesticide.

III. Aggregate Risk Assessment and Determination of Safety

Section 408(b)(2)(A)(i) of FFDCA allows EPA to establish a tolerance (the legal limit for a pesticide chemical residue in or on a food) only if EPA determines that the tolerance is “safe.” Section 408(b)(2)(A)(ii) of FFDCA defines “safe” to mean that “there is a reasonable certainty that no harm will result from aggregate exposure to the pesticide chemical residue, including all anticipated dietary exposures and all other exposures for which there is reliable information.” This includes exposure through drinking water and in residential settings but does not include occupational exposure. Section 408(b)(2)(C) of FFDCA requires EPA to give special consideration to exposure of infants and children to the pesticide chemical residue in establishing a tolerance and to “ensure that there is a reasonable certainty that no harm will result to infants and children from aggregate exposure to the pesticide chemical residue. . . .”

Consistent with FFDCA section 408(b)(2)(D), and the factors specified in FFDCA section 408(b)(2)(D), EPA has reviewed the available scientific data and other relevant information in support of this action. EPA has sufficient data to assess the hazards of and to make a determination on aggregate exposure for L-glufosinate, including exposure resulting from the tolerances established by this action. EPA's assessment of exposures and risks associated with L-glufosinate follows.

A. Toxicological Profile

EPA has evaluated the available toxicity data and considered its validity, completeness, and reliability as well as the relationship of the results of the studies to human risk. EPA has also considered available information concerning the variability of the sensitivities of major identifiable subgroups of consumers, including infants and children.

Glufosinate is racemic mixture comprised of D- and L-stereoisomers, and the D/L form of glufosinate (also referred to as the racemic glufosinate) is currently registered as a pesticide (herbicide) in the United States. The L-isomer is the herbicidally active part of D/L-glufosinate, and the D-isomer is herbicidally inactive. The L-isomer is referred to as L-glufosinate in this document and the supporting risk assessment documents and refers to the active moiety from both L-glufosinate ammonium and L-glufosinate acid, which are two forms of the L-isomer used in pesticide formulations. As mentioned above the Agency has received applications for both L-glufosinate ammonium and L-glufosinate acid. The International Organization for Standardization (ISO) has designated L-glufosinate ammonium as glufosinate-P-ammonium and L-glufosinate free acid as glufosinate-P, so EPA is establishing tolerances using that nomenclature; however, for consistency with EPA's supporting risk assessments, this document is using the terms L-glufosinate ammonium and L-glufosinate acid.

The available *in vivo* and *in vitro* data for comparison across L-glufosinate acid and L-glufosinate ammonium, and the *in vitro* and *in vivo* DNT data for D/L-glufosinate ammonium indicate no significant differences in oral toxicities for the most sensitive endpoint (*i.e.*, neurotoxicity). As such, these databases are being considered together when assessing toxicity and selecting endpoints for pertinent exposures. Hence both L-glufosinate ammonium and L-glufosinate acid are considered toxicologically equivalent for oral and dermal exposure pathways. Also, L-glufosinate ammonium, when dissolved in water, dissociates to L-glufosinate acid. Therefore, the Agency considers glufosinate-P ammonium and glufosinate-P as functionally similar.

The targets identified following oral exposure to L-glufosinate were the brain and peripheral nervous system (rats, mice, and dogs), kidney (rats and mice), thyroid (rats only), and the adrenals (mice only). Neurotoxicity was observed after acute, subchronic, and chronic exposures. Adverse findings included clinical signs indicative of neurotoxicity (*i.e.*, tremors, clonic convulsions, inability to maintain body posture, etc.), increased motor activity, alterations in brain weight, and neuropathology of the brain, eye, and spinal cord. Kidney toxicity manifested as increased kidney weights, alterations in urinalysis parameters, and hypertrophy of the proximal tubular cells of the pars recta. Slight thyroid c-cell hyperplasia was

observed in male rats, while in mice, microscopic findings of the adrenal and increased adrenal weight were noted.

Increased quantitative susceptibility was observed in the L-glufosinate rat prenatal developmental toxicity study, the L-glufosinate range-finding developmental neurotoxicity (DNT) study, and the D/L-glufosinate DNT study.

L-glufosinate is classified as “*Not Likely to be Carcinogenic to Humans*” based on a lack of treatment-related tumor response in both the L-glufosinate rat and mouse carcinogenicity studies. There is a low concern for mutagenicity for L-glufosinate.

Specific information on the studies received and the nature of the adverse effects caused by L-glufosinate as well as the no-observed-adverse-effect-level (NOAEL) and the lowest-observed-adverse-effect-level (LOAEL) from the toxicity studies can be found at <https://www.regulations.gov> in document “L-Glufosinate. Human Health Risk Assessment for New Active Ingredient Isomer” at 21–34 in docket ID number EPA-HQ-OPP-2020-0250.

B. Toxicological Points of Departure/ Levels of Concern

Once a pesticide’s toxicological profile is determined, EPA identifies toxicological points of departure (POD) and levels of concern to use in evaluating the risk posed by human exposure to the pesticide. For hazards that have a threshold below which there is no appreciable risk, the toxicological POD is used as the basis for derivation of reference values for risk assessment. PODs are developed based on a careful analysis of the doses in each toxicological study to determine the dose at which no adverse effects are observed (the NOAEL) and the lowest dose at which adverse effects of concern are identified (the LOAEL). Uncertainty/safety factors are used in conjunction with the POD to calculate a safe exposure level, generally referred to as a population-adjusted dose (PAD) or a reference dose (RfD), and a safe margin of exposure (MOE). For non-threshold risks, the Agency assumes that any amount of exposure will lead to some degree of risk. Thus, the Agency estimates risk in terms of the probability of an occurrence of the adverse effect expected in a lifetime. For more information on the general principles EPA uses in risk characterization and a complete description of the risk assessment process, see <https://www.epa.gov/pesticide-science-and-assessing-pesticide-risks/assessing-human-health-risk-pesticides>.

For more detailed information on the toxicological endpoints for L-glufosinate used for human risk assessment can be found in the L-Glufosinate. Human Health Risk Assessment for New Active Ingredient Isomer in docket ID number EPA-HQ-OPP-2020-0250.

C. Exposure Assessment

1. *Dietary exposure from food and feed uses.* In evaluating dietary exposure to L-glufosinate, EPA considered exposure to L-glufosinate under all tolerances established for racemic glufosinate as well as the petitioned-for tolerances in this rulemaking. EPA assessed dietary exposures from L-glufosinate in food as follows:

i. *Acute exposure.* Quantitative acute dietary exposure and risk assessments are performed for a food-use pesticide if a toxicological study has indicated the possibility of an effect of concern occurring as a result of a 1-day or single exposure.

Such effects were identified for L-glufosinate. In conducting the acute dietary exposure assessment, EPA used the Dietary Exposure Evaluation Model software with the Food and Commodity Intake Database (DEEM-FCID) Version 3.16. This software uses the 2003–2008 food consumption data from the U.S. Department of Agriculture’s (USDA’s) National Health and Nutrition Examination Survey, What We Eat in America (NHANES/WWEIA). As to residue levels in food, EPA conducted an unrefined acute dietary exposure assessment for L-glufosinate assuming tolerance-level residues for L-glufosinate (scaled by 0.5X for application rate adjustment) and 100% CT assumptions for all crops and livestock commodities. The proposed uses of L-glufosinate exactly match the established uses of D/L-glufosinate in terms of crops, number of applications, retreatment intervals, and preharvest intervals; the only difference being that the use rate for L-glufosinate is one-half that of D/L-glufosinate, consistent with herbicidal activity residing primarily in the L-isomer. Since the rate of L-glufosinate is one-half that of D/L-glufosinate, the expected residues for L-glufosinate are one-half those of D/L-glufosinate.

ii. *Chronic exposure.* The chronic dietary exposure assessment also uses the DEEM-FCID Version 3.16 software with the 2003–2008 NHANES/WWEIA data. As to residue levels in food, EPA conducted a partially refined chronic dietary exposure assessment using anticipated residues based on average field trial residue levels for plant commodities, average calculated

residues for livestock commodities, all foods scaled by 0.5X for application rate adjustment, and 100% CT.

iii. *Cancer.* Based on the data summarized in Unit III.A., EPA has concluded that L-glufosinate does not pose a cancer risk to humans. Therefore, a dietary exposure assessment for the purpose of assessing cancer risk is unnecessary.

iv. *Anticipated residue and percent crop treated (PCT) information.*

Section 408(b)(2)(E) of the FFDCA authorizes EPA to use available data and information on the anticipated residue levels of pesticide residues in food and the actual levels of pesticide residues that have been measured in food. If EPA relies on such information, EPA must require pursuant to FFDCA section 408(f)(1) that data be provided 5 years after the tolerance is established, modified, or left in effect, demonstrating that the levels in food are not above the levels anticipated. For the present action, EPA will issue such data call-ins as are required by FFDCA section 408(b)(2)(E) and authorized under FFDCA section 408(f)(1). Data will be required to be submitted no later than 5 years from the date of issuance of these tolerances.

The Agency is not using percent crop treated estimates for assessing acute and chronic exposures.

2. *Dietary exposure from drinking water.* The Agency used screening-level water exposure models in the dietary exposure analysis and risk assessment for L-glufosinate in drinking water. These simulation models take into account data on the physical, chemical, and fate/transport characteristics of L-glufosinate. Further information regarding EPA drinking water models used in pesticide exposure assessment can be found at <https://www.epa.gov/pesticide-science-and-assessing-pesticide-risks/models-pesticide-risk-assessment>.

Determination of the residues of concern for human health in drinking water included consideration of racemic glufosinate and the degradate, 3-methylphosphinico-propionic acid (MPP). Although the chronic EDWCs for MPP are approximately 2× higher than the EDWCs for the racemic glufosinate, EPA has determined that using the EDWCs for the racemic glufosinate will be protective of effects that might occur from exposure to the degradate. This conclusion is based on a comparison of the toxicity databases for glufosinate and MPP, which indicate that glufosinate is more than twice as potent as MPP. Because the toxic effects from glufosinate and MPP are significantly

different, an aggregate assessment of glufosinate and MPP is not appropriate.

Based on the Pesticides in Water Calculator (PWC; version 1.52), the estimated drinking water concentrations (EDWCs) of D/L-glufosinate are estimated to be 201 parts per billion (ppb) for acute dietary exposures and 24.4 ppb for chronic dietary exposures. Surface water simulations resulted in the highest EDWCs.

These values reflect application of D/L-glufosinate and were scaled by half to reflect the reduced application rate and expected concentrations of L-glufosinate in water. The adjusted EDWCs were incorporated in the Dietary Exposure Evaluation Model software with the Food Commodity Intake Database (DEEM-FCID) into the food categories “water, direct, all sources” and “water, indirect, all sources.”

3. *From non-dietary exposure.* The term “residential exposure” is used in this document to refer to non-occupational, non-dietary exposure (e.g., for lawn and garden pest control, indoor pest control, termiticides, and flea and tick control on pets).

L-glufosinate is not being proposed for residential uses. However, there are residential exposures to L-glufosinate as a result of the existing residential uses of the racemic glufosinate. These exposures have been assessed for L-glufosinate and are included in a short-term aggregate assessment for L-glufosinate. For this assessment, the application rate was scaled by 0.5× to reflect residues of L-glufosinate only, and the application rate was converted to acid equivalents because the PODs are likewise expressed as acid equivalents. For currently registered uses of racemic glufosinate, residential handler and post-application dermal and inhalation risks are not of concern for L-glufosinate. The scenarios that are recommended to be considered for aggregate risk assessment are high-contact lawn activities for adults and children 1 to <2 years old and golfer activities for children 6 to <11 years old and children 11 to <16 years old.

4. *Cumulative effects from substances with a common mechanism of toxicity.* Section 408(b)(2)(D)(v) of FFDCA requires that, when considering whether to establish, modify, or revoke a tolerance, the Agency consider “available information” concerning the cumulative effects of a particular pesticide’s residues and “other substances that have a common mechanism of toxicity.”

Unlike other pesticides for which EPA has followed a cumulative risk approach based on a common mechanism of toxicity, EPA has not made a common

mechanism of toxicity finding as to L-glufosinate and any other substances and L-glufosinate does not appear to produce a toxic metabolite produced by other substances. For the purposes of this action, therefore, EPA has not assumed that L-glufosinate has a common mechanism of toxicity with other substances. For information regarding EPA’s efforts to determine which chemicals have a common mechanism of toxicity and to evaluate the cumulative effects of such chemicals, see EPA’s website at <https://www.epa.gov/pesticide-science-and-assessing-pesticide-risks/pesticide-cumulative-risk-assessment-framework>.

D. Safety Factor for Infants and Children

1. *In general.* Section 408(b)(2)(C) of FFDCA provides that EPA shall apply an additional tenfold (10×) margin of safety for infants and children in the case of threshold effects to account for prenatal and postnatal toxicity and the completeness of the database on toxicity and exposure unless EPA determines based on reliable data that a different margin of safety will be safe for infants and children. This additional margin of safety is commonly referred to as the FQPA Safety Factor (SF). In applying this provision, EPA either retains the default value of 10×, or uses a different additional safety factor when reliable data available to EPA support the choice of a different factor.

2. *Prenatal and postnatal sensitivity.* Increased quantitative susceptibility was observed in the L-glufosinate rat prenatal developmental toxicity study, the L-glufosinate range-finding DNT study, and the D/L-glufosinate DNT study. Quantitative susceptibility was observed in the developmental rat study in which decreased fetal body weight in both sexes was observed at the highest dose tested; however, no maternal toxicity was identified. Quantitative susceptibility was observed in a L-glufosinate dose-range finding DNT study in which maternal effects were not observed up to the highest dose tested while offspring toxicity manifested as decreased pup body weight and increased total and ambulatory motor activity counts in males. The D/L-glufosinate DNT study observed alterations in brain morphometrics (a decrease in the mean length of the ventral limb of the dentate hilus), an increase in motor activity, and a decrease in body weight for the offspring at a dose level that did not elicit maternal toxicity.

3. *Conclusion.* EPA has determined that reliable data show the safety of infants and children would be

adequately protected if the FQPA SF were reduced to 1× for all exposure scenarios for glufosinate-P. That decision is based on the following findings:

i. The toxicity database for L-glufosinate is complete, as a result of bridging data between the racemic glufosinate, L-glufosinate, and L-glufosinate ammonium databases.

ii. Evidence of neurotoxicity was observed in the L-glufosinate database in both adults and early life stages. However, the concern is low because all selected endpoints are based on, and protective of, the most sensitive neurotoxic effects in the database, as indicated by the following: (1) the 17% increase in motor activity observed in females in the 28-day range-finding subchronic rat study occurred at a dose level that is approximately 13×–80× higher than the selected PODs; (2) the decreased brain weight and vacuolation of the cerebrum in the chronic mouse study occurred at dose levels approximately 11×–67× higher than the selected PODs; (3) the neuropathology observed in the subchronic neurotoxicity study occurred at a dose level approximately 29×–174× higher than the selected PODs; (4) the increased total and ambulatory motor activity counts in the range-finding DNT study occurred at a dose level approximately 27× higher than the selected PODs; and (5) the brain morphometric changes and increased motor activity observed in the offspring in the D/L-glufosinate DNT occurred at a dose level approximately 42× higher than the selected PODs for all relevant exposure scenarios.

iii. As discussed in Unit III.D.2. above, increased quantitative susceptibility was observed in the L-glufosinate rat prenatal developmental toxicity study, the L-glufosinate range-finding DNT study, and the D/L-glufosinate ammonium DNT study. However, the concern for the increased susceptibility is low, as clear NOAELs have been identified for those studies and all selected PODs are protective of the effects seen in those studies.

iv. There are no residual uncertainties identified in the exposure databases.

The dietary food exposure assessments were performed based on 100% CT and conservative residue estimates. EPA made conservative (protective) assumptions in the ground and surface water modeling used to assess exposure to L-glufosinate in drinking water. These assessments will not underestimate the exposure and risks posed by L-glufosinate.

E. Aggregate Risks and Determination of Safety

EPA determines whether acute and chronic dietary pesticide exposures are safe by comparing aggregate exposure estimates to the acute PAD (aPAD) and chronic PAD (cPAD). For linear cancer risks, EPA calculates the lifetime probability of acquiring cancer given the estimated aggregate exposure. Short-, intermediate-, and chronic-term aggregate risks are evaluated by comparing the estimated aggregate food, water, and residential exposure to the appropriate PODs to ensure that an adequate MOE exists.

1. *Acute risk.* Using the exposure assumptions discussed in this unit for acute exposure, the acute dietary exposure to L-glufosinate from food and water will occupy 26% of the aPAD with the females 13 to 49 years old population subgroup. For all the other population subgroups, the most highly exposed population subgroup is all infants (<1 year old) at 4.7% of the aPAD.

2. *Chronic risk.* Using the exposure assumptions described in this unit for chronic exposure, EPA has concluded that chronic exposure to L-glufosinate from food and water will utilize 12% of the cPAD for children (1–2 years old), the population group receiving the highest exposure.

3. *Short-term risk.* Short-term aggregate exposure takes into account short-term residential exposure plus chronic exposure to food and water (considered to be a background exposure level). Using the exposure assumptions described in this unit for short-term exposures, EPA has concluded the combined short-term food, water, and residential exposures result in aggregate MOEs of 1,100 for adults, 2,600 for children (11 to <16 years old), 1,700 for children (6 to <11 years old) and 230 for children (1 to <2 years old), which are above the LOC (100) and are not of concern.

4. *Intermediate-term risk.* Intermediate-term aggregate exposure takes into account intermediate-term residential exposure plus chronic exposure to food and water (considered to be a background exposure level).

An intermediate-term adverse effect was identified; however, L-glufosinate is not registered for any use patterns that would result in intermediate-term residential exposure. Because there is no intermediate-term residential exposure and chronic dietary exposure has already been assessed under the appropriately protective cPAD, no further assessment of intermediate-term risk is necessary, and EPA relies on the

chronic dietary risk assessment for evaluating intermediate-term risk for L-glufosinate.

5. *Aggregate cancer risk for U.S. population.* Based on the lack of evidence of carcinogenicity in two adequate rodent carcinogenicity studies, L-glufosinate is not expected to pose a cancer risk to humans.

6. *Determination of safety.* Based on these risk assessments, EPA concludes that there is a reasonable certainty that no harm will result to the general population or to infants and children from aggregate exposure to L-glufosinate residues.

IV. Other Considerations

A. Analytical Enforcement Methodology

Two analytical methods have been validated by the Analytical Chemistry Branch (ACB) for enforcement of the currently established tolerances of D/L-glufosinate: (1) method HRAV–5A was validated by ACB for the determination of glufosinate and MPP in/on apple, grape, almond, soybean seed, corn grain, and corn forage and (2) method BK/01/99 was validated by ACB for determination of glufosinate, N-acetylglufosinate (NAG), and MPP in/on canola seed and sugar beet root.

Based on the results from the petition method validations (PMVs) and the ability of the methods to detect both the D- and L- isomers of glufosinate, EPA concludes that adequate enforcement methods are available for L-glufosinate.

The method may be requested from: Chief, Analytical Chemistry Branch, Environmental Science Center, 701 Mapes Rd., Ft. Meade, MD 20755–5350; telephone number: (410) 305–2905; email address: residuemethods@epa.gov.

B. International Residue Limits

In making its tolerance decisions, EPA seeks to harmonize U.S. tolerances with international standards whenever possible, consistent with U.S. food safety standards and agricultural practices. EPA considers the international maximum residue limits (MRLs) established by the Codex Alimentarius Commission (Codex), as required by FFDCA section 408(b)(4). The Codex Alimentarius is a joint United Nations Food and Agriculture Organization/World Health Organization food standards program, and it is recognized as an international food safety standards-setting organization in trade agreements to which the United States is a party. EPA may establish a tolerance that is different from a Codex MRL; however, FFDCA section 408(b)(4) requires that

EPA explain the reasons for departing from the Codex level.

The Codex has not established a MRL for L-glufosinate.

C. Response to Comments

The Agency did receive one comment raising concerns that there are studies indicating that L-glufosinate is harmful and toxic to health of humans even in small doses. The commenter was also concerned over the use of L-glufosinate on corn, cotton and soybean which are staples of American diet. The commenter emphasized the role of EPA in reasonably assessing its analysis of pesticide tolerances, safety, and awareness of disproportionate effects of agricultural production, and its firm commitment to environmental justice.

Although the Agency recognizes that some individuals believe that pesticides should be banned on agricultural crops, the existing legal framework provided by section 408 of the FFDCA authorizes EPA to establish tolerances when it determines that the tolerance is safe. Upon consideration of the validity, completeness, and reliability of the available data as well as other factors the FFDCA requires EPA to consider, EPA has determined that these glufosinate-P tolerances are safe. The commenter provided no information supporting a conclusion that glufosinate-P is not safe, nor did the commenter provide any basis for concluding that the tolerances would have a disproportionate effect on any population.

D. Revisions to Petitioned-For Tolerances

The Agency is establishing a tolerance for residues of glufosinate-P, including its metabolites and degradates, that result from applications of glufosinate-P or glufosinate-P-ammonium, with compliance to be determined by measuring the sum of glufosinate (2-amino-4-(hydroxymethylphosphinyl) butanoic acid) and its metabolites, 2-(acetylamino)-4-(hydroxymethyl phosphinyl) butanoic acid, and 3-(hydroxymethylphosphinyl) propanoic acid, expressed as 2-amino-4-(hydroxymethylphosphinyl)butanoic acid equivalents. BASF Corporation had petitioned for expression of L-glufosinate-ammonium, glufosinate-P-ammonium [(2S)-2-amino-4-(hydroxymethylphosphinyl) butanoic acid -monoammonium salt] as measured by the sum of glufosinate (2-amino-4-(hydroxymethylphosphinyl)butanoic acid) and its metabolites, 2-(acetylamino)-4-(hydroxymethyl phosphinyl) butanoic acid, and 3-(hydroxymethylphosphinyl) propanoic

acid, expressed as 2-amino-4-(hydroxymethylphosphinyl)butanoic acid, and MITSUI Chemicals Crop & Life Solutions, Inc. had petitioned for expression of L-glufosinate free acid, (2S)-2-amino-4-[hydroxy(methyl)phosphinoyl]butyric acid, including its metabolites and degradates, 2-(acetylamino)-4-(hydroxymethylphosphinyl) butanoic acid (NAG), and 3-(hydroxymethylphosphinyl) propanoic acid (MPP), expressed as 2-amino-4-(hydroxymethylphosphinyl) butanoic acid equivalents. As discussed in Unit III.A, glufosinate-P-ammonium (also referred to as L-glufosinate ammonium) is the ammonium salt of glufosinate-P (also referred to as L-glufosinate acid). Since the glufosinate-P-ammonium breaks down into residues of glufosinate-P, EPA is establishing the tolerances for residues of glufosinate-P including its metabolites and degradates, that may result from applications of either form of glufosinate-P.

In addition, the petitioners have withdrawn their requests to establish tolerances on the following crops, so EPA is not establishing tolerances on those crops at this time: apple; beet, sugar, molasses; beet, sugar, roots; beet, sugar, tops (leaves); bushberry subgroup 13–07B; fruit, citrus, crop group 10–10; fruit, pome, crop group 11–10; fruit, stone, crop group 12–12; grape; nut, tree, crop group 14–12; olive; potato; potato, chips; and potato, granules/flakes.

Finally, EPA has applied its policy on OECD Rounding Classes to the petitioned-for tolerances to establish tolerances without trailing zeros after the decimal place.

V. Conclusion

Therefore, tolerances are established for residues of glufosinate-P including its metabolites and degradates in or on canola, meal at 1.1 parts per million (ppm); cattle, fat at 0.4 ppm; cattle, meat at 0.15 ppm; cattle, meat byproducts at 6 ppm; corn, field, forage at 4 ppm; corn, field, grain at 0.2 ppm; corn, field, stover at 6 ppm; corn, sweet, forage at 1.5 ppm; corn, sweet, kernels plus cob with husks removed at 0.3 ppm; corn, sweet, stover at 6 ppm; cotton, gin byproducts at 30 ppm; cotton, seed, subgroup 20C at 15 ppm; egg at 0.15 ppm; goat, fat at 0.4 ppm; goat, meat at 0.15 ppm; goat, meat byproducts at 6 ppm; grain aspirated fractions at 25 ppm; hog, fat at 0.4 ppm; hog, meat at 0.15 ppm; hog, meat byproducts at 6 ppm; horse, fat at 0.4 ppm; horse, meat at 0.15 ppm; horse, meat byproducts at 6 ppm; milk at 0.15 ppm; poultry, fat at 0.15 ppm; poultry, meat at 0.15 ppm;

poultry, meat byproducts at 0.6 ppm; rapeseed, subgroup 20A at 0.4 ppm; sheep, fat at 0.4 ppm; sheep, meat at 0.15 ppm; sheep, meat byproducts at 6 ppm; soybean at 2 ppm; soybean, hulls at 10 ppm.

In addition, tolerances are established for indirect or inadvertent residues of glufosinate-P including its metabolites and degradates in or on barley, hay at 0.4 ppm; barley, straw at 0.4 ppm; buckwheat, fodder at 0.4 ppm; buckwheat, forage at 0.4 ppm; oat, forage at 0.4 ppm; oat, hay at 0.4 ppm; oat, straw at 0.4 ppm; rye, forage at 0.4 ppm; rye, straw at 0.4 ppm; teosinte at 0.4 ppm; triticale at 0.4 ppm; wheat, forage at 0.4 ppm; wheat, hay at 0.4 ppm; and wheat, straw at 0.4 ppm.

VI. Statutory and Executive Order Reviews

This action establishes tolerances under FFDCA section 408(d) in response to a petition submitted to the Agency. The Office of Management and Budget (OMB) has exempted these types of actions from review under Executive Order 12866, entitled “Regulatory Planning and Review” (58 FR 51735, October 4, 1993). Because this action has been exempted from review under Executive Order 12866, this action is not subject to Executive Order 13211, entitled “Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use” (66 FR 28355, May 22, 2001) or Executive Order 13045, entitled “Protection of Children from Environmental Health Risks and Safety Risks” (62 FR 19885, April 23, 1997). This action does not contain any information collections subject to OMB approval under the Paperwork Reduction Act (PRA) (44 U.S.C. 3501 *et seq.*), nor does it require any special considerations under Executive Order 12898, entitled “Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations” (59 FR 7629, February 16, 1994).

Since tolerances and exemptions that are established on the basis of a petition under FFDCA section 408(d), such as the tolerances in this final rule, do not require the issuance of a proposed rule, the requirements of the Regulatory Flexibility Act (RFA) (5 U.S.C. 601 *et seq.*), do not apply.

This action directly regulates growers, food processors, food handlers, and food retailers, not States or tribes, nor does this action alter the relationships or distribution of power and responsibilities established by Congress in the preemption provisions of FFDCA section 408(n)(4). As such, the Agency

has determined that this action will not have a substantial direct effect on States or Tribal governments, on the relationship between the national government and the States or Tribal governments, or on the distribution of power and responsibilities among the various levels of government or between the Federal Government and Indian tribes. Thus, the Agency has determined that Executive Order 13132, entitled “Federalism” (64 FR 43255, August 10, 1999) and Executive Order 13175, entitled “Consultation and Coordination with Indian Tribal Governments” (65 FR 67249, November 9, 2000) do not apply to this action. In addition, this action does not impose any enforceable duty or contain any unfunded mandate as described under Title II of the Unfunded Mandates Reform Act (UMRA) (2 U.S.C. 1501 *et seq.*).

This action does not involve any technical standards that would require Agency consideration of voluntary consensus standards pursuant to section 12(d) of the National Technology Transfer and Advancement Act (NTTAA) (15 U.S.C. 272 note).

VII. Congressional Review Act

Pursuant to the Congressional Review Act (5 U.S.C. 801 *et seq.*), EPA will submit a report containing this rule and other required information to the U.S. Senate, the U.S. House of Representatives, and the Comptroller General of the United States prior to publication of the rule in the **Federal Register**. This action is not a “major rule” as defined by 5 U.S.C. 804(2).

List of Subjects in 40 CFR Part 180

Environmental protection, Administrative practice and procedure, Agricultural commodities, Pesticides and pests, Reporting and recordkeeping requirements.

Dated: October 21, 2024.

Elizabeth Vizard,

Acting Director, Office of Pesticide Programs.

Therefore, for the reasons stated in the preamble, 40 CFR chapter I is amended as follows:

PART 180—TOLERANCES AND EXEMPTIONS FOR PESTICIDE CHEMICAL RESIDUES IN FOOD

■ 1. The authority citation for part 180 continues to read as follows:

Authority: 21 U.S.C. 321(q), 346a and 371.

■ 2. Revise and republish § 180.473 to read as follows:

§ 180.473 Glufosinate; tolerances for residues.

(a) *General.* (1) Tolerances are established for residues of glufosinate, including its metabolites and degradates, in or on the commodities in table 1 to paragraph (a)(1). Compliance with the tolerance levels specified in table 1 to paragraph (a)(1) is to be determined by measuring the sum of glufosinate (2-amino-4-(hydroxymethylphosphinyl)butanoic acid) and its metabolites, 2-(acetylamino)-4-(hydroxymethyl phosphinyl) butanoic acid, and 3-(hydroxymethylphosphinyl) propanoic acid, expressed as 2-amino-4-(hydroxymethylphosphinyl)butanoic acid equivalents.

TABLE 1 TO PARAGRAPH (a)(1)

Commodity	Parts per million
Almond, hulls	0.50
Banana ¹	0.30
Beet, sugar, molasses	5.0
Beet, sugar, roots	0.9
Beet, sugar, tops (leaves)	1.5
Bushberry subgroup 13–07B ..	0.15
Canola, meal	1.1
Cattle, fat	0.40
Cattle, meat	0.15
Cattle, meat byproducts	6.0
Corn, field forage	4.0
Corn, field, grain	0.20
Corn, field, stover	6.0
Corn, sweet, forage	1.5
Corn, sweet, kernels plus cob with husks removed ...	0.30
Corn, sweet, stover	6.0
Cotton, gin byproducts	30
Cottonseed subgroup 20C ...	15
Egg	0.15
Fig, dried	0.15
Fruit, citrus, group 10–10	0.15
Fruit, pome, group 11–10	0.25
Fruit, small, vine climbing, except fuzzy kiwifruit, sub- group 13–07F	0.05
Fruit, stone, group 12–12	0.30
Goat, fat	0.40
Goat, meat	0.15
Goat, meat byproducts	6.0
Grain aspirated fractions	25
Hog, fat	0.40
Hog, meat	0.15
Hog, meat byproducts	6.0
Hop, dried cones	0.9
Horse, fat	0.40
Horse, meat	0.15
Horse, meat byproducts	6.0
Melon subgroup 9A	0.08
Milk	0.15
Nut, tree, group 14–12	0.50
Pepper/eggplant subgroup 8–10B	0.15
Potato, chips	1.6
Potato granules/flakes	2.0
Poultry, fat	0.15
Poultry, meat	0.15
Poultry, meat byproducts	0.60
Rapeseed subgroup 20A	0.4
Rice, grain	1.0

TABLE 1 TO PARAGRAPH (a)(1)—
Continued

Commodity	Parts per million
Rice, hull	2.0
Sheep, fat	0.40
Sheep, meat	0.15
Sheep, meat byproducts	6.0
Soybean	2.0
Soybean, hulls	10
Squash/cucumber subgroup 9B	0.15
Tomato, paste	0.15
Tomato subgroup 8–10A	0.1
Tropical and subtropical, me- dium to large fruit, edible peel, subgroup 23B	0.1
Tropical and subtropical, me- dium to large fruit, smooth, inedible peel, subgroup 24B	0.2
Tropical and subtropical, small fruit, edible peel, subgroup 23A	0.5
Tropical and subtropical, small fruit, inedible peel, subgroup 24A	0.1
Vegetable, tuberous and corn, subgroup 1C	0.8

(2) Tolerances are established for residues of glufosinate-P, including its metabolites and degradates, in or on the commodities in table 2 to paragraph (a)(2), as a result of applications of glufosinate-P or glufosinate-P-ammonium to those commodities. Compliance with the tolerance levels specified in table 2 to paragraph (a)(2) is to be determined by measuring the sum of glufosinate (2-amino-4-(hydroxymethylphosphinyl) butanoic acid) and its metabolites, 2-(acetylamino)-4-(hydroxymethyl phosphinyl) butanoic acid, and 3-(hydroxymethylphosphinyl) propanoic acid, expressed as 2-amino-4-(hydroxymethylphosphinyl)butanoic acid equivalents.

TABLE 2 TO PARAGRAPH (a)(2)

Commodity	Parts per million
Canola, meal	1.1
Cattle, fat	0.4
Cattle, meat	0.15
Cattle, meat byproducts	6
Corn, field, forage	4
Corn, field, grain	0.2
Corn, field, stover	6
Corn, sweet, forage	1.5
Corn, sweet, kernels plus cob with husks removed ...	0.3
Corn, sweet, stover	6
Cotton, gin byproducts	30
Cottonseed, subgroup 20C ..	15
Egg	0.15
Goat, fat	0.4
Goat, meat	0.15
Goat, meat byproducts	6
Grain, aspirated fractions	25

TABLE 2 TO PARAGRAPH (a)(2)—
Continued

Commodity	Parts per million
Hog, fat	0.4
Hog, meat	0.15
Hog, meat byproducts	6
Horse, fat	0.4
Horse, meat	0.15
Horse, meat byproducts	6
Milk	0.15
Poultry, fat	0.15
Poultry, meat	0.15
Poultry, meat byproducts	0.6
Rapeseed, subgroup 20A	0.4
Sheep, fat	0.4
Sheep, meat	0.15
Sheep, meat byproducts	6
Soybean	2
Soybean, hulls	10

(b) [Reserved]

(c) *Tolerances with regional registrations.* Tolerances with regional registrations are established for residues of glufosinate, including its metabolites and degradates, in or on the commodities in table 3 to paragraph (c). Compliance with the tolerance levels specified in table 3 to paragraph (c) is to be determined by measuring the sum of glufosinate, (2-amino-4-(hydroxymethylphosphinyl)butanoic acid) and its metabolites, 2-(acetylamino)-4-(hydroxymethyl phosphinyl) butanoic acid, and 3-(hydroxymethylphosphinyl) propanoic acid, expressed as 2-amino-4-(hydroxymethylphosphinyl)butanoic acid equivalents.

TABLE 3 TO PARAGRAPH (c)

Commodity	Parts per million
Grass, forage	0.15
Grass, hay	0.2

(d) *Indirect or inadvertent residues.*

(1) Tolerances are established for indirect or inadvertent residues of glufosinate, including its metabolites and degradates, in or on the commodities in table 4 to paragraph (d)(1), as a result of the application of glufosinate to crops listed in paragraph (a) of this section. Compliance with the tolerance levels specified in table 4 to paragraph (d)(1) is to be determined by measuring the sum of glufosinate (2-amino-4-(hydroxymethylphosphinyl) butanoic acid) and its metabolite, 3-(hydroxymethylphosphinyl) propanoic acid, expressed as 2-amino-4-(hydroxymethylphosphinyl)butanoic acid equivalents.

TABLE 4 TO PARAGRAPH (d)(1)

Commodity	Parts per million
Barley, hay	0.40
Barley, straw	0.40
Buckwheat, fodder	0.40
Buckwheat, forage	0.40
Oat, forage	0.40
Oat, hay	0.40
Oat, straw	0.40
Rye, forage	0.40
Rye, straw	0.40
Teosinte	0.40
Triticale	0.40
Wheat, forage	0.40
Wheat, hay	0.40
Wheat, straw	0.40

(2) Tolerances are established for indirect or inadvertent residues of glufosinate-P, including its metabolites and degradates, in or on the commodities in table 5 to paragraph (d)(2), as a result of the application of glufosinate-P or glufosinate-P-ammonium to crops listed in paragraph (a)(2) of this section. Compliance with the tolerance levels specified in table 5 to paragraph (d)(2) is to be determined by measuring the sum of glufosinate (2-amino-4-(hydroxymethylphosphinyl)butanoic acid) and its metabolite, 3-(hydroxymethylphosphinyl) propanoic acid, expressed as 2-amino-4-(hydroxymethylphosphinyl)butanoic acid equivalents.”

TABLE 5 TO PARAGRAPH (d)(2)

Commodity	Parts per million
Barley, hay	0.4
Barley, straw	0.4
Buckwheat, fodder	0.4
Buckwheat, forage	0.4
Oat, forage	0.4
Oat, hay	0.4
Oat, straw	0.4
Rye, forage	0.4
Rye, straw	0.4
Teosinte	0.4
Triticale	0.4
Wheat, forage	0.4
Wheat, hay	0.4
Wheat, straw	0.4

[FR Doc. 2024–24831 Filed 10–28–24; 8:45 am]

BILLING CODE 6560–50–P

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

45 CFR Part 2584

RIN 3045–AA60

Protection of Human Subjects

AGENCY: Corporation for National and Community Service.

ACTION: Final rule.

SUMMARY: The Corporation for National and Community Service (operating as AmeriCorps) is finalizing its adoption of the Federal Policy for Protection of Human Subjects (referred to as the Common Rule). The Common Rule outlines the basic ethical principles and procedures that an agency will abide by when conducting or sponsoring research involving human subjects. Among the procedures required by the Common Rule are use of institutional review boards (IRBs), obtaining informed consent of research subjects, and requiring submission of assurances of compliance with the rule. AmeriCorps is making the Common Rule applicable to itself, meaning that all research involving human subjects conducted, supported, or otherwise subject to regulation by AmeriCorps will be subject to the Common Rule’s ethical principles and procedures.

DATES: This rule is effective on November 29, 2024.

FOR FURTHER INFORMATION CONTACT:

Mary Hyde, Ph.D., Director, AmeriCorps Office of Research and Evaluation, at (202) 606–6834 or mhyde@americorps.gov.

SUPPLEMENTARY INFORMATION:

- I. Background
- II. This Final Rule
- III. Comments on and Finalization of the Proposed Rule
- IV. Regulatory Analyses
 - A. Executive Orders 12866 and 13563
 - B. Regulatory Flexibility Act
 - C. Unfunded Mandates Reform Act of 1995
 - D. Paperwork Reduction Act
 - E. Federalism (E.O. 13132)
 - F. Takings (E.O. 12630)
 - G. Civil Justice Reform (E.O. 12988)
 - H. Consultation With Indian Tribes (E.O. 13175)

I. Background

On June 18, 1991, the U.S. Department of Health and Human Services (HHS) issued a rule setting forth the Common Rule requirements for the protection of human subjects. (56 FR 28003). The HHS regulations are codified at 45 CFR part 46. At that time, 15 other agencies joined HHS in adopting a uniform set of rules for the protection of human subjects, identical to subpart A of 45 CFR part 46. The basic provisions of the Common Rule include, among other things, requirements related to the review of human subjects research by an IRB, obtaining and documenting informed consent of human subjects, and submitting written assurance of institutional compliance with the Common Rule. On January 19, 2017 (82

FR 7149), HHS issued a final rule revising the Common Rule, which, among other things, established new requirements regarding the information that must be given to prospective research subjects as part of the informed consent process.

At the time the Common Rule was first adopted in 1991, AmeriCorps had just been established as the Corporation for National and Community Service under the National and Community Service Act of 1990. AmeriCorps was not a participating agency in either that 1991 Common Rule rulemaking or in the subsequent amendments to the Common Rule; however, AmeriCorps believes it is important to adopt this standard framework for AmeriCorps research professionals, prospective and participating human subjects, and consistency among Federal agencies, as described above. This final rule provides the incentives of a mandatory procedural framework and provides human research subjects the assurance of protection offered by the Common Rule.

II. Final Rule

AmeriCorps is codifying the text of the revised Common Rule in its regulations at 45 CFR part 2584 (the proposed rule projected its placement at 45 CFR part 2558, but AmeriCorps has since determined that part 2584 is more appropriate given a planned improvement of chapter 25’s organization). This rule is substantively identical to the HHS regulations in 45 CFR part 46, subpart A, ensuring consistency across Federal agencies. With this codification, AmeriCorps would be subject to the same ethical principles and procedures that other agencies who have adopted the Common Rule are subject to when conducting or supporting research involving human subjects. The rule applies broadly; most relevant to AmeriCorps, it covers instances when an investigator conducting research obtains information through interaction with the individual and uses, studies, or analyzes the information. The rule also sets out certain research that is exempt from the rule. For any non-exempt research, under this rule AmeriCorps would:

- Conduct or support non-exempt research only if the institution engaged in the research has provided an assurance that it will comply with the Common Rule, and
- Conduct or support non-exempt research only if (when required by the rule) the institution has certified to AmeriCorps that the research has been reviewed and approved by an IRB.

The rule also sets out requirements applicable to the IRBs, including requirements for the IRB membership, IRB functions and operations, IRB review of research and criteria for IRB approval of research, IRB authority to suspend or terminate approval of research that is not being conducted in accordance with the IRB's requirements or has been associated with unexpected serious harm to subjects, and IRB records. The rule also sets out the requirements for investigators to obtain the legally effective informed consent of the subject before involving the subject in any non-exempt research. For example, the investigator must seek informed consent only under circumstances that provide sufficient opportunity to discuss and consider whether to participate in the research (to minimize the possibility of coercion or undue influence), and the investigator must provide the prospective subject with information a reasonable person would want to have in order to make an informed decision as to whether to participate in the research and provide the information in language understandable to the prospective subject. The rule also sets out the basic elements of what information must be provided to each prospective subject and how informed consent must be documented.

AmeriCorps at times undertakes research that would be considered non-exempt research under the Common Rule. The Office of Research and Evaluation (ORE), within AmeriCorps, furthers AmeriCorps' mission by providing accurate and timely research on national service, social innovation, volunteering, and civic engagement. ORE conducts original and sponsored research and evaluations, among other activities, to infuse data into AmeriCorps' programs and contribute to the public's understanding of national service. For example, AmeriCorps surveys members/volunteers to inform recruitment and improve member/volunteer experience. ORE uses the survey responses to identify national service trends, such as trends in program participation, motivations, and outcomes. As another example, AmeriCorps sponsors evaluations of national service interventions (*e.g.*, Recovery Coach Programs, Tutoring Programs) that collect information from program participants about their experiences and outcomes.

ORE staff consists of professional social scientists and research analysts who abide by their professions' codes of ethics, including but not limited to those relating to integrity, respect for people's rights, dignity, and diversity,

non-exploitation, and informed consent. AmeriCorps' research is therefore already guided by these codes of ethics, and the agency typically engages in practices such as ensuring that informed consent of human subjects is properly obtained and, when supporting research is conducted by universities and other research partners, ensuring that the research is reviewed and approved by an IRB.

Issuance of this rule will not result in major changes in research conducted and supported by AmeriCorps, but it will provide a more concrete framework for AmeriCorps staff to follow to ensure protection of human research subjects. While AmeriCorps may currently avail itself of the broad range of HHS guidance documents on the Common Rule, adopting the Common Rule itself will ensure that it is interpreting those guidance documents in a manner consistent with the regulatory requirements of the Common Rule. HHS guidance includes decisions charts to guide everything from the analysis of whether an activity is covered by the Common Rule to whether documentation of informed consent can be waived, frequently asked question (FAQ) documents, and various other guidance documents—all of which will assist AmeriCorps in ensuring that its research protects human subjects. AmeriCorps' adoption of the Common Rule also provides assurance to individuals who are prospective and participating human research subjects for AmeriCorps-conducted or supported research that AmeriCorps abides by the same ethical and procedural provisions that HHS and 19 other agencies do. Finally, AmeriCorps' adoption of the Common Rule will ensure consistency across agencies in their approach to protecting human subjects in research.

III. Comments on and Finalization of the Proposed Rule

AmeriCorps proposed adoption of the Common Rule on September 20, 2022, at 87 FR 57435 and invited public comment on the advisability or inadvisability of adopting the Common Rule in whole or in part. In response, AmeriCorps received seven public comments on the proposed rule, all of which expressed support for the rule. Several noted that the rule would provide a more standardized way of conducting ethical research to protect subjects from harm, following the same processes as the other Federal agencies that have adopted the common rule. Several also specifically expressed support for the requirement for informed consent. Several also specifically expressed support for IRB

review. AmeriCorps has reviewed these comments and determined that it is appropriate to finalize the proposed rule without change, with one exception. The Agency is removing the provisions that transition research projects from the pre-2018 requirements to current requirements because the Agency has no pre-2018 requirements to transition away from. AmeriCorps is publishing this final rule after a delay of over a year because the Agency first finalized internal guidance to ensure compliance with the Common Rule before finalizing it.

IV. Regulatory Analyses

A. Executive Orders 12866 and 13563

Executive Orders (E.O.) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. The Office of Information and Regulatory Affairs in the Office of Management and Budget has determined that this is not a significant regulatory action and, therefore, was not subject to review under section 6(b) of E.O. 12866.

B. Regulatory Flexibility Act

As required by the Regulatory Flexibility Act of 1980 (5 U.S.C. 601 *et seq.*), AmeriCorps certifies that this rule does not have a significant economic impact on a substantial number of small entities. Therefore, AmeriCorps has not performed the initial regulatory flexibility analysis that is required under the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*) for rules that are expected to have such results.

C. Unfunded Mandates Reform Act of 1995

For purposes of Title II of the Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1531–1538, as well as Executive Order 12875, this regulatory action does not contain any Federal mandate that may result in increased expenditures in either Federal, State, local, or Tribal governments in the aggregate, or impose an annual burden exceeding \$100 million on the private sector.

D. Paperwork Reduction Act

Under the PRA, an agency may not conduct or sponsor a collection of

information unless the collections of information display valid control numbers. The information collections in this rule at sections 2584.103, 2584.104, 2584.108, 2584.109, 2584.113, and 2584.115–2584.17 are approved by the Office of Management and Budget under Control Number 0990–0260.

E. Federalism (E.O. 13132)

Executive Order 13132, Federalism, prohibits an agency from publishing any rule that has federalism implications if the rule imposes substantial direct compliance costs on State and local governments and is not required by statute, or the rule preempts State law, unless the agency meets the consultation and funding requirements of section 6 of the Executive Order. This rule does not have any federalism implications, as described above.

F. Takings (E.O. 12630)

This rule does not affect a taking of private property or otherwise have taking implications under Executive Order 12630 because this rule does not affect individual property rights protected by the Fifth Amendment or involve a compensable “taking.” A takings implication assessment is not required.

G. Civil Justice Reform (E.O. 12988)

This rule complies with the requirements of Executive Order 12988. Specifically, this rule: (a) meets the criteria of section 3(a) requiring that all regulations be reviewed to eliminate errors and ambiguity and be written to minimize litigation; and (b) meets the criteria of section 3(b)(2) requiring that all regulations be written in clear language and contain clear legal standards.

H. Consultation With Indian Tribes (E.O. 13175)

AmeriCorps recognizes the inherent sovereignty of Indian Tribes and their right to self-governance. We have evaluated this rule under our consultation policy and the criteria in E.O. 13175 and determined that this rule does not impose substantial direct effects on federally recognized Tribes.

List of Subjects in 45 CFR Part 2584

Human research subjects, Reporting and recordkeeping requirements, Research.

■ For the reasons stated in the preamble, the Corporation for National and Community Service amends title 45 of the Code of Federal Regulations by adding part 2584 to read as follows:

PART 2584—PROTECTION OF HUMAN SUBJECTS

Sec.

- 2584.101 To what does this part apply?
- 2584.102 Definitions for purposes of this part.
- 2584.103 Assuring compliance with this part—research conducted or supported by any Federal department or agency.
- 2584.104 Exempt research.
- 2584.105–2584.106 [Reserved]
- 2584.107 IRB membership.
- 2584.108 IRB functions and operations.
- 2584.109 IRB review of research.
- 2584.110 Expedited review procedures for certain kinds of research involving no more than minimal risk, and for minor changes in approved research.
- 2584.111 Criteria for IRB approval of research.
- 2584.112 Review by institution.
- 2584.113 Suspension or termination of IRB approval of research.
- 2584.114 Cooperative research.
- 2584.115 IRB records.
- 2584.116 General requirements for informed consent.
- 2584.117 Documentation of informed consent.
- 2584.118 Applications and proposals lacking definite plans for involvement of human subjects.
- 2584.119 Research undertaken without the intention of involving human subjects.
- 2584.120 Evaluation and disposition of applications and proposals for research to be conducted or supported by a Federal department or agency.
- 2584.121 [Reserved]
- 2584.122 Use of Federal funds.
- 2584.123 Early termination of research support: Evaluation of applications and proposals.
- 2584.124 Conditions.

Authority: 42 U.S.C. 12651c(c).

§ 2584.101 To what does this part apply?

(a) Except as detailed in § 2584.104, this part applies to all research involving human subjects conducted, supported, or otherwise subject to regulation by any Federal department or agency that takes appropriate administrative action to make the policy applicable to such research. This includes research conducted by Federal civilian employees or military personnel, except that each department or agency head may adopt such procedural modifications as may be appropriate from an administrative standpoint. It also includes research conducted, supported, or otherwise subject to regulation by the Federal Government outside the United States. Institutions that are engaged in research described in this paragraph and institutional review boards (IRBs) reviewing research that is subject to this policy must comply with this part.

(b) [Reserved]

(c) Department or agency heads retain final judgment as to whether a particular activity is covered by this part and this judgment shall be exercised consistent with the ethical principles of the Belmont Report.¹

(d) Department or agency heads may require that specific research activities or classes of research activities conducted, supported, or otherwise subject to regulation by the Federal department or agency but not otherwise covered by this part comply with some or all of the requirements of this part.

(e) Compliance with this part requires compliance with pertinent Federal laws or regulations that provide additional protections for human subjects.

(f) This part does not affect any state or local laws or regulations (including Tribal law passed by the official governing body of an American Indian or Alaska Native Tribe) that may otherwise be applicable and that provide additional protections for human subjects.

(g) This part does not affect any foreign laws or regulations that may otherwise be applicable and that provide additional protections to human subjects of research.

(h) When research covered by this part takes place in foreign countries, procedures normally followed in the foreign countries to protect human subjects may differ from those set forth in this part. In these circumstances, if a department or agency head determines that the procedures prescribed by the institution afford protections that are at least equivalent to those provided in this part, the department or agency head may approve the substitution of the foreign procedures in lieu of the procedural requirements provided in this part. Except when otherwise required by statute, Executive order, or the department or agency head, notices of these actions as they occur will be published in the **Federal Register** or will be otherwise published as provided in department or agency procedures.

(i) Unless otherwise required by law, the department or agency head may waive the applicability of some or all of the provisions of this part to specific research activities or classes of research activities otherwise covered by this part, provided the alternative procedures to be followed are consistent with the principles of the Belmont Report.² Except when otherwise required by statute or Executive Order, the

¹ The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research* (Apr. 18, 1979).

² Id.

department or agency head shall forward advance notices of these actions to the Office for Human Research Protections, Department of Health and Human Services (HHS), or any successor office, or to the equivalent office within the appropriate Federal department or agency, and shall also publish them in the **Federal Register** or in such other manner as provided in department or agency procedures. The waiver notice must include a statement that identifies the conditions under which the waiver will be applied and a justification as to why the waiver is appropriate for the research, including how the decision is consistent with the principles of the Belmont Report.

(j) Federal guidance on the requirements of this part shall be issued only after consultation, for the purpose of harmonization (to the extent appropriate), with other Federal departments and agencies that have adopted this policy, unless such consultation is not feasible.

(k)–(l) [Reserved]

(m) **Severability:** Any provision of this part held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, shall be construed so as to continue to give maximum effect to the provision permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which event the provision shall be severable from this part and shall not affect the remainder thereof or the application of the provision to other persons not similarly situated or to other dissimilar circumstances.

§ 2584.102 Definitions for purposes of this part.

Certification means the official notification by the institution to the supporting Federal department or agency component, in accordance with the requirements of this part, that a research project or activity involving human subjects has been reviewed and approved by an IRB in accordance with an approved assurance.

Clinical trial means research study in which one or more human subjects are prospectively assigned to one or more interventions (which may include placebo or other control) to evaluate the effects of the interventions on biomedical or behavioral health-related outcomes.

Department or agency head means the head of any Federal department or agency, for example, the Secretary of HHS, and any other officer or employee of any Federal department or agency to whom the authority provided by these regulations to the department or agency head has been delegated.

Federal department or agency refers to a Federal department or agency (the department or agency itself rather than its bureaus, offices or divisions) that takes appropriate administrative action to make this part applicable to the research involving human subjects it conducts, supports, or otherwise regulates (e.g., the U.S. Department of Health and Human Services, the U.S. Department of Defense, or the Central Intelligence Agency).

Human subject means:

(1) A living individual about whom an investigator (whether professional or student) conducting research:

(i) Obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or

(ii) Obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

(2) Intervention includes both physical procedures by which information or biospecimens are gathered (e.g., venipuncture) and manipulations of the subject or the subject's environment that are performed for research purposes.

(3) Interaction includes communication or interpersonal contact between investigator and subject.

(4) Private information includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (e.g., a medical record).

(5) Identifiable private information is private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.

(6) An identifiable biospecimen is a biospecimen for which the identity of the subject is or may readily be ascertained by the investigator or associated with the biospecimen.

(7) Federal departments or agencies implementing this policy shall:

(i) Upon consultation with appropriate experts (including experts in data matching and re-identification), reexamine the meaning of “identifiable private information,” as defined in paragraph (5) of this definition, and “identifiable biospecimen,” as defined in paragraph (6) of this definition. This reexamination shall take place within 1 year and regularly thereafter (at least every 4 years). This process will be conducted by collaboration among the

Federal departments and agencies implementing this policy. If appropriate and permitted by law, such Federal departments and agencies may alter the interpretation of these terms, including through the use of guidance.

(ii) Upon consultation with appropriate experts, assess whether there are analytic technologies or techniques that should be considered by investigators to generate “identifiable private information,” as defined in paragraph (5) of this definition, or an “identifiable biospecimen,” as defined in paragraph (6) of this definition. This assessment shall take place within 1 year and regularly thereafter (at least every 4 years). This process will be conducted by collaboration among the Federal departments and agencies implementing this policy. Any such technologies or techniques will be included on a list of technologies or techniques that produce identifiable private information or identifiable biospecimens. This list will be published in the **Federal Register** after notice and an opportunity for public comment. The Secretary, HHS, shall maintain the list on a publicly accessible website.

(f) **Institution** means any public or private entity, or department or agency (including Federal, state, and other agencies).

(g) **IRB** means an institutional review board established in accord with and for the purposes expressed in this part.

(h) **IRB approval** means the determination of the IRB that the research has been reviewed and may be conducted at an institution within the constraints set forth by the IRB and by other institutional and Federal requirements.

(i) **Legally authorized representative** means an individual or judicial or other body authorized under applicable law to consent on behalf of a prospective subject to the subject's participation in the procedure(s) involved in the research. If there is no applicable law addressing this issue, legally authorized representative means an individual recognized by institutional policy as acceptable for providing consent in the nonresearch context on behalf of the prospective subject to the subject's participation in the procedure(s) involved in the research.

(j) **Minimal risk** means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.

(k) *Public health authority* means an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, an Indian Tribe, or a foreign government, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

(l) *Research* means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research for purposes of this part, whether or not they are conducted or supported under a program that is considered research for other purposes. For example, some demonstration and service programs may include research activities. For purposes of this part, the following activities are deemed not to be research:

(1) Scholarly and journalistic activities (e.g., oral history, journalism, biography, literary criticism, legal research, and historical scholarship), including the collection and use of information, that focus directly on the specific individuals about whom the information is collected.

(2) Public health surveillance activities, including the collection and testing of information or biospecimens, conducted, supported, requested, ordered, required, or authorized by a public health authority. Such activities are limited to those necessary to allow a public health authority to identify, monitor, assess, or investigate potential public health signals, onsets of disease outbreaks, or conditions of public health importance (including trends, signals, risk factors, patterns in diseases, or increases in injuries from using consumer products). Such activities include those associated with providing timely situational awareness and priority setting during the course of an event or crisis that threatens public health (including natural or man-made disasters).

(3) Collection and analysis of information, biospecimens, or records by or for a criminal justice agency for activities authorized by law or court order solely for criminal justice or criminal investigative purposes.

(4) Authorized operational activities (as determined by each agency) in support of intelligence, homeland security, defense, or other national security missions.

(m) *Written*, or *in writing*, for purposes of this part, refers to writing on a tangible medium (e.g., paper) or in an electronic format.

§ 2558.103 Assuring compliance with this part—research conducted or supported by any Federal department or agency.

(a) Each institution engaged in research that is covered by this part, with the exception of research eligible for exemption under § 2584.104, and that is conducted or supported by a Federal department or agency, shall provide written assurance satisfactory to the department or agency head that it will comply with the requirements of this part. In lieu of requiring submission of an assurance, the department or agency head shall accept the existence of a current assurance, appropriate for the research in question, on file with the Office for Human Research Protections, HHS, or any successor office, and approved for Federal-wide use by that office. When the existence of an HHS-approved assurance is accepted in lieu of requiring submission of an assurance, reports (except certification) required by this part to be made to department and agency heads shall also be made to the Office for Human Research Protections, HHS, or any successor office. Federal departments and agencies will conduct or support research covered by this policy only if the institution has provided an assurance that it will comply with the requirements of this part, as provided in this section, and only if the institution has certified to the department or agency head that the research has been reviewed and approved by an IRB (if such certification is required by paragraph (d) of this section).

(b) The assurance shall be executed by an individual authorized to act for the institution and to assume on behalf of the institution the obligations imposed by this part and shall be filed in such form and manner as the department or agency head prescribes.

(c) The department or agency head may limit the period during which any assurance shall remain effective or otherwise condition or restrict the assurance.

(d) Certification is required when the research is supported by a Federal department or agency and not otherwise waived under § 2584.101(i) or exempted under § 2584.104. For such research, institutions shall certify that each proposed research study covered by the assurance and this section has been reviewed and approved by the IRB. Such certification must be submitted as prescribed by the Federal department or agency component supporting the

research. Under no condition shall research covered by this section be initiated prior to receipt of the certification that the research has been reviewed and approved by the IRB.

(e) For nonexempt research involving human subjects covered by this part (or exempt research for which limited IRB review takes place pursuant to § 2584.104(d)(2)(iii), (d)(3)(i)(C), or (d)(7) or (8)) that takes place at an institution in which IRB oversight is conducted by an IRB that is not operated by the institution, the institution and the organization operating the IRB shall document the institution's reliance on the IRB for oversight of the research and the responsibilities that each entity will undertake to ensure compliance with the requirements of this part (e.g., in a written agreement between the institution and the IRB, by implementation of an institution-wide policy directive providing the allocation of responsibilities between the institution and an IRB that is not affiliated with the institution, or as set forth in a research protocol).

§ 2584.104 Exempt research.

(a) Unless otherwise required by law or by the department or agency head, research activities in which the only involvement of human subjects will be in one or more of the categories in paragraph (d) of this section are exempt from the requirements of this part, except that such activities must comply with the requirements of this section and as specified in each category.

(b) Use of the exemption categories for research subject to the requirements of 45 CFR part 46, subparts B, C, and D. Application of the exemption categories to research subject to the requirements of subparts B, C, and D, is as follows:

(1) *Subpart B.* Each of the exemptions at this section may be applied to research subject to 45 CFR part 46, subpart B, if the conditions of the exemption are met.

(2) *Subpart C.* The exemptions at this section do not apply to research subject to 45 CFR part 46, subpart C, except for research aimed at involving a broader subject population that only incidentally includes prisoners.

(3) *Subpart D.* The exemptions at paragraphs (d)(1), (4), (5), (6), (7), and (8) of this section may be applied to research subject to 45 CFR part 46, subpart D, if the conditions of the exemption are met. Paragraphs (d)(2)(i) and (ii) of this section only may apply to research subject to subpart D involving educational tests or the observation of public behavior when the investigator(s) do not participate in the

activities being observed. Paragraph (d)(2)(iii) of this section may not be applied to research subject to subpart D.

(c) [Reserved]

(d) Except as described in paragraph (a) of this section, the following categories of human subjects research are exempt from this part:

(1) Research, conducted in established or commonly accepted educational settings, that specifically involves normal educational practices that are not likely to adversely impact students' opportunity to learn required educational content or the assessment of educators who provide instruction. This includes most research on regular and special education instructional strategies, and research on the effectiveness of or the comparison among instructional techniques, curricula, or classroom management methods.

(2) Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) if at least one of the following criteria is met:

(i) The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects;

(ii) Any disclosure of the human subjects' responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation; or

(iii) The information obtained is recorded by the investigator in such a manner that the identity of the human subjects can readily be ascertained, directly or through identifiers linked to the subjects, and an IRB conducts a limited IRB review to make the determination required by § 2584.111(a)(7).

(3)(i) Research involving benign behavioral interventions in conjunction with the collection of information from an adult subject through verbal or written responses (including data entry) or audiovisual recording if the subject prospectively agrees to the intervention and information collection and at least one of the following criteria is met:

(A) The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects;

(B) Any disclosure of the human subjects' responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation; or

(C) The information obtained is recorded by the investigator in such a manner that the identity of the human subjects can readily be ascertained, directly or through identifiers linked to the subjects, and an IRB conducts a limited IRB review to make the determination required by § 2584.111(a)(7).

(ii) For the purpose of this provision, benign behavioral interventions are brief in duration, harmless, painless, not physically invasive, not likely to have a significant adverse lasting impact on the subjects, and the investigator has no reason to think the subjects will find the interventions offensive or embarrassing. Provided all such criteria are met, examples of such benign behavioral interventions would include having the subjects play an online game, having them solve puzzles under various noise conditions, or having them decide how to allocate a nominal amount of received cash between themselves and someone else.

(iii) If the research involves deceiving the subjects regarding the nature or purposes of the research, this exemption is not applicable unless the subject authorizes the deception through a prospective agreement to participate in research in circumstances in which the subject is informed that he or she will be unaware of or misled regarding the nature or purposes of the research.

(4) Secondary research for which consent is not required: Secondary research uses of identifiable private information or identifiable biospecimens, if at least one of the following criteria is met:

(i) The identifiable private information or identifiable biospecimens are publicly available;

(ii) Information, which may include information about biospecimens, is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained directly or through identifiers linked to the subjects, the investigator does not contact the subjects, and the investigator will not re-identify subjects;

(iii) The research involves only information collection and analysis involving the investigator's use of identifiable health information when that use is regulated under 45 CFR part 160 and part 164, subparts A and E, for the purposes of "health care operations" or "research" as those terms are defined

at 45 CFR 164.501 or for "public health activities and purposes" as described under 45 CFR 164.512(b); or

(iv) The research is conducted by, or on behalf of, a Federal department or agency using government-generated or government-collected information obtained for nonresearch activities, if the research generates identifiable private information that is or will be maintained on information technology that is subject to and in compliance with section 208(b) of the E-Government Act of 2002, 44 U.S.C. 3501 note, if all of the identifiable private information collected, used, or generated as part of the activity will be maintained in systems of records subject to the Privacy Act of 1974, 5 U.S.C. 552a, and, if applicable, the information used in the research was collected subject to the Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq.*

(5) Research and demonstration projects that are conducted or supported by a Federal department or agency, or otherwise subject to the approval of the department or agency head (or the approval of the heads of bureaus or other subordinate agencies that have been delegated authority to conduct the research and demonstration projects), and that are designed to study, evaluate, improve, or otherwise examine public benefit or service programs, including procedures for obtaining benefits or services under those programs, possible changes in or alternatives to those programs or procedures, or possible changes in methods or levels of payment for benefits or services under those programs. Such projects include, but are not limited to, internal studies by Federal employees, and studies under contracts or consulting arrangements, cooperative agreements, or grants. Exempt projects also include waivers of otherwise mandatory requirements using authorities such as sections 1115 and 1115A of the Social Security Act, as amended.

(i) Each Federal department or agency conducting or supporting the research and demonstration projects must establish, on a publicly accessible Federal website or in such other manner as the department or agency head may determine, a list of the research and demonstration projects that the Federal department or agency conducts or supports under this provision. The research or demonstration project must be published on this list prior to commencing the research involving human subjects.

(ii) [Reserved]

(6) Taste and food quality evaluation and consumer acceptance studies:

(i) If wholesome foods without additives are consumed, or

(ii) If a food is consumed that contains a food ingredient at or below the level and for a use found to be safe, or agricultural chemical or environmental contaminant at or below the level found to be safe, by the Food and Drug Administration or approved by the Environmental Protection Agency or the Food Safety and Inspection Service of the U.S. Department of Agriculture.

(7) Storage or maintenance for secondary research for which broad consent is required: Storage or maintenance of identifiable private information or identifiable biospecimens for potential secondary research use if an IRB conducts a limited IRB review and makes the determinations required by § 2584.111(a)(8).

(8) Secondary research for which broad consent is required: Research involving the use of identifiable private information or identifiable biospecimens for secondary research use, if the following criteria are met:

(i) Broad consent for the storage, maintenance, and secondary research use of the identifiable private information or identifiable biospecimens was obtained in accordance with § 2584.116(a)(1) through (4) and (6) and (d);

(ii) Documentation of informed consent or waiver of documentation of consent was obtained in accordance with § 2584.117;

(iii) An IRB conducts a limited IRB review and makes the determination required by § 2584.111(a)(7) and makes the determination that the research to be conducted is within the scope of the broad consent referenced in paragraph (d)(8)(i) of this section; and

(iv) The investigator does not include returning individual research results to subjects as part of the study plan. This provision does not prevent an investigator from abiding by any legal requirements to return individual research results.

§§ 2584.105–2584.106 [Reserved]

§ 2584.107 IRB membership.

(a) Each IRB shall have at least five members, with varying backgrounds to promote complete and adequate review of research activities commonly conducted by the institution. The IRB shall be sufficiently qualified through the experience and expertise of its members (professional competence), and the diversity of its members, including race, gender, and cultural backgrounds and sensitivity to such issues as community attitudes, to

promote respect for its advice and counsel in safeguarding the rights and welfare of human subjects. The IRB shall be able to ascertain the acceptability of proposed research in terms of institutional commitments (including policies and resources) and regulations, applicable law, and standards of professional conduct and practice. The IRB shall therefore include persons knowledgeable in these areas. If an IRB regularly reviews research that involves a category of subjects that is vulnerable to coercion or undue influence, such as children, prisoners, individuals with impaired decision-making capacity, or economically or educationally disadvantaged persons, consideration shall be given to the inclusion of one or more individuals who are knowledgeable about and experienced in working with these categories of subjects.

(b) Each IRB shall include at least one member whose primary concerns are in scientific areas and at least one member whose primary concerns are in nonscientific areas.

(c) Each IRB shall include at least one member who is not otherwise affiliated with the institution and who is not part of the immediate family of a person who is affiliated with the institution.

(d) No IRB may have a member participate in the IRB's initial or continuing review of any project in which the member has a conflicting interest, except to provide information requested by the IRB.

(e) An IRB may, in its discretion, invite individuals with competence in special areas to assist in the review of issues that require expertise beyond or in addition to that available on the IRB. These individuals may not vote with the IRB.

§ 2584.108 IRB functions and operations.

(a) In order to fulfill the requirements of this part each IRB shall:

(1) Have access to meeting space and sufficient staff to support the IRB's review and recordkeeping duties;

(2) Prepare and maintain a current list of the IRB members identified by name; earned degrees; representative capacity; indications of experience such as board certifications or licenses sufficient to describe each member's chief anticipated contributions to IRB deliberations; and any employment or other relationship between each member and the institution, for example, full-time employee, part-time employee, member of governing panel or board, stockholder, paid or unpaid consultant;

(3) Establish and follow written procedures for:

(i) Conducting its initial and continuing review of research and for reporting its findings and actions to the investigator and the institution;

(ii) Determining which projects require review more often than annually and which projects need verification from sources other than the investigators that no material changes have occurred since previous IRB review; and

(iii) Ensuring prompt reporting to the IRB of proposed changes in a research activity, and for ensuring that investigators will conduct the research activity in accordance with the terms of the IRB approval until any proposed changes have been reviewed and approved by the IRB, except when necessary to eliminate apparent immediate hazards to the subject.

(4) Established and follow written procedures for ensuring prompt reporting to the IRB; appropriate institutional officials; the department or agency head; and the Office for Human Research Protections, HHS, or any successor office, or the equivalent office within the appropriate Federal department or agency of

(i) Any unanticipated problems involving risks to subjects or others or any serious or continuing noncompliance with this part or the requirements or determinations of the IRB; and

(ii) Any suspension or termination of IRB approval

(b) Except when an expedited review procedure is used (as described in § 2584.110), an IRB must review proposed research at convened meetings at which a majority of the members of the IRB are present, including at least one member whose primary concerns are in nonscientific areas. In order for the research to be approved, it shall receive the approval of a majority of those members present at the meeting.

§ 2584.109 IRB review of research.

(a) An IRB shall review and have authority to approve, require modifications in (to secure approval), or disapprove all research activities covered by this part, including exempt research activities under § 2584.104 for which limited IRB review is a condition of exemption (under § 2584.104(d)(2)(iii), (d)(3)(i)(C), and (d)(7) and (8)).

(b) An IRB shall require that information given to subjects (or legally authorized representatives, when appropriate) as part of informed consent is in accordance with § 2584.116. The IRB may require that information, in addition to that specifically mentioned in § 2584.116, be given to the subjects

when in the IRB's judgment the information would meaningfully add to the protection of the rights and welfare of subjects.

(c) An IRB shall require documentation of informed consent or may waive documentation in accordance with § 2584.117.

(d) An IRB shall notify investigators and the institution in writing of its decision to approve or disapprove the proposed research activity, or of modifications required to secure IRB approval of the research activity. If the IRB decides to disapprove a research activity, it shall include in its written notification a statement of the reasons for its decision and give the investigator an opportunity to respond in person or in writing.

(e) An IRB shall conduct continuing review of research requiring review by the convened IRB at intervals appropriate to the degree of risk, not less than once per year, except as described in paragraph (f) of this section.

(f)(1) Unless an IRB determines otherwise, continuing review of research is not required in the following circumstances:

(i) Research eligible for expedited review in accordance with § 2584.110;

(ii) Research reviewed by the IRB in accordance with the limited IRB review described in § 2584.104(d)(2)(iii), (d)(3)(i)(C), or (d)(7) or (8);

(iii) Research that has progressed to the point that it involves only one or both of the following, which are part of the IRB-approved study:

(A) Data analysis, including analysis of identifiable private information or identifiable biospecimens, or

(B) Accessing follow-up clinical data from procedures that subjects would undergo as part of clinical care.

(2) [Reserved]

(g) An IRB shall have authority to observe or have a third party observe the consent process and the research.

§ 2584.110 Expedited review procedures for certain kinds of research involving no more than minimal risk, and for minor changes in approved research.

(a) The Secretary of HHS has established, and published as a notice in the **Federal Register**, a list of categories of research that may be reviewed by the IRB through an expedited review procedure. The Secretary will evaluate the list at least every 8 years and amend it, as appropriate, after consultation with other Federal departments and agencies and after publication in the **Federal Register** for public comment. A copy of the list is available from the Office for Human Research Protections, HHS, or any successor office.

(b)(1) An IRB may use the expedited review procedure to review the following:

(i) Some or all of the research appearing on the list described in paragraph (a) of this section, unless the reviewer determines that the study involves more than minimal risk;

(ii) Minor changes in previously approved research during the period for which approval is authorized; or

(iii) Research for which limited IRB review is a condition of exemption under § 2584.104(d)(2)(iii), (d)(3)(i)(C), and (d)(7) and (8)

(2) Under an expedited review procedure, the review may be carried out by the IRB chairperson or by one or more experienced reviewers designated by the chairperson from among members of the IRB. In reviewing the research, the reviewers may exercise all of the authorities of the IRB except that the reviewers may not disapprove the research. A research activity may be disapproved only after review in accordance with the non-expedited procedure set forth in § 2584.108(b).

(c) Each IRB that uses an expedited review procedure shall adopt a method for keeping all members advised of research proposals that have been approved under the procedure.

(d) The department or agency head may restrict, suspend, terminate, or choose not to authorize an institution's or IRB's use of the expedited review procedure.

§ 2258.111 Criteria for IRB approval of research.

(a) In order to approve research covered by this part the IRB shall determine that all of the following requirements are satisfied:

(1) Risks to subjects are minimized:

(i) By using procedures that are consistent with sound research design and that do not unnecessarily expose subjects to risk, and

(ii) Whenever appropriate, by using procedures already being performed on the subjects for diagnostic or treatment purposes.

(2) Risks to subjects are reasonable in relation to anticipated benefits, if any, to subjects, and the importance of the knowledge that may reasonably be expected to result. In evaluating risks and benefits, the IRB should consider only those risks and benefits that may result from the research (as distinguished from risks and benefits of therapies subjects would receive even if not participating in the research). The IRB should not consider possible long-range effects of applying knowledge gained in the research (e.g., the possible effects of the research on public policy)

as among those research risks that fall within the purview of its responsibility.

(3) Selection of subjects is equitable.

In making this assessment the IRB should take into account the purposes of the research and the setting in which the research will be conducted. The IRB should be particularly cognizant of the special problems of research that involves a category of subjects who are vulnerable to coercion or undue influence, such as children, prisoners, individuals with impaired decision-making capacity, or economically or educationally disadvantaged persons.

(4) Informed consent will be sought from each prospective subject or the subject's legally authorized representative, in accordance with, and to the extent required by, § 2584.116.

(5) Informed consent will be appropriately documented or appropriately waived in accordance with § 2584.117.

(6) When appropriate, the research plan makes adequate provision for monitoring the data collected to ensure the safety of subjects.

(7) When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

(i) The Secretary of HHS will, after consultation with the Office of Management and Budget's privacy office and other Federal departments and agencies that have adopted this policy, issue guidance to assist IRBs in assessing what provisions are adequate to protect the privacy of subjects and to maintain the confidentiality of data.

(ii) [Reserved]

(8) For purposes of conducting the limited IRB review required by § 2584.104(d)(7)), the IRB need not make the determinations at paragraphs (a)(1) through (7) of this section, and shall make the following determinations:

(i) Broad consent for storage, maintenance, and secondary research use of identifiable private information or identifiable biospecimens is obtained in accordance with the requirements of § 2584.116(a)(1) through (4) and (6) and (d);

(ii) Broad consent is appropriately documented or waiver of documentation is appropriate, in accordance with § 2584.117; and

(iii) If there is a change made for research purposes in the way the identifiable private information or identifiable biospecimens are stored or maintained, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

(b) When some or all of the subjects are likely to be vulnerable to coercion or

undue influence, such as children, prisoners, individuals with impaired decision-making capacity, or economically or educationally disadvantaged persons, additional safeguards have been included in the study to protect the rights and welfare of these subjects.

§ 2584.112 Review by institution.

Research covered by this part that has been approved by an IRB may be subject to further appropriate review and approval or disapproval by officials of the institution. However, those officials may not approve the research if it has not been approved by an IRB.

§ 2258.113 Suspension or termination of IRB approval of research.

An IRB shall have authority to suspend or terminate approval of research that is not being conducted in accordance with the IRB's requirements or that has been associated with unexpected serious harm to subjects. Any suspension or termination of approval shall include a statement of the reasons for the IRB's action and shall be reported promptly to the investigator, appropriate institutional officials, and the department or agency head.

§ 2584.114 Cooperative research.

(a) Cooperative research projects are those projects covered by this part that involve more than one institution. In the conduct of cooperative research projects, each institution is responsible for safeguarding the rights and welfare of human subjects and for complying with this policy.

(b)(1) Any institution located in the United States that is engaged in cooperative research must rely upon approval by a single IRB for that portion of the research that is conducted in the United States. The reviewing IRB will be identified by the Federal department or agency supporting or conducting the research or proposed by the lead institution subject to the acceptance of the Federal department or agency supporting the research.

(2) The following research is not subject to this provision:

(i) Cooperative research for which more than single IRB review is required by law (including Tribal law passed by the official governing body of an American Indian or Alaska Native Tribe); or

(ii) Research for which any Federal department or agency supporting or conducting the research determines and documents that the use of a single IRB is not appropriate for the particular context.

(c) For research not subject to paragraph (b) of this section, an institution participating in a cooperative project may enter into a joint review arrangement, rely on the review of another IRB, or make similar arrangements for avoiding duplication of effort.

§ 2584.115 IRB records.

(a) An institution, or when appropriate an IRB, shall prepare and maintain adequate documentation of IRB activities, including the following:

(1) Copies of all research proposals reviewed, scientific evaluations, if any, that accompany the proposals, approved sample consent forms, progress reports submitted by investigators, and reports of injuries to subjects.

(2) Minutes of IRB meetings which shall be in sufficient detail to show attendance at the meetings; actions taken by the IRB; the vote on these actions including the number of members voting for, against, and abstaining; the basis for requiring changes in or disapproving research; and a written summary of the discussion of controverted issues and their resolution.

(3) Records of continuing review activities, including the rationale for conducting continuing review of research that otherwise would not require continuing review as described in § 2584.109(f)(1).

(4) Copies of all correspondence between the IRB and the investigators.

(5) A list of IRB members in the same detail as described in § 2584.108(a)(2).

(6) Written procedures for the IRB in the same detail as described in § 2584.108(a)(3) and (4).

(7) Statements of significant new findings provided to subjects, as required by § 2584.116(c)(5).

(8) The rationale for an expedited reviewer's determination under § 2584.110(b)(1)(i) that research appearing on the expedited review list described in § 2584.110(a) is more than minimal risk.

(9) Documentation specifying the responsibilities that an institution and an organization operating an IRB each will undertake to ensure compliance with the requirements of this part, as described in § 2584.103(e).

(b) The records required by this part shall be retained for at least 3 years, and records relating to research that is conducted shall be retained for at least 3 years after completion of the research. The institution or IRB may maintain the records in printed form, or electronically. All records shall be accessible for inspection and copying by authorized representatives of the

Federal department or agency at reasonable times and in a reasonable manner.

§ 2584.116 General requirements for informed consent.

(a) *General.* General requirements for informed consent, whether written or oral, are set forth in this paragraph and apply to consent obtained in accordance with the requirements set forth in paragraphs (b) through (d) of this section. Broad consent may be obtained in lieu of informed consent obtained in accordance with paragraphs (b) and (c) of this section only with respect to the storage, maintenance, and secondary research uses of identifiable private information and identifiable biospecimens. Waiver or alteration of consent in research involving public benefit and service programs conducted by or subject to the approval of state or local officials is described in paragraph (e) of this section. General waiver or alteration of informed consent is described in paragraph (f) of this section. Except as provided elsewhere in this part:

(1) Before involving a human subject in research covered by this part, an investigator shall obtain the legally effective informed consent of the subject or the subject's legally authorized representative.

(2) An investigator shall seek informed consent only under circumstances that provide the prospective subject or the legally authorized representative sufficient opportunity to discuss and consider whether or not to participate and that minimize the possibility of coercion or undue influence.

(3) The information that is given to the subject or the legally authorized representative shall be in language understandable to the subject or the legally authorized representative.

(4) The prospective subject or the legally authorized representative must be provided with the information that a reasonable person would want to have in order to make an informed decision about whether to participate, and an opportunity to discuss that information.

(5) Except for broad consent obtained in accordance with paragraph (d) of this section:

(i) Informed consent must begin with a concise and focused presentation of the key information that is most likely to assist a prospective subject or legally authorized representative in understanding the reasons why one might or might not want to participate in the research. This part of the informed consent must be organized

and presented in a way that facilitates comprehension.

(ii) Informed consent as a whole must present information in sufficient detail relating to the research and must be organized and presented in a way that does not merely provide lists of isolated facts, but rather facilitates the prospective subject's or legally authorized representative's understanding of the reasons why one might or might not want to participate.

(6) No informed consent may include any exculpatory language through which the subject or the legally authorized representative is made to waive or appear to waive any of the subject's legal rights, or releases or appears to release the investigator, the sponsor, the institution, or its agents from liability for negligence.

(b) *Basic elements of informed consent.* Except as provided in paragraph (d), (e), or (f) of this section, in seeking informed consent the following information shall be provided to each subject or the legally authorized representative:

(1) A statement that the study involves research, an explanation of the purposes of the research and the expected duration of the subject's participation, a description of the procedures to be followed, and identification of any procedures that are experimental;

(2) A description of any reasonably foreseeable risks or discomforts to the subject;

(3) A description of any benefits to the subject or to others that may reasonably be expected from the research;

(4) A disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject;

(5) A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained;

(6) For research involving more than minimal risk, an explanation as to whether any compensation and an explanation as to whether any medical treatments are available if injury occurs and, if so, what they consist of, or where further information may be obtained;

(7) An explanation of whom to contact for answers to pertinent questions about the research and research subjects' rights, and whom to contact in the event of a research-related injury to the subject;

(8) A statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and the subject may discontinue participation at any time without

penalty or loss of benefits to which the subject is otherwise entitled; and

(9) One of the following statements about any research that involves the collection of identifiable private information or identifiable biospecimens:

(i) A statement that identifiers might be removed from the identifiable private information or identifiable biospecimens and that, after such removal, the information or biospecimens could be used for future research studies or distributed to another investigator for future research studies without additional informed consent from the subject or the legally authorized representative, if this might be a possibility; or

(ii) A statement that the subject's information or biospecimens collected as part of the research, even if identifiers are removed, will not be used or distributed for future research studies.

(c) *Additional elements of informed consent.* Except as provided in paragraph (d), (e), or (f) of this section, one or more of the following elements of information, when appropriate, shall also be provided to each subject or the legally authorized representative:

(1) A statement that the particular treatment or procedure may involve risks to the subject (or to the embryo or fetus, if the subject is or may become pregnant) that are currently unforeseeable;

(2) Anticipated circumstances under which the subject's participation may be terminated by the investigator without regard to the subject's or the legally authorized representative's consent;

(3) Any additional costs to the subject that may result from participation in the research;

(4) The consequences of a subject's decision to withdraw from the research and procedures for orderly termination of participation by the subject;

(5) A statement that significant new findings developed during the course of the research that may relate to the subject's willingness to continue participation will be provided to the subject;

(6) The approximate number of subjects involved in the study;

(7) A statement that the subject's biospecimens (even if identifiers are removed) may be used for commercial profit and whether the subject will or will not share in this commercial profit;

(8) A statement regarding whether clinically relevant research results, including individual research results, will be disclosed to subjects, and if so, under what conditions; and

(9) For research involving biospecimens, whether the research will (if known) or might include whole genome sequencing (*i.e.*, sequencing of a human germline or somatic specimen with the intent to generate the genome or exome sequence of that specimen).

(d) *Elements of broad consent for the storage, maintenance, and secondary research use of identifiable private information or identifiable biospecimens.* Broad consent for the storage, maintenance, and secondary research use of identifiable private information or identifiable biospecimens (collected for either research studies other than the proposed research or nonresearch purposes) is permitted as an alternative to the informed consent requirements in paragraphs (b) and (c) of this section. If the subject or the legally authorized representative is asked to provide broad consent, the following shall be provided to each subject or the subject's legally authorized representative:

(1) The information required in paragraphs (b)(2), (3), (5), and (8) of this section and, when appropriate, paragraphs (c)(7) and (9) of this section;

(2) A general description of the types of research that may be conducted with the identifiable private information or identifiable biospecimens. This description must include sufficient information such that a reasonable person would expect that the broad consent would permit the types of research conducted;

(3) A description of the identifiable private information or identifiable biospecimens that might be used in research, whether sharing of identifiable private information or identifiable biospecimens might occur, and the types of institutions or researchers that might conduct research with the identifiable private information or identifiable biospecimens;

(4) A description of the period of time that the identifiable private information or identifiable biospecimens may be stored and maintained (which period of time could be indefinite), and a description of the period of time that the identifiable private information or identifiable biospecimens may be used for research purposes (which period of time could be indefinite);

(5) Unless the subject or legally authorized representative will be provided details about specific research studies, a statement that they will not be informed of the details of any specific research studies that might be conducted using the subject's identifiable private information or identifiable biospecimens, including the purposes of the research, and that they

might have chosen not to consent to some of those specific research studies;

(6) Unless it is known that clinically relevant research results, including individual research results, will be disclosed to the subject in all circumstances, a statement that such results may not be disclosed to the subject; and

(7) An explanation of whom to contact for answers to questions about the subject's rights and about storage and use of the subject's identifiable private information or identifiable biospecimens, and whom to contact in the event of a research-related harm.

(e) *Waiver or alteration of consent in research involving public benefit and service programs conducted by or subject to the approval of state or local officials*—(1) *Waiver*. An IRB may waive the requirement to obtain informed consent for research under paragraphs (a) through (c) of this section, provided the IRB satisfies the requirements of paragraph (e)(3) of this section. If an individual was asked to provide broad consent for the storage, maintenance, and secondary research use of identifiable private information or identifiable biospecimens in accordance with the requirements at paragraph (d) of this section, and refused to consent, an IRB cannot waive consent for the storage, maintenance, or secondary research use of the identifiable private information or identifiable biospecimens.

(2) *Alteration*. An IRB may approve a consent procedure that omits some, or alters some or all, of the elements of informed consent set forth in paragraphs (b) and (c) of this section provided the IRB satisfies the requirements of paragraph (e)(3) of this section. An IRB may not omit or alter any of the requirements described in paragraph (a) of this section. If a broad consent procedure is used, an IRB may not omit or alter any of the elements required under paragraph (d) of this section.

(3) *Requirements for waiver and alteration*. In order for an IRB to waive or alter consent as described in this subsection, the IRB must find and document that:

(i) The research or demonstration project is to be conducted by or subject to the approval of state or local government officials and is designed to study, evaluate, or otherwise examine:

(A) Public benefit or service programs;

(B) Procedures for obtaining benefits or services under those programs;

(C) Possible changes in or alternatives to those programs or procedures; or

(D) Possible changes in methods or levels of payment for benefits or services under those programs; and

(ii) The research could not practicably be carried out without the waiver or alteration.

(f) *General waiver or alteration of consent*—(1) *Waiver*. An IRB may waive the requirement to obtain informed consent for research under paragraphs (a) through (c) of this section, provided the IRB satisfies the requirements of paragraph (f)(3) of this section. If an individual was asked to provide broad consent for the storage, maintenance, and secondary research use of identifiable private information or identifiable biospecimens in accordance with the requirements at paragraph (d) of this section, and refused to consent, an IRB cannot waive consent for the storage, maintenance, or secondary research use of the identifiable private information or identifiable biospecimens.

(2) *Alteration*. An IRB may approve a consent procedure that omits some, or alters some or all, of the elements of informed consent set forth in paragraphs (b) and (c) of this section provided the IRB satisfies the requirements of paragraph (f)(3) of this section. An IRB may not omit or alter any of the requirements described in paragraph (a) of this section. If a broad consent procedure is used, an IRB may not omit or alter any of the elements required under paragraph (d) of this section.

(3) *Requirements for waiver and alteration*. In order for an IRB to waive or alter consent as described in this subsection, the IRB must find and document that:

(i) The research involves no more than minimal risk to the subjects;

(ii) The research could not practicably be carried out without the requested waiver or alteration;

(iii) If the research involves using identifiable private information or identifiable biospecimens, the research could not practicably be carried out without using such information or biospecimens in an identifiable format;

(iv) The waiver or alteration will not adversely affect the rights and welfare of the subjects; and

(v) Whenever appropriate, the subjects or legally authorized representatives will be provided with additional pertinent information after participation.

(g) *Screening, recruiting, or determining eligibility*. An IRB may approve a research proposal in which an investigator will obtain information or biospecimens for the purpose of screening, recruiting, or determining the eligibility of prospective subjects without the informed consent of the prospective subject or the subject's legally authorized representative, if

either of the following conditions are met:

(1) The investigator will obtain information through oral or written communication with the prospective subject or legally authorized representative, or

(2) The investigator will obtain identifiable private information or identifiable biospecimens by accessing records or stored identifiable biospecimens.

(h) *Posting of clinical trial consent form*. (1) For each clinical trial conducted or supported by a Federal department or agency, one IRB-approved informed consent form used to enroll subjects must be posted by the awardee or the Federal department or agency component conducting the trial on a publicly available Federal website that will be established as a repository for such informed consent forms.

(2) If the Federal department or agency supporting or conducting the clinical trial determines that certain information should not be made publicly available on a Federal website (e.g., confidential commercial information), such Federal department or agency may permit or require redactions to the information posted.

(3) The informed consent form must be posted on the Federal website after the clinical trial is closed to recruitment, and no later than 60 days after the last study visit by any subject, as required by the protocol.

(i) *Preemption*. The informed consent requirements in this part are not intended to preempt any applicable Federal, state, or local laws (including Tribal laws passed by the official governing body of an American Indian or Alaska Native Tribe) that require additional information to be disclosed in order for informed consent to be legally effective.

(j) *Emergency medical care*. Nothing in this part is intended to limit the authority of a physician to provide emergency medical care, to the extent the physician is permitted to do so under applicable Federal, state, or local law (including Tribal law passed by the official governing body of an American Indian or Alaska Native Tribe).

§ 2584.117 Documentation of informed consent.

(a) Except as provided in paragraph (c) of this section, informed consent shall be documented by the use of a written informed consent form approved by the IRB and signed (including in an electronic format) by the subject or the subject's legally authorized representative. A written

copy shall be given to the person signing the informed consent form.

(b) Except as provided in paragraph (c) of this section, the informed consent form may be either of the following:

(1) A written informed consent form that meets the requirements of § 2584.116. The investigator shall give either the subject or the subject's legally authorized representative adequate opportunity to read the informed consent form before it is signed; alternatively, this form may be read to the subject or the subject's legally authorized representative.

(2) A short form written informed consent form stating that the elements of informed consent required by § 2584.116 have been presented orally to the subject or the subject's legally authorized representative, and that the key information required by § 2584.116(a)(5)(i) was presented first to the subject, before other information, if any, was provided. The IRB shall approve a written summary of what is to be said to the subject or the legally authorized representative. When this method is used, there shall be a witness to the oral presentation. Only the short form itself is to be signed by the subject or the subject's legally authorized representative. However, the witness shall sign both the short form and a copy of the summary, and the person actually obtaining consent shall sign a copy of the summary. A copy of the summary shall be given to the subject or the subject's legally authorized representative, in addition to a copy of the short form.

(c)(1) An IRB may waive the requirement for the investigator to obtain a signed informed consent form for some or all subjects if it finds any of the following:

(i) That the only record linking the subject and the research would be the informed consent form and the principal risk would be potential harm resulting from a breach of confidentiality. Each subject (or legally authorized representative) will be asked whether the subject wants documentation linking the subject with the research, and the subject's wishes will govern;

(ii) That the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context; or

(iii) If the subjects or legally authorized representatives are members of a distinct cultural group or community in which signing forms is not the norm, that the research presents no more than minimal risk of harm to

subjects and provided there is an appropriate alternative mechanism for documenting that informed consent was obtained.

(2) In cases in which the documentation requirement is waived, the IRB may require the investigator to provide subjects or legally authorized representatives with a written statement regarding the research.

§ 2584.118 Applications and proposals lacking definite plans for involvement of human subjects.

Certain types of applications for grants, cooperative agreements, or contracts are submitted to Federal departments or agencies with the knowledge that subjects may be involved within the period of support, but definite plans would not normally be set forth in the application or proposal. These include activities such as institutional type grants when selection of specific projects is the institution's responsibility; research training grants in which the activities involving subjects remain to be selected; and projects in which human subjects' involvement will depend upon completion of instruments, prior animal studies, or purification of compounds. Except for research waived under § 2584.101(i) or exempted under § 2584.104, no human subjects may be involved in any project supported by these awards until the project has been reviewed and approved by the IRB, as provided in this part, and certification submitted, by the institution, to the Federal department or agency component supporting the research.

§ 2584.119 Research undertaken without the intention of involving human subjects.

Except for research waived under § 2584.101(i) or exempted under § 2584.104, in the event research is undertaken without the intention of involving human subjects, but it is later proposed to involve human subjects in the research, the research shall first be reviewed and approved by an IRB, as provided in this part, a certification submitted by the institution to the Federal department or agency component supporting the research, and final approval given to the proposed change by the Federal department or agency component.

§ 2584.120 Evaluation and disposition of applications and proposals for research to be conducted or supported by a Federal department or agency.

(a) The department or agency head will evaluate all applications and proposals involving human subjects submitted to the Federal department or agency through such officers and

employees of the Federal department or agency and such experts and consultants as the department or agency head determines to be appropriate. This evaluation will take into consideration the risks to the subjects, the adequacy of protection against these risks, the potential benefits of the research to the subjects and others, and the importance of the knowledge gained or to be gained.

(b) On the basis of this evaluation, the department or agency head may approve or disapprove the application or proposal or enter into negotiations to develop an approvable one.

§ 2584.121 [Reserved]

§ 2584.122 Use of Federal funds.

Federal funds administered by a Federal department or agency may not be expended for research involving human subjects unless the requirements of this part have been satisfied.

§ 2584.123 Early termination of research support: Evaluation of applications and proposals.

(a) The department or agency head may require that Federal department or agency support for any project be terminated or suspended in the manner prescribed in applicable program requirements, when the department or agency head finds an institution has materially failed to comply with the terms of this part.

(b) In making decisions about supporting or approving applications or proposals covered by this part the department or agency head may take into account, in addition to all other eligibility requirements and program criteria, factors such as whether the applicant has been subject to a termination or suspension under paragraph (a) of this section and whether the applicant or the person or persons who would direct or has/have directed the scientific and technical aspects of an activity has/have, in the judgment of the department or agency head, materially failed to discharge responsibility for the protection of the rights and welfare of human subjects (whether or not the research was subject to Federal regulation).

§ 2584.124 Conditions.

With respect to any research project or any class of research projects the department or agency head of either the conducting or supporting Federal department or agency may impose additional conditions prior to or at the time of approval when in the judgment of the department or agency head

additional conditions are necessary for the protection of human subjects.

Andrea Grill,

Acting General Counsel.

[FR Doc. 2024-24517 Filed 10-28-24; 8:45 am]

BILLING CODE 6050-28-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 635

[Docket No. 241010-0271]

RIN 0648-BK89

Atlantic Highly Migratory Species; Updates Regarding Sea Turtle Careful Release Equipment and Techniques

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Final rule.

SUMMARY: In this final rule, NMFS updates the Atlantic highly migratory species (HMS) regulations regarding the sea turtle safe handling and release requirements and equipment in the HMS pelagic and bottom longline fisheries. This action is based in part on two technical memoranda published by NMFS' Southeast Fisheries Science Center (SEFSC). The regulatory updates replace some of the more technical terms with those that are more commonly used, add more detail to make the regulations more understandable, and add additional tools or options for fishermen to use to safely handle and release sea turtles. In addition, this final rule simplifies the regulations by removing redundancies, making minor changes in formatting, and revising wording to clarify responsibility of implementation.

DATES: This final rule is effective November 29, 2024.

ADDRESSES: Additional information related to this final rule, including electronic copies of the supporting documents are available from the HMS Management Division website at: <https://www.fisheries.noaa.gov/topic/atlantic-highly-migratory-species>, at: <https://www.regulations.gov> (enter "NOAA-NMFS-2024-0046" in the Search box), or by contacting Becky Curtis at becky.curtis@noaa.gov. The referenced technical memoranda are available from the HMS Management Division website at: <https://www.fisheries.noaa.gov/resource/outreach-materials/atlantic-highly-migratory-species-safe-handling-release-and>.

migratory-species-safe-handling-release-and. These documents are also available upon request from the HMS Management Division by phone at 301-427-8503.

FOR FURTHER INFORMATION CONTACT:

Becky Curtis, becky.curtis@noaa.gov, Steve Durkee, steve.durkee@noaa.gov or Karyl Brewster-Geisz, karyl.brewster-geisz@noaa.gov; 301-427-8503.

SUPPLEMENTARY INFORMATION:

Background

Atlantic HMS fisheries are managed under the 2006 Consolidated HMS Fishery Management Plan (FMP) and its amendments, pursuant to the Magnuson-Stevens Fishery Conservation and Management Act (Magnuson-Stevens Act) (16 U.S.C. 1801 *et seq.*) and consistent with the Atlantic Tunas Convention Act (ATCA) (16 U.S.C. 971 *et seq.*). HMS implementing regulations are at 50 CFR part 635. The sea turtle handling and release requirements and equipment are located at § 635.21(b) through (d).

This final rule is issued pursuant to, and subject to requirements of, the Magnuson-Stevens Act. Specifically in regard to the sea turtle safe handling and release measures implemented in this rule, 16 U.S.C. 1851(a)(9) requires NMFS to implement fishery management measures that minimize bycatch, and to the extent bycatch cannot be avoided, minimize the mortality of bycatch. The Magnuson-Stevens Act defines bycatch as fish which are harvested but which are not sold or kept for personal use at 16 U.S.C. 1802(2) (see also 16 U.S.C. 1802(12) (defining "fish")). Sea turtles are listed and protected under the Endangered Species Act and cannot be sold or kept for personal use (see 16 U.S.C. 1538(a)(1) and 16 U.S.C. 1533(d)).

Background information about the need for regulatory updates to modify the sea turtle handling and release requirements and equipment and specific examples of updates made under this action were provided in the preamble to the proposed rule (89 FR 24416, April 8, 2024) and are not repeated here. In summary, two technical memoranda were published by the SEFSC in 2019: NMFS-SEFSC TM735: "Careful Release Protocols for Sea Turtle Release with Minimal Injury," and NMFS-SEFSC TM738: "Design Standards and Equipment for Careful Release of Sea Turtles Caught in Hook-and-Line Fisheries." NMFS decided that it would be helpful to revise the existing regulations in light of the 2019 technical memoranda. Based in

part on those memoranda, this final rule modifies the regulations by: (1) adding additional options for tools and procedures for fishermen to use to safely handle and release sea turtles; (2) replacing some of the more technical terms with those that are more commonly used; (3) adding more detail to make the regulations more understandable; and (4) simplifying the regulations by removing redundancies. NMFS received five written comments during the public comment period for the proposed rule, which closed on May 8, 2024. The comments received, and responses to those comments, are summarized in the Response to Comments section. No changes to the final rule are planned in response to the comments received. However, one minor change from the proposed rule is outlined in the Changes from Proposed Rule section.

Under this final rule, fishermen are able to continue using existing, approved sea turtle bycatch mitigation equipment. The final rule also provides additional tool and procedural options that fishermen may use to meet the sea turtle safe handling and release requirements.

Response to Comments

Written comments can be found at: <https://www.regulations.gov>; type "NOAA-NMFS-2024-0046" in the Search box. Below, NMFS summarizes and responds to the comments made on the proposed rule during the comment period. Comments covering the same topics were consolidated.

Comment 1: NMFS received multiple comments expressing support for the proposed update of sea turtle careful handling and release regulations. Commenters noted that the updates would improve outcomes for incidentally-caught sea turtles released by fishermen and improve clarity of the sea turtle safe handling and release regulations, improve awareness of and confidence in sea turtle release techniques, and, due to the additional approved tools, reduce instances where the required tools are forgotten or not on hand.

Response: NMFS agrees that the proposed changes would provide clarity regarding sea turtle safe handling and release requirements. Additionally, the proposed changes will increase flexibility for complying with these requirements.

Comment 2: NMFS received one comment expressing concerns about the cost of the new, optional tools that would be authorized for sea turtle safe handling techniques, and whether that

cost might hinder adoption of the new equipment.

Response: The additional tools that would be authorized are strictly optional and not necessary for regulatory compliance. Instead, the additional tools provide fishermen additional flexibility to comply with the handling and release requirements in a manner that maximizes the efficacy of the operations on their vessel. If fishery participants decide not to purchase the additional tools due to their cost, they can remain in compliance by carrying the tools that are already approved under the current regulations.

Comment 3: NMFS received multiple comments on topics that reach beyond the minor regulatory updates and sea turtle bycatch issues in the proposed rule. One commenter mentioned that additional actions should be taken to prevent bycatch of sea turtles, including restricting fishing activities based on water temperature, reducing soak times, and changing fishing techniques and equipment. Another commenter suggested that all longline fishing for HMS be banned. Finally, another commenter focused on wind energy production and its potential threats to birds and turtles.

Response: NMFS considers these comments to be outside the scope of the current rulemaking. The focus of this rule is to update current sea turtle safe handling and release requirements to more clearly describe safe handling techniques, update the names of some required tools, approve additional tools for safe handling and release procedures, and to simplify regulations by removing redundancies, and making minor changes to clarify responsibility of implementation.

Changes From the Proposed Rule

No changes were made from the proposed rule in response to public comments. However, in this final rule, the term “comatose” has been replaced with “unresponsive” when referring to turtles that must be brought on board for gear removal. This change more accurately describes the state of the turtle and matches other agency resuscitation guidance.

Classification

As described in the statutory information in the Background section above, NMFS is issuing this rule pursuant to the Magnuson-Stevens Act, including sections 301(a)(9) and 304(g). The NMFS Assistant Administrator has determined that the final rule is consistent with the 2006 Consolidated HMS FMP and its amendments, other

provisions of the Magnuson-Stevens Act, ATCA, and other applicable law.

This final rule has been determined to be not significant for purposes of Executive Order 12866.

The Chief Council for Regulation of the Department of Commerce certified to the Chief Council for Advocacy of the Small Business Administration that the proposed rule, if adopted, would not have a significant economic impact on a substantial number of small entities. No comments were received regarding this certification. As a result, a regulatory flexibility analysis was not required and none was prepared. For Regulatory Flexibility Act (RFA) compliance purposes, NMFS established a small business size standard of \$11 million in annual gross receipts for all businesses in the commercial fishing industry (North American Industry Classification System (NAICS) 11411). The Small Business Administration (SBA) has established size standards for all other major industry sectors in the United States, including the scenic and sightseeing transportation (water) sector (NAICS code 487210), which includes for-hire (charter/party boat) fishing entities. The SBA has defined a small entity under the scenic and sightseeing transportation (water) sector as one with average annual receipts (revenue) of less than \$14 million. NMFS considers all HMS permit holders to be small entities because they had average annual receipts of less than their respective sector’s standard of \$11 million and \$14 million. Regarding those entities that would be directly affected by the measures under this final rule, the average revenue for the entire Atlantic shark commercial fishery from 2017 through 2021 is \$2,579,228, which is well below the NMFS small business size standard for commercial fishing businesses of \$11 million. The average annual revenue per active pelagic longline vessel in HMS fisheries is estimated to be \$222,000, also well below the small business size standard. While the entire HMS pelagic longline fishery (approximately 82 active vessels) produced an estimated \$18.2 million in revenue in 2020, no single pelagic longline vessel has exceeded \$11 million in revenue in recent years. Additionally, HMS bottom longline commercial fishing vessels typically earn less revenue than pelagic longline vessels and, thus, would also be considered small entities. While all entities directly affected by the measures under this final rule are considered small entities, significant economic impacts are not expected and a regulatory flexibility analysis was not

required and none was prepared for this final rule.

This final rule contains no information collection requirements under the Paperwork Reduction Act of 1995.

List of Subjects in 50 CFR Part 635

Fisheries, Fishing, Fishing vessels, Foreign relations, Imports, Penalties, Reporting and recordkeeping requirements, Statistics, Treaties.

Dated: October 21, 2024.

Samuel D. Rauch III,

Deputy Assistant Administrator for Regulatory Programs, National Marine Fisheries Service.

For the reasons set out in the preamble, NMFS amends 50 CFR part 635 to read as follows:

PART 635—ATLANTIC HIGHLY MIGRATORY SPECIES

■ 1. The authority citation for part 635 continues to read as follows:

Authority: 16 U.S.C. 971 *et seq.*; 16 U.S.C. 1801 *et seq.*

■ 2. In § 635.21:

■ a. Revise paragraphs (b)(3) and (c)(2)(iv)(C);

■ b. Remove paragraphs (c)(2)(iv)(D) through (G); and

■ c. Revise paragraphs (c)(5) introductory paragraph, (c)(5)(i)(B) through (L), (c)(5)(i)(M)(1) and (2), (c)(5)(ii)(A) through (C), (c)(5)(iii) introductory text, and (d)(2) introductory text.

The revisions read as follows:

§ 635.21 Gear operation and deployment restrictions.

* * * * *

(b) * * *

(3) When a marine mammal or sea turtle is hooked or entangled by pelagic or bottom longline gear, the owner and operator of the vessel must immediately release the animal, retrieve the pelagic or bottom longline gear, and move at least 1 nmi (2 km) from the location of the incident before resuming fishing. Similarly, when a smalltooth sawfish is hooked or entangled by bottom longline gear, the operator of the vessel must immediately release the animal, retrieve the bottom longline gear, and move at least 1 nmi (2 km) from the location of the incident before resuming fishing. Reports of marine mammal entanglements must be submitted to NMFS consistent with regulations in § 229.6 of this title.

* * * * *

(c) * * *

(2) * * *

(iv) * * *

(C) All sea turtle bycatch mitigation measures specified in paragraph (c)(5) of this section, except for the mitigation measures specified in paragraphs (c)(5)(iii)(B) and (C) of this section, as these paragraphs specify bait, hook size, and hook type requirements for vessels fishing outside the NED as defined in § 635.2. Instead, persons on board the vessel must comply with hook size and type requirements in paragraph (c)(2)(iv)(A) of this section and bait restrictions in paragraph (c)(2)(iv)(B) of this section.

* * * * *

(5) The owner and operator of a vessel permitted or required to be permitted under this part and that has pelagic longline gear on board must undertake the following sea turtle bycatch mitigation measures:

(i) * * *

(B) *Long-handled dehooker for internal hooks.* A long-handled dehooking device is intended to remove internal hooks from sea turtles that cannot be boated. It should also be used to engage a loose hook when a turtle is entangled but not hooked, and line is being removed. The design must shield the point of the hook and prevent the hook from re-engaging during the removal process. One long-handled device, meeting the minimum design standards as described below, is required on board to remove internal hooks. The minimum design standards are as follows:

(1) *Hook removal device.* Marine-grade stainless steel (316 L or 304 L) or similar (*i.e.*, designed to resist corrosion during exposure to saltwater) must be used for all components. The hook removal device must be constructed of three-sixteenths to five-sixteenths of an inch (4.76–7.94 mm) marine-grade stainless steel and have a dehooking end no larger than 1 $\frac{7}{8}$ -inch (4.76-cm) outside diameter. The device must securely engage and control the leader while shielding the point of the hook to prevent the hook from re-engaging during removal. The hook removal device must not have any unprotected points (including blunt ones), as these could cause injury to the mouth and esophagus during hook removal. The device must be of a size appropriate to secure the range of hook sizes and styles used in the pelagic longline fishery targeting swordfish and tuna.

(2) *Extended reach handle.* The dehooking end must be securely fastened to an extended reach handle or pole with a minimum length equal to or greater than 150 percent of the height of the vessel's freeboard, or 6 ft (1.83 m), whichever is greater. It is recommended,

but not required, that the handle break down into sections. The handle must be sturdy and strong enough to facilitate the secure attachment of the hook removal device.

(C) *Long-handled dehooker for external hooks.* A long-handled dehooker, meeting the minimum design standards, is required on board for use on externally hooked sea turtles that cannot be boated. The long-handled dehooker for internal hooks described in paragraph (c)(5)(i)(B) of this section meets this requirement. The minimum design standards are as follows:

(1) *Hook removal device.* Marine-grade stainless steel (316 L or 304 L) or similar (*i.e.*, designed to resist corrosion during exposure to saltwater) must be used for all components on any style of long-handled dehooker. If utilizing a wire-style dehooker (*e.g.*, a pigtail or J-style dehooker), the long-handled dehooker must be constructed of three-sixteenths to five-sixteenths of an inch (4.76–7.94 mm) marine-grade stainless steel. All long-handled dehookers must have a dehooking end no larger than 1 $\frac{7}{8}$ -inch (4.76-cm) outside diameter. Smaller dehooking ends may be appropriate when encountering small turtles. A 5-inch (12.7-cm) tube T-handle of 1-inch (2.54-cm) outside diameter is recommended, but not required. The design must be such that a fish hook can be rotated out, without pulling it out at an angle, as described in paragraphs (c)(5)(ii)(B) and (C) of this section, and in the NMFS–SEFSC TM–735 Careful Release Protocols. The dehooking end must be blunt with all edges rounded. The device must be of a size appropriate to secure the range of hook sizes and styles used in the pelagic longline fishery targeting swordfish and tuna.

(2) *Extended reach handle.* The dehooking end must be securely fastened to an extended reach handle or pole. The handle must be a minimum length equal to or greater than 150 percent of the height of the vessel's freeboard or 6 ft (1.83 m), whichever is greater.

(D) *Long-handled device to pull an "inverted V."* This tool is used to pull a "V" in the fishing line when implementing the "inverted V" dehooking technique, as described in paragraph (c)(5)(ii)(C) of this section and in the NMFS–SEFSC TM–735 Careful Release Protocols, for disentangling and dehooking entangled sea turtles. One long-handled device to pull an "inverted V", meeting the minimum design standards, is required on board. If a 6 ft (1.83 m) or longer J-style dehooker is used to comply with paragraph (c)(5)(i)(C) of this section, it

will also satisfy this requirement. Minimum design standards are as follows:

(1) *Hook end.* This device, such as a standard boat hook, gaff, or long-handled J-style dehooker must be constructed of stainless steel or aluminum. A sharp point, such as on a gaff hook, is to be used only for holding the monofilament fishing line and must never contact the sea turtle.

(2) *Extended reach handle.* The handle must have a minimum length equal to or greater than 150 percent of the height of the vessel's freeboard, or 6 ft (1.83 m), whichever is greater. The handle must be sturdy and strong enough to facilitate the secure attachment of the gaff hook.

(E) *Boating the turtle.* A device to bring incidentally caught sea turtles aboard the vessel must be carried on board the vessel to facilitate safe handling of sea turtles by allowing them to be brought on board for fishing gear removal without causing further injury to the animal. Sea turtles must never be brought on board without a net or hoist. Using the involved fishing gear to raise the turtle can result in serious injury. The following devices are options to meet this requirement.

(1) *Dipnet.* The dipnet must have a sturdy net hoop of at least 31 inches (78.74 cm) of inside diameter and a bag depth of at least 38 inches (96.52 cm) to accommodate turtles below 3 ft (91.44 cm) carapace length. The bag mesh openings may not exceed 3 inches (7.62 cm) bar measure, defined as the non-stretched distance between a side knot and a bottom knot of a net mesh (also known as the square mesh measurement). There must be no sharp edges or burrs on the hoop, or where the hoop is attached to the handle. The dipnet hoop must be securely fastened to an extended reach handle or pole with a minimum length equal to, or greater than, 150 percent of the height of the vessel's freeboard, or at least 6 ft (1.83 m), whichever is greater. The handle must be made of a rigid material strong enough to facilitate the sturdy attachment of the net hoop and able to support a minimum of 100 lb (45.36 kg) without breaking or significant bending or distortion. It is recommended, but not required, that the extended reach handle break down into sections.

(2) *Collapsible hoop net.* The collapsible hoop net frame must be constructed of stiff wire cable that coils to compress the size for storage. This device must have a minimum 31-inch (78.74-cm) inside diameter and a bag depth of at least 38 inches (96.52 cm) to accommodate turtles up to 3 ft (91.44 cm) in straight carapace length. The bag

mesh openings may not exceed 3 inches (7.62 cm) bar measure, defined as the non-stretched distance between a side knot and a bottom knot of a net mesh (also known as the square mesh measurement). There must be no sharp edges or burrs on the hoop. The device must be capable of lifting at least 100 lb (45.36 kg). No extended reach handle is needed on this type of net, although the rope handle length must be 6 ft (1.83 m) or 150 percent of freeboard height, whichever is greater.

(3) *Turtle hoist*. A turtle hoist consists of a supportive frame with mesh netting. A turtle hoist can be used to bring turtles on board that cannot be boated using a dipnet or collapsible hoop net. The two sizes that meet the design standards are described in paragraphs (c)(5)(i)(E)(3)(i) and (ii) of this section. The size of the turtle hoist used should match the size of turtles encountered.

(i) *Small turtle hoist*. The frame must be capable of supporting at least 100 lb (45.36 kg), with a minimum inside diameter of 31 inches (78.74 cm) to accommodate turtles up to 3 ft (91.44 cm) straight carapace length. This frame can be hinged or otherwise designed so that it can be folded for ease of storage as long as it can be quickly reassembled. If the frame is designed to fold or break down for storage, the hardware must be self-contained (e.g., barrel bolts on both sides to lock down frame with no loose pieces like through bolts and nuts), and there must be no sharp edges. The shape of the frame does not matter (e.g., round, square, rectangular, or a “U-shaped” or “J-shaped” basket) as long as it meets the required specifications and securely contains the turtle. The frame may be constructed of heavy-duty stainless steel tubing welded into shape or polyvinyl chloride (PVC) pipe (recommended 2-inch (5.08-cm) diameter with a required minimum strength of Schedule 40) connected and glued at the corners using 90° elbow fittings. PVC pipes can be drilled to facilitate water drainage for ease of hauling. A shallow bag net with mesh openings not to exceed 3 × 3 inches (7.62 × 7.62 cm) (bar measure) must be securely affixed to the frame, and lines (e.g., polypropylene, nylon, polyester) must be securely attached to each corner to control and retrieve the frame and net. The lines can be operated using a pulley system if available on the vessel. No rigid extended reach handle is needed on this type of net, although the rope handle length must be 6 ft (1.83 m) or 150 percent of freeboard height, whichever is greater.

(ii) *Large turtle hoist*. The large turtle hoist must be capable of lifting a minimum of half a ton. The structure of the hoist must consist of three circular

aluminum bar rings (top, middle, and bottom) connected with mesh and spokes. The hoist should be designed so that when on board, the turtle is suspended above the deck on a platform of mesh netting (8 mm, 6.5 inches (16.51 cm) stretch knotless 600-ply polyethylene netting) stretched across the middle ring. The turtle should be contained within a webbing fence (at least 18 inches (45.72 cm) high) which is supported by the top and middle rings and made of 3 mm, 4.7 inches (11.94 cm) stretch mesh braided polyethylene webbing, and wrapped along the top ring with ½-inch (1.27-cm) polypropylene rope. The top and middle rings (1¾ inch (4.45 cm) 50 series aluminum round bar) should be 7 ft and 6 inches (2.29 m) in diameter. The bottom ring (1½ inches (3.81 cm) 50 series aluminum round bar) should be 4 ft (1.22 m) in diameter. The middle and bottom rings are connected using 12 spoke braces (approximately 23 inches (58.42 cm) long, 1 inch (2.54 cm) round 50 series aluminum round bar or 6061 T6 1 inch (2.54 cm) Schedule 40 pipe) angled at approximately 25° and welded in place with an appropriate welding wire (5052, 6061 or 3003 wire). Rubber cookies (8 × 2½ inches (20.32 × 6.35 cm), 4 per each of 12 sections) may be used on the middle ring to facilitate rolling the hoist up the side of the vessel and to cushion impact of the hoist against the side of the vessel. When deployed in rough seas, the hoist should be held to the side of the vessel to prevent swinging and collision with the vessel hull. A 3- or 4-point bridle is attached to the top ring using pair links and three-quarter-inch (1.91-cm) nylon 3-strand line, and a hydraulic lift is used to bring hoist aboard.

(F) *Cushion/support device for boated turtles*. Each vessel is required to carry a device that effectively cushions and supports a sea turtle while it is on board. The device used must be appropriately sized to support the sea turtle encountered. The device must be puncture proof (e.g., no inner tubes, pool toys) and cannot be a primary safety device (e.g., primary life ring or life jacket dedicated to personnel on board). Examples that meet current design standards include:

(1) *A standard automobile tire*. A standard (not from a truck or heavy equipment) passenger vehicle tire not mounted on a rim and free of exposed steel belts, is effective for supporting a turtle in an upright orientation while it is on board. An assortment of sizes is recommended to accommodate a range of turtle sizes. If the turtle is too large for the tire, it must be contained and

supported on an alternative cushioned surface.

(2) *Boat cushion*. A standard boat cushion can effectively support smaller turtles.

(3) *Large turtle hoist*. This style is recommended for supporting large turtles such as leatherbacks, which need a supportive platform while on board. The large turtle hoist described in paragraph (c)(5)(i)(E)(3)(ii) of this section satisfies this requirement.

(G) *Short-handled dehooker for internal hooks*. One short-handled device, meeting the minimum design standards, is required on board for removing hooks that are internal or ingested. This dehooker is designed to remove internal hooks from boated sea turtles. It can also be used on external hooks or hooks in the front of the mouth. Minimum design standards are as follows:

(1) *Hook removal device*. Unless otherwise noted, all components must be made of marine-grade stainless steel (316 L or 304 L). If utilizing a wire-style dehooker (e.g., a pigtail or J-style dehooker), the hook removal device must be constructed of three-sixteenths to five-sixteenths of an inch (4.76–7.94 mm) marine-grade stainless steel (316 L or 304 L) rod and have a dehooking end no wider than 1⅞ inches (4.76 cm) total width. The end must allow the hook to be secured and the point to be shielded without re-engaging during the removal process. It may not have any unprotected terminal points or sharp edges, as this could cause injury to the esophagus during hook removal. A sliding PVC bite block must be used to protect the beak and facilitate hook removal if the turtle bites down on the dehooking device. The bite block should be constructed of a three-quarter- to 1-inch (1.91–2.54 cm) inside diameter high-impact plastic cylinder (e.g., Schedule 80 PVC) that is 4–6 in (10.16–15.24 cm) long to allow for at least 5 inches (12.7 cm) of slide along the shaft. The device must be of a size appropriate to secure the range of hook sizes and styles used in the pelagic longline fishery targeting swordfish and tuna.

(2) *Handle length*. The handle must be 16–24 inches (40.64–60.96 cm) in length, with a tube T-handle, wire loop handle, or similar type of handle that is approximately 4–6 inches (10.16–15.24 cm) long.

(H) *Short-handled dehooker for external hooks*. One short-handled dehooker for external hooks, meeting the minimum design standards, is required on board. The short-handled dehooker for internal hooks required to comply with paragraph (c)(5)(i)(G) of this section will also satisfy this

requirement. Minimum design standards are as follows:

(1) *Hook removal device.* Marine-grade stainless steel (316 L or 304 L) must be used for all components. If utilizing a wire-style dehooker (e.g., a pigtail or J-style dehooker), the dehooker must be constructed of three-sixteenths to five-sixteenths of an inch (4.76–7.94 mm) marine-grade stainless steel (316 L or 304 L) and have a dehooking end no wider than $1\frac{7}{8}$ inches (4.76 cm) total width. The design must be such that a hook can be rotated out without pulling it out at an angle. The dehooking end must be blunt, and all edges rounded. The device must be of a size appropriate to secure the range of hook sizes and styles used in the pelagic longline fishery targeting swordfish and tuna.

(2) *Handle length.* The handle must be 16–24 inches (40.64–60.96 cm) long with a tube T-handle, wire loop handle, or similar type of handle that is approximately 4–6 inches (10.16–15.24 cm) long.

(I) *Long-nose or needle-nose pliers.* One pair of long-nose or needle-nose pliers is required to be on board. Such pliers must be a minimum of 11 inches (27.94 cm) in length, and should be constructed of stainless steel material or other material designed to resist corrosion during exposure to saltwater. The pliers can be used to remove embedded hooks from the turtle's flesh or hooks in the front of the mouth. The pliers are also useful for holding PVC splice couplings in place as mouth openers.

(J) *Bolt cutters.* One pair of bolt cutters is required on board. Such bolt cutters must be a minimum of 14 inches (35.56 cm) in total length, with a minimum of 4 inches (10.16 cm) long blades that are a minimum of $2\frac{1}{4}$ inches (5.72 cm) wide, when closed, and with 10- to 13-inch (25.40- to 33.02-cm) long handles. Such bolt cutters must be able to cut hard metals, such as stainless or carbon steel hooks, up to one-quarter of an inch (6.35 mm) in diameter, and they must be capable of cutting through the hooks used on a vessel. The required bolt cutters may be used to cut hooks to facilitate their removal. They should be used to cut off the eye or point of a hook, so that it can safely be pushed through a sea turtle without causing further injury. They should also be used to cut off as much of the hook as possible, when the remainder of the hook cannot be removed.

(K) *Monofilament line cutters.* One pair of monofilament line cutters is required on board. Such monofilament line cutters must be a minimum of 6 inches (15.24 cm) in overall length. The

blades must be 1 inch (2.54 cm) in length and five-eighths inch (1.59 cm) wide, when closed, and are recommended to be coated with Teflon (a trademark owned by E.I. DuPont de Nemours and Company Corp.). The line cutters must be used to remove netting, entangling line, or fishing line as close to the eye of the hook as possible, if the hook is swallowed or cannot be removed safely.

(L) *Mouth openers/mouth gags.* Required mouth openers and mouth gags are used to open sea turtle mouths, and to keep them open when removing internal hooks from boated turtles. They must allow access to the hook or line without causing further injury to the turtle. Design standards are included in the item descriptions. At least 2 of the 7 different types of mouth openers/gags described below are required on board the vessel:

(1) *A block of hard wood.* Placed in the corner of the jaw, a block of hard wood may be used to gag open a turtle's mouth. A smooth block of hard wood of a type that does not splinter (e.g., maple) with rounded edges must be sanded smooth. The dimensions should be appropriately sized for the size of turtles that may be caught or approximately $10 \times 0.75 \times 0.75$ inches (25.40 $\times$ 1.91 $\times$ 1.91 cm). A long-handled, wire shoe brush with a wooden handle, and with the wires removed, is an inexpensive, effective and practical mouth-opening device that meets these requirements. A wooden hammer handle (without the head attached) may also be suitable, provided it is made from wood that does not splinter under pressure (e.g., ash, maple).

(2) *A set of three canine mouth gags.* Canine mouth gags are highly recommended to hold a turtle's mouth open, because the gag locks into an open position to allow for hands-free operation after it is in place. A set of canine mouth gags must include one of each of the following sizes: small (5 in; 12.7 cm), medium (6 in; 15.24 cm), and large (7 in; 17.78 cm). They must be constructed of stainless steel.

(3) *A set of two sturdy dog chew bones.* Placed in the corner of a turtle's jaw, canine chew bones are used to gag open a sea turtle's mouth. Required canine chews must be constructed of durable nylon, zylene resin, or thermoplastic polymer, and strong enough to withstand biting without splintering. To accommodate a variety of turtle beak sizes, a set must include one large (5.5–8 inches (13.97–20.32 cm) in length) and one small (3.5–4.5 inches (8.89–11.43 cm) in length) canine chew bone.

(4) *A set of two rope loops covered with hose.* A set of 2 rope loops covered with a piece of hose or flexible tubing can be used as a mouth opener, and to keep a turtle's mouth open during hook and/or line removal. A required set consists of two 3-ft (91.44-cm) lengths of poly braid rope (three-eighths of an inch (9.53 mm) in diameter is suggested), each covered with an 8-inch (20.32-cm) section of half-inch (1.27-cm) or three-quarter-inch (1.91-cm) light-duty garden hose or flexible tubing, and each tied into a loop. The upper loop of rope covered with hose is secured on the upper beak to give control with one hand, and the second piece of rope covered with hose is secured on the lower beak to give control with the user's foot.

(5) *A hank of rope.* Placed in the corner of a turtle's jaw, a hank of rope can be used to gag open a sea turtle's mouth. A 6-ft (1.83-m) lanyard with a minimum of three-sixteenths-inch (4.76-mm) braided soft rope may be folded to create a hank, (or a coiled or looped bundle), of rope. Any size braided soft rope is allowed; however, it must create a hank of approximately 2–4 inches (5.08–10.16 cm) in thickness.

(6) *A set of four PVC splice couplings.* PVC splice couplings can be positioned inside a turtle's mouth to allow access to the back of the mouth for hook and line removal. They are to be held in place with the needle-nose pliers. To ensure proper fit and access, a required set must consist of the following Schedule 40 PVC splice coupling sizes: 1 inch (2.54 cm), $1\frac{1}{4}$ inches (3.18 cm), $1\frac{1}{2}$ inches (3.81 cm), and 2 inches (5.08 cm).

(7) *A large avian oral speculum.* A large avian oral speculum provides the ability to hold a turtle's mouth open and to control the head with one hand, while removing a hook with the other hand. The avian oral speculum must be 9 inches (22.86 cm) long and constructed of three-sixteenths-inch (4.76-mm) wire diameter surgical stainless steel (Type 304). It must be covered with 8 inches (20.32 cm) of clear vinyl tubing (five-sixteenths-inch (7.94-mm) outside diameter, three-sixteenths-inch (4.76-mm) inside diameter), friction tape, or similar material to pad the surface.

(M) * * *

(1) *Turtle tether and extended reach handle.* Approximately 15–20 ft (4.57–6.10 m) of half-inch (1.27 cm) hard lay negative buoyancy line or similar is used to make an approximately 30-inch (76.2-cm) loop to slip over the flipper. The line is fed through a three-quarter-inch (1.91-cm) inside diameter fair lead, eyelet, or eyebolt at the working end of

a pole and through a three-quarter-inch (1.91-cm) eyelet or eyebolt in the midsection. A half-inch (1.27-cm) quick release cleat holds the line in place near the end of the pole. A final three-quarter-inch (1.91-cm) eyelet or eyebolt should be positioned approximately 7 inches (17.78 cm) behind the cleat to secure the line, while allowing a safe working distance to avoid injury when releasing the line from the cleat. The line must be securely fastened to an extended reach handle or pole with a minimum length equal to, or greater than, 150 percent of the height of the vessel's freeboard, or a minimum of 6 ft (1.83 m), whichever is greater. There is no restriction on the type of material used to construct this handle, as long as it is sturdy. The handle must include a tag line to attach the tether to the vessel to prevent the turtle from breaking away with the tether still attached.

(2) *Ninja sticks and extended reach handles.* Approximately 30–35 ft (9.14–10.67 m) of one-half to five-eighths of an inch (1.27–1.59 cm) of soft lay polypropylene line, nylon line or similar line is fed through 2 PVC conduit, fiberglass, or similar sturdy poles and knotted using an overhand (recommended) knot at the end of both poles or otherwise secured. There should be approximately 18–24 inches (45.72–60.96 cm) of exposed rope between the poles to be used as a working surface to capture and secure the flipper. Knot the line at the ends of both poles to prevent line slippage if they are not otherwise secured. The remaining line is used to tether the apparatus to the boat unless an additional tag line is used. Two lengths of sunlight resistant three-quarter-inch (1.91-cm) schedule 40 PVC electrical conduit, fiberglass, aluminum, or similar material should be used to construct the apparatus with a minimum length equal to, or greater than, 150 percent of the height of the vessel's freeboard, or 6 ft (1.83 m), whichever is greater.

(ii) * * *

(A) *Sea turtle bycatch mitigation gear and protocols.* Sea turtle bycatch mitigation gear, as required by paragraphs (c)(5)(i)(A) through (D) of this section, must be used to disengage any hooked or entangled sea turtles that cannot be brought on board. Sea turtle bycatch mitigation gear, as required by paragraphs (c)(5)(i)(E) through (M) of this section, must be used to facilitate access, safe handling, disentanglement, and hook removal or hook cutting of sea turtles that can be brought on board, where feasible. Sea turtles must be handled, and bycatch mitigation gear must be used, in accordance with the

careful release protocols and handling/release guidelines specified in paragraphs (c)(5)(ii)(B) and (C) of this section, and in accordance with the onboard handling and resuscitation requirements specified in 50 CFR 223.206(d)(1).

(B) *Boated turtles.* When practicable, active and unresponsive sea turtles must be brought on board, with a minimum of injury, using a dipnet, collapsible hoop net, or turtle hoist, as required by paragraph (c)(5)(i)(E) of this section. All turtles less than 3 ft (91.44 cm) carapace length must be boated, if sea conditions permit. Turtles must be lifted and carried by holding the front and back of the carapace (shell) or by holding the shell by both sides. A turtle must be cradled while holding the shell and base of the flippers. A turtle must never be lifted or dragged by the flippers when it is brought on board, handled on deck, or released.

(1) *Preparation for gear and hook removal.* A boated turtle must be placed on a device that effectively cushions and supports a sea turtle while it is on board, as described in paragraph (c)(5)(i)(F) of this section. The turtle must be in an upright orientation to immobilize it and facilitate gear removal. Then, it should be determined if the hook can be removed without causing further injury.

(2) *External hook removal.* All externally embedded hooks must be removed, unless hook removal would result in further injury to the turtle. No attempt to remove a hook should be made if it has been swallowed and the insertion point is not visible, or if it is determined that removal would result in further injury.

(3) *Irremovable hook protocol.* If a hook cannot be removed, as much line as possible must be removed from the turtle using monofilament cutters as required by paragraph (c)(5)(i)(K) of this section, and the hook should be cut as close as possible to the insertion point before releasing the turtle, using bolt cutters as required by paragraph (c)(5)(i)(J) of this section.

(4) *Removable hook protocol.* If a hook can be removed, an effective technique may be to cut off either the barb, or the eye, of the hook using bolt cutters, and then to slide the hook out. When the hook is visible in the front of the mouth, a mouth-opener, as required by paragraph (c)(5)(i)(L) of this section, may facilitate opening the turtle's mouth and a gag may facilitate keeping the mouth open. Short-handled dehookers for internal hooks, long-nose pliers, or needle-nose pliers, as required by paragraphs (c)(5)(i)(G) through (I) of this section, should be used to remove

visible hooks from the mouth that have not been swallowed, as appropriate.

(5) *Gear removal.* As much gear as possible must be removed from the turtle without causing further injury prior to its release. Refer to the careful release protocols and handling/release guidelines required in this paragraph (c)(5)(ii)(B), and the handling and resuscitation requirements specified in 50 CFR 223.206(d)(1), for additional information.

(C) *Non-boated turtles.* If a sea turtle is too large, or hooked in a manner that precludes safe boating without causing further damage or injury to the turtle, sea turtle bycatch mitigation gear required by paragraphs (c)(5)(i)(A) through (D) of this section must be used to disentangle sea turtles from fishing gear and disengage any hooks, or to clip the line and remove as much line as possible from a hook that cannot be removed, prior to releasing the turtle, in accordance with the protocols specified in this paragraph.

(1) *Preparation for hook removal.* Non-boated turtles should be brought close to the boat and provided with time to calm down. Then, it must be determined whether the hook can be removed without causing further injury. A front flipper or flippers of the turtle must be secured with an approved turtle control device from the list specified in paragraph (c)(5)(i)(M) of this section.

(2) *Hook removal protocol.* All externally embedded hooks must be removed, unless hook removal would result in further injury to the turtle. No attempt should be made to remove a hook if it has been swallowed, or if it is determined that removal would result in further injury. If the hook cannot be removed and/or if the animal is entangled, as much line as possible must be removed prior to release, using a line cutter as required by paragraph (c)(5)(i)(K) of this section. If the hook can be removed, it must be removed using a long-handled dehooker as required by paragraph (c)(5)(i) of this section.

(3) *Gear removal.* Without causing further injury, as much gear and line as possible must be removed from the turtle prior to its release. Refer to the careful release protocols and handling/release guidelines required in this paragraph (c)(5)(ii)(C), and the handling and resuscitation requirements specified in 50 CFR 223.206(d)(1) for additional information.

(iii) *Gear modifications.* The following measures are required of vessel owners and operators to reduce the incidental capture and mortality of sea turtles:

* * * * *

(d) * * *

(2) The owner and operator of a vessel required to be permitted under this part and that has bottom longline gear on board must undertake the following bycatch mitigation measures:

* * * * *

[FR Doc. 2024-24870 Filed 10-28-24; 8:45 am]

BILLING CODE 3510-22-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 648

[Docket No. 241022-0277]

RIN 0648-BN02

Fisheries of the Northeastern United States; Framework Adjustment 16 to the Mackerel, Squid, and Butterfish Fishery Management Plan

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Final rule.

SUMMARY: NMFS approves and implements Framework Adjustment 16 to the Mackerel, Squid, and Butterfish Fishery Management Plan. Framework Adjustment 16 was developed by the Mid-Atlantic Fishery Management Council to establish a volumetric vessel hold capacity baseline for limited access *Illex* squid vessels, allow NMFS to collect information on vessel processing type from limited access *Illex* and Tier 1 longfin squid vessels, and clarify existing *Illex* squid reporting requirements. This action is necessary to restrict future increases in capacity in the *Illex* squid fishery and gain more accurate catch information to inform stock assessments.

DATES: Effective November 29, 2024, except for instruction 3 amending §§ 648.4(a)(5)(ii)(F), 648.4(a)(5)(ii)(H), and 648.4(c)(2)(viii), which is effective November 28, 2025.

ADDRESSES: Copies of Framework Adjustment 16, including the preliminary Regulatory Impact Review and the Regulatory Flexibility Act Analysis prepared by the Mid-Atlantic Fishery Management Council, are available from Dr. Christopher M. Moore, Executive Director, Mid-Atlantic Fishery Management Council, Suite 201, 800 North State Street, Dover, DE 19901. The document is also accessible via the internet at <https://www.mafmc.org/supporting-documents>.

Copies of the small entity compliance guide are available from Michael Pentony, Regional Administrator, NMFS, Greater Atlantic Regional Fisheries Office, 55 Great Republic Drive, Gloucester, MA 01930-2298, or via the internet at <https://www.greateratlantic.fisheries.noaa.gov>.

FOR FURTHER INFORMATION CONTACT:

Maria Fenton, Fishery Policy Analyst, (978) 281-9196, or maria.fenton@noaa.gov.

SUPPLEMENTARY INFORMATION:

Background

The Mid-Atlantic Fishery Management Council adopted Framework Adjustment 16 to the Mackerel, Squid, and Butterfish Fishery Management Plan (FMP) during its October 2023 meeting. This action was initiated following NMFS' September 7, 2022, disapproval of Amendment 22 to the Mackerel, Squid, and Butterfish FMP. The purpose of Amendment 22 was to better align fleet capacity with current quotas by creating a tiered permit system for the current limited access *Illex* squid permits to remove latent effort from the fishery. Amendment 22 was developed in response to an overall increase in the number of active limited access *Illex* vessels, which had no trip limits, and a perceived increase in racing to fish during the weeks leading up to *Illex* fishery closures since 2017. To address these issues, Amendment 22 proposed reallocating existing *Illex* squid limited access permits through tiered permitting measures. NMFS' review of Amendment 22 determined that the record supporting the Council's proposal was not adequate or sufficient to support a decision to further restrict the number and types of permits in the *Illex* fishery in light of the Magnuson-Stevens Fishery Conservation and Management Act's (Magnuson-Stevens Act) National Standards. Amendment 22's stated purpose and need, and the goals and objectives of the FMP. Following the disapproval of Amendment 22, the Council considered alternative measures to address potential latent effort in the *Illex* fishery through Framework 16.

Approved Measures

This action approves the management measures recommended in Framework Adjustment 16 to the Mackerel, Squid, and Butterfish FMP. The measures implemented in this final rule are:

1. Volumetric Hold Baseline for Limited Access *Illex* Squid Vessels

Section 303(b)(4) of the Magnuson-Stevens Act allows for provisions in an

FMP that limit the type and quantity of vessels participating in a fishery, for conservation and management purposes. This action establishes a volumetric vessel hold capacity baseline for limited access *Illex* squid vessels in order to restrict future increases in capacity in the fishery. This baseline will be required in addition to the standard length and horsepower baselines that are mandatory for all Federal limited access permits in the Greater Atlantic Region.

In order to establish its volumetric hold baseline, a limited access *Illex* squid vessel's fish hold capacity measurement must be certified by a qualified individual or entity as specified at 50 CFR 648.4(a)(5)(ii)(H)(1). Limited access *Illex* squid vessels must submit a fish hold capacity measurement, along with a signed certification by the qualified individual or entity, to NMFS within 395 days of the publication of this final rule. A similar volumetric hold baseline was implemented for Tier 1 and Tier 2 Atlantic mackerel permit holders through Amendment 11 to the Mackerel, Squid, and Butterfish FMP (76 FR 68642, November 7, 2011). If a vessel already has a volumetric hold baseline related to a Tier 1 or Tier 2 mackerel permit, that baseline could be used for its limited access *Illex* squid permit as well, and no new survey is required.

If a limited access *Illex* squid permit is in Confirmation of Permit History (CPH) when fish hold capacity measurements are due, the default volumetric hold baseline for that CPH permit will be established based on the fish hold capacity measurement of the first replacement vessel greater than 20 feet (ft) (6.09 meters (m)) after the permit is removed from CPH (at which point the vessel's fish hold would have to be measured consistent with the requirements at § 648.4(a)(5)(ii)(H)(1) before the vessel could fish under the permit). If a permit in CPH already had an existing fish hold capacity measurement from the vessel immediately preceding the permit's placement into CPH that met the certification requirements, that measurement could be used to establish a volumetric hold baseline for the *Illex* squid permit during the implementation period.

If a limited access *Illex* squid vessel is upgraded (through refitting or replacement), the upgraded vessel's volumetric hold capacity cannot exceed its volumetric hold baseline by more than 10 percent. The modified fish hold, or the fish hold of the replacement vessel, must be surveyed by a qualified

surveyor, as described at § 648.4(a)(5)(ii)(H), unless the replacement vessel already has an appropriate fish hold capacity measurement on file with NMFS, in which case no new survey is required.

2. Limited Access *Illex* and Longfin Squid Processing Type

Section 303(a)(5) of the Magnuson-Stevens Act requires FMPs to specify the pertinent data that shall be submitted to the Secretary with respect to commercial, recreational, charter fishing, and fish processing in the fishery. This action authorizes NMFS to collect information on processing type (e.g., frozen at-sea, refrigerated sea water, fresh/iced) from vessels issued a limited access *Illex* or Tier 1 longfin squid permit. Vessel processing type information will be collected annually during the permit renewal process as described at § 648.4(c)(2)(ix), beginning in permit year 2025 (starting January 1, 2025). This information will help scientists analyze the catch per unit effort (CPUE) in the *Illex* and longfin squid fisheries, which will improve the monitoring and management of these fisheries.

3. Clarifications to Existing *Illex* Squid Vessel Reporting Requirements

Section 305(d) of the Magnuson-Stevens Act requires the Secretary to promulgate regulations necessary to carry out any FMP, FMP amendment, or other provision of the Magnuson-Stevens Act. This action clarifies an existing requirement that limited access *Illex* squid vessels are required to submit daily vessel monitoring system (VMS) catch reports while on declared *Illex* squid trips, as described at § 648.7(b)(3)(iv).

Comments and Responses

We received nine public comments on the Framework Adjustment 16 proposed rule during the public comment period: One from Seafreeze Ltd.; four from the Town Dock; one from Lund's Fisheries; and three from members of the public. Consolidated responses are provided to similar comments on the proposed measures.

Limited Access *Illex* Squid Vessel Volumetric Hold Baseline

Comment 1: Two commenters (Seafreeze Ltd. and Lund's Fisheries) supported the proposed measure establishing a volumetric hold baseline for limited access *Illex* squid vessels. Seafreeze Ltd. stated that establishing a volumetric hold baseline will help prevent speculative entry and activation of latent effort (from smaller-capacity

vessels onto larger-capacity vessels) in the *Illex* squid fishery. Seafreeze Ltd. also explained that many existing participants in the *Illex* squid fishery hold Tier 1 or Tier 2 mackerel permits with associated hold capacity baselines, but new entrants often do not. Therefore, because those new vessels do not have an existing baseline limiting hold expansion, their entry into the fishery could significantly increase fleet capacity. Lund's Fisheries stated that establishing a volumetric hold baseline for limited access *Illex* squid vessels would be a good first step towards freezing the footprint of the fishery and matching harvesting capacity to resource availability. Lund's Fisheries also noted that in its experience, certified hold measurements can be obtained at a reasonable cost, and would provide the Council with important effort information. Lund's Fisheries was also supportive of the flexibility given to permits in CPH being able to use an existing fish hold measurement from a previous vessel to establish that permit's hold capacity baseline.

Response 1: We agree and are approving and implementing the measure as proposed.

Comment 2: Seven commenters (four from the Town Dock and three members of the public) opposed the implementation of a volumetric hold baseline for limited access *Illex* squid vessels. Six commenters (three from the Town Dock and three members of the public) felt that the establishment of this baseline was redundant and unnecessary, given that limited access permits in the Greater Atlantic Region already have length and horsepower baselines and with associated upgrade restrictions. Five commenters (three from the Town Dock and one member of the public) stated that adding a hold capacity baseline will make it more difficult for permit holders to upgrade aging vessels in the future, as finding replacement vessels that fits the existing length and horsepower baselines is already challenging.

Response 2: We have considered this comment and disagree that establishing a volumetric hold baseline for limited access *Illex* squid vessels is unnecessary. While it is true that Greater Atlantic Region limited access permits are already subject to length and horsepower baselines and upgrade restrictions, due to the high volume nature of the *Illex* fishery, a vessel's fishing capacity can be significantly increased via hold modification while staying within its length and horsepower requirements. This is why the Council chose to pursue hold capacity restrictions as a tool to cap

fishing power in the *Illex* fishery and we are implementing the measure as proposed. We acknowledge that accommodating a third baseline may make it more difficult to find replacement vessels in the future, but the overall benefits to the fleet resulting from the establishment of a volumetric hold baseline outweigh this challenge.

Comment 3: Three commenters from the Town Dock commented that overfishing of *Illex* squid is not occurring, and only a relatively small percentage of the quota has been harvested in recent years. Commenters stated that this indicates that there is not an overcapacity issue in the fishery, and wondered why additional restrictions on hold capacity are necessary. Similarly, one member of the comment questioned why this measure is necessary given that the *Illex* commercial quota has increased in recent years.

Response 3: The statement that overfishing of the *Illex* squid stock is not occurring requires some clarification. The 2022 *Illex* squid management track assessment was unable to make overfishing or overfished determinations for the stock because there are no reference points or accepted methods for estimating fishing mortality rate and biomass. As a result, the stock status is unknown.

It is true that in recent years the *Illex* squid acceptable biological catch (ABC) has increased (from 30,000 mt in 2020 to 40,000 mt in 2023), and a relatively small percentage of the domestic annual harvest (DAH) has been caught annually in the last few years (15 percent in 2022 and 14 percent in 2023). However, during 2019–2021, data indicate that 98–113 percent of the *Illex* squid DAH was caught. Further, when resource abundance was high during 2017–2019, the number of active vessels participating in the fishery increased, landings in the weeks leading up to closures increased, and landings per active vessel declined. In response to these findings, the Council developed the volumetric hold baseline measure to help freeze the footprint of the *Illex* squid fishery and curb further increases in fishing capacity, and we are implementing the measure as proposed.

Comment 4: Several commenters (four from the Town Dock and three members of the public) referenced the estimated costs associated with implementing a vessel hold capacity baseline, explaining that this will be burdensome to vessel owners. Four commenters (three from the Town Dock and one member of the public) explained that recent poor harvest of *Illex* and longfin squid has already put the fleet under

financial strain, which will make it even more difficult to pay to obtain certified hold measurements. One commenter from the Town Dock estimated that it could cost more than \$30,000 to get their vessels measured, and explained that other recent increases in business expenses (e.g., fuel, labor, insurance) will make these costs more difficult to accommodate.

Response 4: While the economic impact of complying with the volumetric hold baseline may be substantial for some participants in the *Illex* squid fishery, we considered the nature and extent of these costs relative to the benefits of the measure. We also attempted to minimize the costs to the fleet by giving permit holders the flexibility to use existing certified hold measurements (e.g., from a Tier 1 or Tier 2 mackerel permit, from a vessel prior to a permit going into CPH) to establish the volumetric hold baseline for their limited access *Illex* squid permit.

Limited Access Illex and Tier 1 Longfin Squid Processing Type

Comment 5: Lund's Fisheries opposed allowing NMFS to collect information about processing type from limited access *Illex* and Tier 1 longfin squid vessels, stating that this information is already recorded through the Northeast Fisheries Science Center's Study Fleet program and has already been used by scientists in recent stock assessments.

Response 5: We disagree that processing type information is already readily available for the *Illex* and longfin squid fisheries. Study Fleet program data, including processing type information, was used in the 2022 *Illex* squid research track assessment to calculate CPUE information for the "wet" and "freezer" components of the fleet. The assessment report states that the data collected through the Study Fleet program appear to be fairly representative of the wet boat portion of the fleet, but the utility of the data for calculating CPUE for the freezer boat portion is limited due to the fact that only one freezer vessel participates. Authorizing NMFS to collect processing type information from all limited access *Illex* and Tier 1 longfin squid vessels will help fill this data gap and improve scientists' ability to calculate CPUE for all components of both fisheries. Additionally, because this information will be collected through a single question on a vessel application that is already required annually, we expect there to be negligible added burden to the fleet resulting from this measure.

Clarifications to Existing Illex Squid Vessel Reporting Requirements

Comment 6: Lund's Fisheries supported the proposed clarifications to existing *Illex* squid vessel reporting requirements.

Response 6: NMFS agrees and is approving and implementing the clarification as proposed.

Changes From the Proposed Rule

There are no changes from the proposed rule.

Classification

NMFS is issuing this rule pursuant to sections 304(b) and 305(d) of the Magnuson-Stevens Act. The NMFS Assistant Administrator has determined that this final rule is consistent with the Mackerel, Squid, and Butterfish FMP, other provisions of the Magnuson-Stevens Act, and other applicable law.

This final rule has been determined to be not significant for purposes of Executive Order (E.O.) 12866.

This final rule does not contain policies with federalism or takings implications as those terms are defined in E.O. 13132 and E.O. 12630, respectively.

The Chief Counsel for Regulation of the Department of Commerce certified to the Chief Counsel for Advocacy of the Small Business Administration during the proposed rule stage that this action would not have a significant economic impact on a substantial number of small entities. The factual basis for the certification was published in the proposed rule and is not repeated here. As a result, a final regulatory flexibility analysis was not required and none was prepared.

This final rule contains collection-of-information requirements subject to review and approval by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA). This rule revises the existing requirements for the collection of information OMB Control No. 0648-0202, Greater Atlantic Region Permit Family of Forms, by requiring limited *Illex* squid vessels obtain a vessel hold measurement and submit that documentation to NMFS. There are 46 limited access *Illex* squid permits that do not currently have a vessel hold measurement on file with NMFS; the remaining *Illex* squid permits already have a vessel hold measurement on file due to the same requirement for their Tier 1 or Tier 2 Atlantic mackerel permit. The burden estimate for verifying vessel specifications is 3 hours per vessel therefore the total burden hours would be 138 hours. The hourly

wage rate is \$33.78, which would result in a wage burden increase of \$4,661.64 (138 hours × \$33.78).

Vessel processing type information will be collected through an existing permit renewal form and will add a negligible additional burden amounting to no cost; therefore, it does not need additional approval through the PRA. The costs and burden hours for daily VMS reporting in the *Illex* squid fishery have already been calculated and received public comments through a previous action. Therefore, the changes in this final rule are simply a clarification of existing regulatory requirements and do not need additional approval through the PRA.

Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA, unless that collection of information displays a currently valid OMB Control Number.

List of Subjects in 50 CFR Part 648

Fisheries, Fishing, Reporting and recordkeeping requirements.

Dated: October 22, 2024.

Samuel D. Rauch, III,

Deputy Assistant Administrator for Regulatory Programs, National Marine Fisheries Service.

For the reasons set out in the preamble, NMFS amends 50 CFR part 648 as follows:

PART 648—FISHERIES OF THE NORTHEASTERN UNITED STATES

■ 1. The authority citation for part 648 continues to read as follows:

Authority: 16 U.S.C. 1801 *et seq.*

■ 2. Amend § 648.4 by adding paragraph (c)(2)(viii) and (ix) to read as follows:

§ 648.4 Vessel permits.

* * * * *

(c) * * *

(viii) [Reserved]

(ix) An application for limited access *Illex* squid and Tier 1 longfin squid permit must also contain the primary vessel processing type for the coming fishing year.

* * * * *

■ 3. Effective November 28, 2025, further amend § 648.4 by revising paragraphs (a)(5)(ii)(F) and (H) and adding paragraph (c)(2)(viii) to read as follows:

§ 648.4 Vessel permits.

(a) * * *

(5) * * *

(ii) * * *

(F) *Upgraded vessel*. See paragraph (a)(1)(i)(F) of this section. In addition for moratorium *Illex* squid permits, the upgraded vessel's volumetric hold capacity may not exceed by more than 10 percent the volumetric fish hold capacity of the vessel's baseline specifications. The modified fish hold, or the fish hold of the replacement vessel, must be surveyed by a surveyor (accredited as in paragraph (a)(5)(ii)(H) of this section) and submitted to NMFS unless the replacement vessel already had an appropriate certification.

* * * * *

(H) *Vessel Baseline specifications*. (1) The volumetric fish hold capacity of vessels with an *Illex* squid moratorium permit will be considered a vessel baseline specification in addition to the baseline specifications set forth in paragraph (a)(3)(i)(H) of this section. Volumetric fish hold capacity for vessels with moratorium *Illex* squid permit must be established not later than November 28, 2025 if not previously established as specified in paragraphs (a)(5)(ii)(H)(2) of this section. The fish hold capacity measurement must be certified by one of the following qualified individuals or entities: An individual credentialed as a Certified Marine Surveyor with a fishing specialty by the National Association of Marine Surveyors (NAMS); an individual credentialed as an Accredited Marine Surveyor with a fishing specialty by the Society of Accredited Marine Surveyors (SAMS); employees or agents of a classification society approved by the Coast Guard pursuant to 46 U.S.C. 3316(c); the Maine State Sealer of Weights and Measures; a professionally-licensed and/or registered Marine Engineer; or a Naval Architect with a professional engineer

license. The fish hold capacity measurement submitted to NMFS as required in this paragraph (a)(5)(ii)(H)(1) must include a signed certification by the individual or entity that completed the measurement, specifying how they meet the definition of a qualified individual or entity. If the vessel's permit suite does not include a Tier 1 or Tier 2 limited access Atlantic mackerel permit for which a volumetric fish hold capacity baseline has been established, the permit is not in CPH, or the volumetric hold measurement is not submitted as established by the date listed above, the subsequent moratorium *Illex* squid permit renewal application may be deemed incomplete until the volumetric hold measurement has been established.

(2) If an *Illex* squid vessel already possesses a volumetric hold baseline related to its Tier 1 or Tier 2 limited access Atlantic mackerel permit as specified in paragraph (a)(3)(iii)(H)(1), that measurement could be applied as a baseline specification for its *Illex* squid moratorium permit.

(3) If an *Illex* squid permit in CPH has an existing volumetric hold measurement pursuant to paragraph (a)(5)(ii)(H)(1) of this section for the vessel immediately preceding the permit's placement into CPH, that volumetric hold measurement may be used to establish a vessel hold baseline specification not later than November 28, 2025. In the alternative, if an *Illex* squid permit is in CPH, the volumetric hold capacity baseline may be the hold capacity of the first replacement vessel greater than 20 ft (6.09 m) after the permits are removed from CPH. Hold capacity for the replacement vessel must be measured pursuant to paragraph (a)(5)(ii)(H)(1) of this section.

* * * * *

(c) * * *

(2) * * *

(viii) The owner of a vessel that has been issued a limited access *Illex* squid permit must submit a volumetric hold certification measurement, as described paragraph (a)(5)(ii)(H) of this section, otherwise the permit application for 2026 will be considered incomplete.

* * * * *

■ 4. In § 648.7, add paragraph (b)(3)(iv) to read as follows:

§ 648.7 Record keeping and reporting requirements.

* * * * *

(b) * * *

(3) * * *

(iv) *Illex* squid moratorium permit owners or operators. The owner or operator of a vessel issued an *Illex* squid moratorium permit must report catch (retained and discarded of *Illex* squid daily via VMS, unless exempted by the Regional Administrator. The report must include at least the following information, and any other information required by the Regional Administrator: Electronic Vessel Trip Report Trip Identifier; month, day, and year *Illex* squid was caught; total pounds of *Illex* squid retained and total pounds of all fish retained. Daily *Illex* squid VMS catch reports must be submitted in 24-hr intervals for each day and must be submitted by 0900 hr on the following day. Reports are required even if *Illex* squid caught that day have not yet been landed. This report does not exempt the owner or operator from other applicable reporting requirements of this section.

* * * * *

[FR Doc. 2024-24928 Filed 10-28-24; 8:45 am]

BILLING CODE 3510-22-P

Proposed Rules

Federal Register

Vol. 89, No. 209

Tuesday, October 29, 2024

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

NUCLEAR REGULATORY COMMISSION

10 CFR Parts 50 and 52

[NRC-2024-0161]

Draft Regulatory Guide: Qualification of Fiber-Optic Cables, Connections, and Optical Fiber Splices for Use in Safety Systems for Production and Utilization Facilities

AGENCY: Nuclear Regulatory Commission.

ACTION: Draft guide; request for comment.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is issuing for public comment a draft Regulatory Guide (DG), DG-1427, “Qualification of Fiber-Optic Cables, Connections, and Optical Fiber Splices for Use in Safety Systems for Production and Utilization Facilities.” DG-1427 is newly proposed Revision 0 of Regulatory Guide (RG) 1.257 and describes an approach that is acceptable to the staff of the NRC for use in complying with NRC regulations that address the environmental qualification of fiber-optic cables, connections, and optical fiber splices in safety systems in production and utilization facilities.

DATES: Submit comments by November 29, 2024. Comments received after this date will be considered if it is practical to do so, but the NRC is able to ensure consideration only for comments received on or before this date.

ADDRESSES: You may submit comments by any of the following methods; however, the NRC encourages electronic comment submission through the Federal rulemaking website.

- *Federal rulemaking website:* Go to <https://www.regulations.gov> and search for Docket ID NRC-2024-0161. Address questions about Docket IDs in *Regulations.gov* to Stacy Schumann; telephone: 301-415-0624; email: Stacy.Schumann@nrc.gov. For technical questions, contact the individuals listed in the **FOR FURTHER INFORMATION CONTACT** section of this document.

- *Mail comments to:* Office of Administration, Mail Stop: TWFN-7-A60M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Program Management, Announcements and Editing Staff.

For additional direction on obtaining information and submitting comments, see “Obtaining Information and Submitting Comments” in the **SUPPLEMENTARY INFORMATION** section of this document.

FOR FURTHER INFORMATION CONTACT:

Sheila Ray, Office of Nuclear Reactor Regulation, telephone: 301-415-3653; email: Sheila.Ray@nrc.gov and Vance Petrella, Office of Nuclear Regulatory Research, telephone: 301-415-1048; email: Vance.Petrella@nrc.gov. Both are staff of the U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

SUPPLEMENTARY INFORMATION:

I. Obtaining Information and Submitting Comments

A. Obtaining Information

Please refer to Docket ID NRC-2024-0161 when contacting the NRC about the availability of information for this action. You may obtain publicly available information related to this action by any of the following methods:

- *Federal Rulemaking Website:* Go to <https://www.regulations.gov> and search for Docket ID NRC-2024-0161.

- *NRC's Agencywide Documents Access and Management System (ADAMS):* You may obtain publicly available documents online in the ADAMS Public Documents collection at <https://www.nrc.gov/reading-rm/adams.html>. To begin the search, select “Begin Web-based ADAMS Search”. For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, at 301-415-4737, or by email to PDR.Resource@nrc.gov. DG-1427, “Qualification of Fiber-Optic Cables, Connections, and Optical Fiber Splices for Use in Safety Systems for Production and Utilization Facilities,” is available in ADAMS under Accession No. ML24201A068.

- *NRC's PDR:* The PDR, where you may examine and order copies of publicly available documents, is open by appointment. To make an appointment to visit the PDR, please send an email to PDR.Resource@nrc.gov

or call 1-800-397-4209 or 301-415-4737, between 8 a.m. and 4 p.m. eastern time (ET), Monday through Friday, except Federal holidays.

B. Submitting Comments

The NRC encourages electronic comment submission through the Federal rulemaking website (<https://www.regulations.gov>). Please include Docket ID NRC-2024-0161 in your comment submission.

The NRC cautions you not to include identifying or contact information that you do not want to be publicly disclosed in your comment submission. The NRC will post all comment submissions at <https://www.regulations.gov> as well as enter the comment submissions into ADAMS. The NRC does not routinely edit comment submissions to remove identifying or contact information.

If you are requesting or aggregating comments from other persons for submission to the NRC, then you should inform those persons not to include identifying or contact information that they do not want to be publicly disclosed in their comment submission. Your request should state that the NRC does not routinely edit comment submissions to remove such information before making the comment submissions available to the public or entering the comment into ADAMS.

II. Additional Information

The NRC is issuing for public comment a DG in the NRC's “Regulatory Guide” series. This series was developed to describe methods that are acceptable to the NRC staff for implementing specific parts of the NRC's regulations, to explain techniques that the staff uses in evaluating specific issues or postulated events, and to describe information that the staff needs in its review of applications for permits and licenses.

The DG, entitled “Qualification of Fiber-Optic Cables, Connections, and Optical Fiber Splices for Use in Safety Systems for Production and Utilization Facilities,” is temporarily identified by its task number, DG-1427, and describes an approach that is acceptable to the NRC staff for use in complying with NRC regulations that address the environmental qualification of fiber-optic cables, connections, and optical fiber splices in safety systems in production and utilization facilities.

DG-1427 is newly proposed Revision 0 of RG 1.257 and endorses, subject to the conditions described in Section C of this DG, the Institute of Electrical and Electronics Engineers Standard 1682-2023, which provides methods, directions, and documentation for the qualification of fiber optic cables, connections, and optical fiber splices in safety systems of production and utilization facilities.

The staff is also issuing for public comment a draft regulatory analysis (ADAMS Accession No. ML24201A069). The staff developed a regulatory analysis to assess the value of issuing or revising an RG as well as alternative courses of action.

As noted in the **Federal Register** on December 9, 2022 (87 FR 75671), this document is being published in the "Proposed Rules" section of the **Federal Register** to comply with publication requirements under chapter I of title 1 of the *Code of Federal Regulations* (CFR).

III. Backfitting, Forward Fitting, and Issue Finality

Issuance of DG-1427, if finalized, would not constitute backfitting as defined in 10 CFR 50.109, "Backfitting," and as described in NRC Management Directive (MD) 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests"; does not affect issue finality of any approval issued under 10 CFR part 52, "Licenses, Certificates, and Approvals for Nuclear Power Plants"; nor constitute forward fitting as defined in MD 8.4, because, as explained in this DG, licensees would not be required to comply with the positions set forth in this DG.

IV. Submitting Suggestions for Improvement of Regulatory Guides

A member of the public may, at any time, submit suggestions to the NRC for improvement of existing RGs or for the development of new RGs. Suggestions can be submitted on the NRC's public website at <https://www.nrc.gov/reading-rm/doc-collections/reg-guides/contactus.html>. Suggestions will be considered in future updates and enhancements to the "Regulatory Guide" series.

Dated: October 23, 2024.

For the Nuclear Regulatory Commission

Stanley Gardocki,

Acting Chief, Regulatory Guide and Programs Management Branch, Division of Engineering, Office of Nuclear Regulatory Research.

[FR Doc. 2024-25038 Filed 10-28-24; 8:45 am]

BILLING CODE 7590-01-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA-2024-2414; Project Identifier MCAI-2024-00530-E]

RIN 2120-AA64

Airworthiness Directives; Rolls-Royce Deutschland Ltd & Co KG

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: The FAA proposes to adopt a new airworthiness directive (AD) for all Rolls-Royce Deutschland Ltd & Co KG Model Trent 1000-AE3, Trent 1000-CE3, Trent 1000-D3, Trent 1000-G3, Trent 1000-H3, Trent 1000-J3, Trent 1000-K3, Trent 1000-L3, Trent 1000-M3, Trent 1000-N3, Trent 1000-P3, Trent 1000-Q3, Trent 1000-R3, Trent 7000-72, and Trent 7000-72C engines. This proposed AD was prompted by reports of cracked intermediate pressure compressor (IPC) shaft assembly front air seals. This proposed AD would require an inspection of the affected IPC shaft assembly for cracking and, depending on the results of the inspection, repetitive inspections or replacement of the IPC shaft assembly front air seals, as specified in a European Union Aviation Safety Agency (EASA) AD, which is incorporated by reference. The FAA is proposing this AD to address the unsafe condition on these products.

DATES: The FAA must receive comments on this NPRM by December 13, 2024.

ADDRESSES: You may send comments, using the procedures found in 14 CFR 11.43 and 11.45, by any of the following methods:

- **Federal eRulemaking Portal:** Go to [regulations.gov](https://www.regulations.gov). Follow the instructions for submitting comments.
- **Fax:** (202) 493-2251.
- **Mail:** U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590.

- **Hand Delivery:** Deliver to Mail address above between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

AD Docket: You may examine the AD docket at [regulations.gov](https://www.regulations.gov) under Docket No. FAA-2024-2414; or in person at Docket Operations between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The AD docket contains this NPRM, the mandatory

continuing airworthiness information (CAI), any comments received, and other information. The street address for Docket Operations is listed above.

Material Incorporated by Reference:

- For EASA material identified in this proposed AD, contact EASA, Konrad-Adenauer-Ufer 3, 50668 Cologne, Germany; phone: +49 221 8999 000; email: ADs@easa.europa.eu; website: easa.europa.eu. You may find this material on the EASA website at ad.easa.europa.eu.

- You may view this material at the FAA, Airworthiness Products Section, Operational Safety Branch, 1200 District Avenue, Burlington, MA 01803. For information on the availability of this material at the FAA, call (817) 222-5110.

FOR FURTHER INFORMATION CONTACT:

Barbara Caufield, Aviation Safety Engineer, FAA, 2200 South 216th Street, Des Moines, WA 98198; phone: (781) 238-7146; email: barbara.caufield@faa.gov.

SUPPLEMENTARY INFORMATION:

Comments Invited

The FAA invites you to send any written relevant data, views, or arguments about this proposal. Send your comments to an address listed under **ADDRESSES**. Include "Docket No. FAA-2024-2414; Project Identifier MCAI-2024-00530-E" at the beginning of your comments. The most helpful comments reference a specific portion of the proposal, explain the reason for any recommended change, and include supporting data. The FAA will consider all comments received by the closing date and may amend this proposal because of those comments.

Except for Confidential Business Information (CBI) as described in the following paragraph, and other information as described in 14 CFR 11.35, the FAA will post all comments received, without change, to [regulations.gov](https://www.regulations.gov), including any personal information you provide. The agency will also post a report summarizing each substantive verbal contact received about this NPRM.

Confidential Business Information

CBI is commercial or financial information that is both customarily and actually treated as private by its owner. Under the Freedom of Information Act (FOIA) (5 U.S.C. 552), CBI is exempt from public disclosure. If your comments responsive to this NPRM contain commercial or financial information that is customarily treated as private, that you actually treat as private, and that is relevant or

responsive to this NPRM, it is important that you clearly designate the submitted comments as CBI. Please mark each page of your submission containing CBI as “PROPIN.” The FAA will treat such marked submissions as confidential under the FOIA, and they will not be placed in the public docket of this NPRM. Submissions containing CBI should be sent to Barbara Caufield, Aviation Safety Engineer, FAA, 2200 South 216th Street, Des Moines, WA 98198. Any commentary that the FAA receives which is not specifically designated as CBI will be placed in the public docket for this rulemaking.

Background

EASA, which is the Technical Agent for the Member States of the European Union, has issued EASA AD 2024–0178, dated September 12, 2024 (EASA AD 2024–0178) (also referred to as the MCAI), to address an unsafe condition for all Model Trent 1000–AE3, Trent 1000–CE3, Trent 1000–D3, Trent 1000–G3, Trent 1000–H3, Trent 1000–J3, Trent 1000–K3, Trent 1000–L3, Trent 1000–M3, Trent 1000–N3, Trent 1000–P3, Trent 1000–Q3, Trent 1000–R3, Trent 7000–72, and Trent 7000–72 C engines. The MCAI states that there were reports of cracked IPC shaft assembly front air seals. Subsequent investigations identified possible change of the vibration and flutter characteristics of the affected IPC shaft assembly and identified a potential propagation of the cracking into the IPC stage 1 disc. Such cracking could lead to IPC stage 1 disk burst with consequent release of high energy debris and damage to the airplane or failure of the IPC front seal and release of debris,

which could lead to an engine in-flight shutdown (IFSD) and in the case of a dual IFSD could result in reduced control of the airplane.

You may examine the MCAI in the AD docket at *regulations.gov* under Docket No. FAA–2024–2414.

Material Incorporated by Reference Under 1 CFR Part 51

The FAA reviewed EASA AD 2024–0178, which specifies procedures for inspection of the affected IPC shaft assembly and replacement of the IPC shaft assembly front air seals. This material is reasonably available because the interested parties have access to it through their normal course of business or by the means identified in the ADDRESSES section.

FAA’s Determination

These products have been approved by the aviation authority of another country and are approved for operation in the United States. Pursuant to the FAA’s bilateral agreement with this State of Design Authority, it has notified the FAA of the unsafe condition described in the MCAI referenced above. The FAA is issuing this NPRM after determining that the unsafe condition described previously is likely to exist or develop on other products of the same type design.

Proposed AD Requirements in This NPRM

This proposed AD would require accomplishing the actions specified in the MCAI described previously, except for any differences identified as exceptions in the regulatory text of this proposed AD.

Explanation of Required Compliance Information

In the FAA’s ongoing efforts to improve the efficiency of the AD process, the FAA developed a process to use some civil aviation authority (CAA) ADs as the primary source of information for compliance with requirements for corresponding FAA ADs. The FAA has since coordinated with other manufacturers and CAAs to use this process. As a result, the FAA proposes to incorporate by reference EASA AD 2024–0178 in the FAA final rule. This proposed AD would, therefore, require compliance with EASA AD 2024–0178 in its entirety through that incorporation, except for any differences identified as exceptions in the regulatory text of this proposed AD. Using common terms that are the same as the heading of a particular section in the EASA AD does not mean that operators need comply only with that section. For example, where the AD requirement refers to “all required actions within the compliance times,” compliance with this AD requirement is not limited to the section titled “Required Action(s) and Compliance Time(s)” in EASA AD 2024–0178. Service information required by the EASA AD for compliance will be available at *regulations.gov* under Docket No. FAA–2024–2414 after the FAA final rule is published.

Costs of Compliance

The FAA estimates that this AD, if adopted as proposed, would affect 64 engines installed on airplanes of U.S. registry. The FAA estimates the following costs to comply with this proposed AD:

ESTIMATED COSTS

Action	Labor cost	Parts cost	Cost per product	Cost on U.S. operators
Inspect IPC shaft assembly	5 work-hours × \$85 per hour = \$425	\$0	\$425	\$27,200

The FAA estimates the following costs to do any necessary replacements that would be required based on the

results of the proposed inspection. The agency has no way of determining the

number of engines that might need these replacements.

ON-CONDITION COSTS

Action	Labor cost	Parts cost	Cost per product
Replace IPC shaft assembly front air seals	80 work-hours × \$85 per hour = \$6,800	\$7,000	\$13,800

Authority for This Rulemaking

Title 49 of the United States Code specifies the FAA’s authority to issue

rules on aviation safety. Subtitle I, section 106, describes the authority of the FAA Administrator. Subtitle VII:

Aviation Programs, describes in more detail the scope of the Agency’s authority.

The FAA is issuing this rulemaking under the authority described in Subtitle VII, Part A, Subpart III, Section 44701: General requirements. Under that section, Congress charges the FAA with promoting safe flight of civil aircraft in air commerce by prescribing regulations for practices, methods, and procedures the Administrator finds necessary for safety in air commerce. This regulation is within the scope of that authority because it addresses an unsafe condition that is likely to exist or develop on products identified in this rulemaking action.

Regulatory Findings

The FAA determined that this proposed AD would not have federalism implications under Executive Order 13132. This proposed AD would not have a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.

For the reasons discussed above, I certify this proposed regulation:

- (1) Is not a “significant regulatory action” under Executive Order 12866,
- (2) Would not affect intrastate aviation in Alaska, and
- (3) Would not have a significant economic impact, positive or negative, on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

List of Subjects in 14 CFR Part 39

Air transportation, Aircraft, Aviation safety, Incorporation by reference, Safety.

The Proposed Amendment

Accordingly, under the authority delegated to me by the Administrator, the FAA proposes to amend 14 CFR part 39 as follows:

PART 39—AIRWORTHINESS DIRECTIVES

- 1. The authority citation for part 39 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701.

§ 39.13 [Amended]

- 2. The FAA amends § 39.13 by adding the following new airworthiness directive:

Rolls-Royce Deutschland Ltd & Co KG:
Docket No. FAA–2024–2414; Project Identifier MCAI–2024–00530–E.

(a) Comments Due Date

The FAA must receive comments on this airworthiness directive (AD) by December 13, 2024.

(b) Affected ADs

None.

(c) Applicability

This AD applies to Rolls-Royce Deutschland Ltd & Co KG Model Trent 1000–AE3, Trent 1000–CE3, Trent 1000–D3, Trent 1000–G3, Trent 1000–H3, Trent 1000–J3, Trent 1000–K3, Trent 1000–L3, Trent 1000–M3, Trent 1000–N3, Trent 1000–P3, Trent 1000–Q3, Trent 1000–R3, Trent 7000–72, and Trent 7000–72C engines.

(d) Subject

Joint Aircraft System Component (JASC) Code 7230, Turbine Engine Compressor Section.

(e) Unsafe Condition

This AD was prompted by reports of cracked intermediate pressure compressor (IPC) shaft assembly front air seals. The FAA is issuing this AD to prevent an IPC stage 1 disk burst or failure of the IPC front seal. The unsafe condition, if not addressed, could result in an IPC stage 1 disk burst with consequent release of high energy debris and damage to the airplane or failure of the IPC front seal and release of debris, which could lead to an engine in-flight shutdown (IFSD) and in the case of a dual IFSD could result in reduced control of the airplane.

(f) Compliance

Comply with this AD within the compliance times specified, unless already done.

(g) Required Actions

Except as specified in paragraphs (h), (i), and (j) of this AD: Perform all required actions within the compliance times specified in, and in accordance with, European Union Aviation Safety Agency AD 2024–0178, dated September 12, 2024 (EASA AD 2024–0178).

(h) Exceptions to EASA AD 2024–0178

(1) Where EASA AD 2024–0178 refers to its effective date, this AD requires using the effective date of this AD.

(2) Where the service information referenced in EASA AD 2024–0178 specifies to reject the engine, this AD requires removing the affected part from service.

(3) This AD does not adopt the Remarks paragraph of EASA AD 2024–0178.

(i) No Reporting Requirement

Although the service information referenced in EASA AD 2024–0178 specifies to submit certain information to the manufacturer, this AD does not include that requirement.

(j) Alternative Methods of Compliance (AMOCs)

(1) The Manager, AIR–520 Continued Operational Safety Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or local Flight Standards District Office, as appropriate. If sending information directly to the Manager, AIR–520 Continued Operational Safety Branch, send it to the

attention of the person identified in paragraph (k) of this AD and email to: AMOC@faa.gov.

(2) Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the local flight standards district office/certificate holding district office.

(k) Additional Information

For more information about this AD, contact Barbara Caufield, Aviation Safety Engineer, FAA, 2200 South 216th Street, Des Moines, WA 98198; phone: (781) 238–7146; email: barbara.caufield@faa.gov.

(l) Material Incorporated by Reference

(1) The Director of the Federal Register approved the incorporation by reference (IBR) of the material listed in this paragraph under 5 U.S.C. 552(a) and 1 CFR part 51.

(2) You must use this material as applicable to do the actions required by this AD, unless the AD specifies otherwise.

(i) European Union Aviation Safety Agency (EASA) AD 2024–0178, dated September 12, 2024.

(ii) [Reserved]

(3) For EASA material identified in this AD, contact EASA, Konrad-Adenauer-Ufer 3, 50668 Cologne, Germany; phone: +49 221 8999 000; email: ADS@easa.europa.eu; website: easa.europa.eu. You may find this EASA AD on the EASA website at ad.easa.europa.eu.

(4) You may view this material at FAA, Airworthiness Products Section, Operational Safety Branch, 1200 District Avenue, Burlington, MA 01803. For information on the availability of this material at the FAA, call (817) 222–5110.

(5) You may view this material at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, visit www.archives.gov/federal-register/cfr/ibr-locations or email fr.inspection@nara.gov.

Issued on October 22, 2024.

Peter A. White,

Deputy Director, Integrated Certificate Management Division, Aircraft Certification Service.

[FR Doc. 2024–24964 Filed 10–28–24; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 310

[Docket ID: DoD–2024–OS–0112]

RIN 0790–AL45

Privacy Act of 1974; Implementation

AGENCY: Office of the Secretary, Department of Defense (DoD).

ACTION: Proposed rule.

SUMMARY: The Department of Defense (Department or DoD) is giving concurrent notice of a new system of

records pursuant to the Privacy Act of 1974 for the DoD–0024, “Catch a Serial Offender (CATCH) Program Records,” system of records and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of this system of records from certain provisions of the Privacy Act to avoid interference during the conduct of criminal, civil, or administrative actions or investigations; and to protect the identity of confidential sources incident involving adult sexual assault allegations.

DATES: Send comments on or before December 30, 2024.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods.

* *Federal eRulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for submitting comments.

* *Mail:* Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 05F16, Alexandria, VA 22350–1700.

Instructions: All submissions received must include the agency name and docket number or Regulation Identifier Number (RIN) for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Rahwa Keleta, OSD.DPCLTD@mail.mil, (703) 256–1408.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, the DoD is establishing a new system of records titled “Catch a Serial Offender (CATCH) Program Records,” DoD–0024. This system of records covers DoD’s maintenance of records used to collect and compare sexual assault reports for the purpose of identifying alleged serial sexual assault offenders. These records will consist of information voluntarily submitted into the CATCH system by eligible victims who elect to participate in the CATCH program and provide information about an alleged adult sexual assault incident, without identifying such victims, through established CATCH processes.

II. Privacy Act Exemption

The Privacy Act allows Federal agencies to exempt eligible records in a system of records from certain provisions of the Act, including those that provide individuals with a right to request access to and amendment of their own records. If an agency intends to exempt a particular system of records, it must first go through the rulemaking process to provide public notice and an opportunity to comment on the proposed exemption. This proposed rule explains why an exemption is being claimed for this system of records and invites public comment, which DoD will consider before the issuance of a final rule implementing the exemption.

The DoD proposes to modify 32 CFR part 310 to add a new Privacy Act exemption rule for the DoD–0024, “Catch a Serial Offender (CATCH) Program Records,” system of records. The DoD proposes to exempt this system of records because these records support the conduct of criminal law enforcement activities, and certain requirements of the Privacy Act may interfere with the effective execution of these activities. The Privacy Act, pursuant to 5 U.S.C. 552a(j)(2), authorizes agencies with a principal law enforcement function pertaining to the enforcement of criminal laws (including activities of prosecutors, courts, etc.) to claim an exemption for systems of records that contain information identifying criminal offenders and alleged offenders, information compiled for the purpose of criminal investigation, or reports compiled during criminal law enforcement proceedings. The DoD is proposing to claim exemptions from several provisions of the Privacy Act, including various access, amendment, disclosure accounting, and notice requirements, pursuant to 5 U.S.C. 552a(j)(2) to prevent the harms articulated in this rule from occurring.

A notice of a new system of records for DoD–0024, “Catch a Serial Offender (CATCH) Program Records,” is published elsewhere in this issue of the **Federal Register**.

Regulatory Analysis

Executive Order 12866, “Regulatory Planning and Review,” as Amended by Executive Order 14094, “Modernizing Regulatory Review,” and Executive Order 13563, “Improving Regulation and Regulatory Review”

Executive Orders 12866 (as amended by Executive Order 14094) and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is

necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distribute impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. It has been determined that this rule is not a significant regulatory action.

Section 202, Public Law 104–4, “Unfunded Mandates Reform Act”

Section 202(a) of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532(a)) requires agencies to assess anticipated costs and benefits before issuing any rule whose mandates may result in the expenditure by State, local, and Tribal governments in the aggregate, or by the private sector, in any one year of \$100 million in 1995 dollars, updated annually for inflation. This rule will not mandate any requirements for State, local, or Tribal governments, nor will it affect private sector costs.

Public Law 96–354, “Regulatory Flexibility Act” (5 U.S.C. Chapter 6)

The Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency has certified that this proposed rule is not subject to the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. This proposed rule is concerned only with the administration of Privacy Act systems of records within the DoD. Therefore, the Regulatory Flexibility Act, as amended, does not require DoD to prepare a regulatory flexibility analysis.

Public Law 96–511, “Paperwork Reduction Act” (44 U.S.C. Chapter 35)

The Paperwork Reduction Act (44 U.S.C. 3501 *et seq.*) was enacted to minimize the paperwork burden for individuals; small businesses; educational and nonprofit institutions; Federal contractors; State, local, and Tribal governments; and other persons resulting from the collection of information by or for the Federal Government. The Act requires agencies obtain approval from the Office of Management and Budget before using identical questions to collect information from ten or more persons. This proposed rule does not impose reporting or recordkeeping requirements on the public.

Executive Order 13132, “Federalism”

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule that has federalism implications, imposes substantial direct compliance costs on State and local governments, and is not required by statute, or has federalism implications and preempts state law. This proposed rule will not have a substantial effect on State and local governments.

Executive Order 13175, “Consultation and Coordination With Indian Tribal Governments”

Executive Order 13175 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct compliance costs on one or more Indian Tribes, preempts Tribal law, or affects the distribution of power and responsibilities between the Federal Government and Indian Tribes. This proposed rule will not have a substantial effect on Indian Tribal governments.

List of Subjects in 32 CFR Part 310

Privacy.

Accordingly, 32 CFR part 310 is proposed to be amended as follows:

PART 310—PROTECTION OF PRIVACY AND ACCESS TO AND AMENDMENT OF INDIVIDUAL RECORDS UNDER THE PRIVACY ACT OF 1974

■ 1. The authority citation for 32 CFR part 310 continues to read as follows:

Authority: 5 U.S.C. 552a.

■ 2. Amend § 310.13 by adding paragraph (e)(15) to read as follows:

§ 310.13 Exemptions for DoD-wide systems.

* * * * *

(e) * * *

(15) *System identifier and name.*

DoD–0024, “Catch a Serial Offender (CATCH) Program Records.”

(i) *Exemptions.* This system of records is exempt from 5 U.S.C. 552a (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1); (e)(2); (e)(3); (e)(4)(G), (H), and (I); (e)(5); (e)(8); (f) and (g).

(ii) *Authority.* 5 U.S.C. 552a (j)(2).

(iii) *Exemption from the particular subsections.* Exemption from the particular subsections is justified pursuant to 5 U.S.C. 552a(j)(2) for the following reasons:

(A) *Subsection (c)(3), (d)(1), and (d)(2).* Records in this system of records may contain investigatory material compiled for criminal law enforcement

purposes to include information identifying criminal offenders and alleged offenders, information compiled for the purpose of criminal investigation, or reports compiled during criminal law enforcement proceedings. Application of exemption (j)(2) may be necessary as access to, amendment of, or release of the accounting of disclosures of such records could inform a record subject of an investigation of the existence, nature, or scope of an actual or potential law enforcement or disciplinary investigation, and thereby seriously impede law enforcement or prosecutorial efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties or disciplinary measures; access to, amendment of, or release of the accounting of disclosures could also reveal confidential sources who might not have otherwise come forward to assist in an investigation and thereby hinder DoD’s ability to obtain information from future confidential sources and result in an unwarranted invasion of the privacy of others.

(B) *Subsection (c)(4), (d)(3) and (4).* These subsections are inapplicable to the extent that an exemption is being claimed from subsections (d)(1) and (2).

(C) *Subsection (e)(1).* In the collection of information for investigatory or law enforcement purposes, it is not always possible to conclusively determine the relevance and necessity of particular information in the early stages of the investigation or adjudication. In some instances, it will be only after the collected information is evaluated in light of other information that its relevance and necessity for effective investigation and adjudication can be assessed. Collection of such information permits more informed decision-making by the Department when making required disciplinary and prosecutorial determinations.

(D) *Subsection (e)(2).* To collect information from the subject individual could serve notice that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations. Collection of information only from the individual accused of criminal activity or misconduct could also subvert discovery of relevant evidence and subvert the course of justice. Accordingly, application of exemption (j)(2) may be necessary.

(E) *Subsection (e)(3).* To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.

Accordingly, application of exemption (j)(2) may be necessary.

(F) *Subsection (e)(4)(G) and (H).*

These subsections are inapplicable to the extent exemption is claimed from subsections (d)(1) and (2).

(G) *Subsection (e)(4)(I).* To the extent that this provision is construed to require more detailed disclosure about record sources than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. Accordingly, application of exemption (j)(2) may be necessary.

(H) *Subsection (e)(5).* It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to maintain an accurate record of the investigatory activity to preserve the integrity of the investigation and satisfy various Constitutional and evidentiary requirements, such as mandatory disclosure of potentially exculpatory information in the investigative file to a defendant. It is also necessary to retain this information to aid in establishing patterns of activity and provide investigative leads. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined through judicial processes. Accordingly, application of exemption (j)(2) may be necessary.

(I) *Subsection (e)(8).* To serve notice could give persons sufficient warning to evade investigative efforts. Accordingly, application of exemption (j)(2) may be necessary.

(J) *Subsection (f).* To the extent that portions of the system are exempt from the provisions of the Privacy Act concerning individual access and amendment of records, DoD is not required to establish rules concerning procedures and requirements relating to such provisions. Accordingly, application of exemptions (j)(2) may be necessary.

(K) *Subsection (g).* This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act to which the civil remedies provisions pertain.

(iv) *Exempt records from other systems.* In the course of carrying out the overall purpose for this system, exempt records from other systems of records may in turn become part of the

records maintained in this system. To the extent that copies of exempt records from those other systems of records are maintained in this system, the DoD claims the same exemptions for the records from those other systems that are entered into this system, as claimed for the prior system(s) of which they are a part, provided the reason for the exemption remains valid and necessary.

Dated: October 23, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison
Officer, Department of Defense.

[FR Doc. 2024–25035 Filed 10–28–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF TRANSPORTATION

Federal Railroad Administration

49 CFR Part 211

[Docket No. FRA–2024–0033]

RIN 2130–AC97

Federal Railroad Administration's Procedures for Waivers and Safety- Related Proceedings

AGENCY: Federal Railroad Administration (FRA), U.S. Department of Transportation (DOT).

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: This proposed rule would update FRA's procedures for waivers and safety-related proceedings to define the two components of the statutory waiver and suspension standard, “in the public interest” and “consistent with railroad safety.” By defining these terms, FRA intends to clarify the standard the agency will apply when evaluating petitions for regulatory relief. FRA also proposes to require petitions for relief to include evidence of meaningful consultation with appropriate stakeholders. Additionally, FRA proposes to make minor updates to agency rules of practice.

DATES: Written comments on this proposed rule must be received on or before December 30, 2024. Comments received after that date will be considered to the extent possible without incurring additional expense or delay.

ADDRESSES:

Comments: Comments related to Docket No. FRA–2024–0033 may be submitted by going to www.regulations.gov and following the online instructions for submitting comments.

Instructions: All submissions received must include the agency name and

docket number or Regulatory Identification Number (RIN) for this rulemaking. All comments received will be posted without change to www.regulations.gov; this includes any personal information. Please see the Privacy Act heading in the **SUPPLEMENTARY INFORMATION** section of this document for Privacy Act information related to any submitted comments or materials.

Docket: For access to the docket to read background documents or comments received, go to www.regulations.gov and follow the online instructions for accessing the docket.

FOR FURTHER INFORMATION CONTACT:

Veronica Chittim, Senior Attorney, Office of the Chief Counsel, at veronica.chittim@dot.gov, 202–480–3410; or Lucinda Henriksen, Senior Advisor, Office of Railroad Safety, at lucinda.henriksen@dot.gov, 202–657–2842.

SUPPLEMENTARY INFORMATION:

I. Background

FRA has broad discretionary authority to waive or suspend the requirement to comply with any rule, regulation, or order upon a finding that doing so is “in the public interest and consistent with railroad safety.” 49 U.S.C. 20103(d).¹ Within FRA, decisional authority for waivers rests with FRA's Railroad Safety Board (Board).² FRA's Rules of Practice, 49 CFR part 211, set forth the general requirements for petitions to the Board and the general outline of the Board's processes.³ The burden of proving the request is justified rests with the petitioner.⁴

In January 2023, FRA published guidance pertaining to waiver procedures and process titled *Guidance on Submitting Requests for Waivers, Block Signal Applications, and Other Approval Requests to FRA* (Guidance).⁵ The Guidance outlined best practices for petitioners to use when developing and submitting waiver, suspension, and other approval requests, and best practices impacted stakeholders (e.g., the public, railroad employees, and labor organizations) may use to ensure their views, concerns, and comments

¹ The Secretary of Transportation is authorized to issue such waivers or suspensions and the Secretary has delegated that authority to FRA. 49 U.S.C. 20103(d)(1) and 49 CFR 1.89(a).

² 49 CFR 211.41(a).

³ 49 CFR part 211, subpart C (§§ 211.41 through 211.45).

⁴ See 49 CFR 211.9.

⁵ <https://railroads.dot.gov/elibrary/guidance-submitting-requests-waivers-block-signal-applications-and-other-approval-requests>; 88 FR 1448 (Jan. 10, 2023).

are thoroughly considered throughout the process. This proposal would provide additional detail on portions of the guidance, and make certain recommendations therein mandatory, such as the recommended consultation prior to filing of a petition.

In this rulemaking, FRA is proposing to update its procedures for waivers and safety-related proceedings in 49 CFR part 211 to clarify the standard to be applied by FRA when deciding whether to grant a request for regulatory relief. Specifically, FRA is proposing to define both the “in the public interest” and “consistent with railroad safety” components of the statutory standard in 49 U.S.C. 20103(d), for purposes of evaluating waiver or suspension requests. Additionally, FRA is proposing to require petitions for regulatory relief to include evidence of meaningful consultation with stakeholders.

II. Section-by-Section Analysis

Part 211

§ 211.1 General

FRA proposes to make minor editorial amendments to § 211.1(a) to remove outdated language regarding the Federal Railroad Safety Act (concerning proceedings initiated after 1976). Further, FRA proposes to replace the obsolete statutory citation (45 U.S.C. 432) for emergency orders with the current citation, 49 U.S.C. 20104. FRA also proposes to clarify that a proceeding will be deemed to be initiated and the time period for its disposition will begin on the date a petition or application that complies with the requirements of this chapter is confirmed to be complete (not merely the date it is received) by FRA.

FRA also proposes to make technical amendments to the definitions of “Safety Act,” “Docket Clerk,” and “Railroad Safety Board.” Specifically, in the definition of “Safety Act” in § 211.1(b)(3), FRA proposes to update the citation (45 U.S.C. 421 *et seq.*) to 49 U.S.C. ch. 201 *et seq.*, as the existing citation is obsolete. FRA proposes to add a cross-reference in § 211.1(a) to the proposed updated definition of “Safety Act” in § 211.1(b)(3). In the definition of “Docket Clerk” in § 211.1(b)(4), FRA proposes to (1) remove the reference to the “Office of Chief Counsel Docket Clerk,” as this position no longer exists at FRA, and (2) replace the physical address for the DOT Docket Clerk with the website www.regulations.gov. Within the definition of “Railroad Safety Board” in § 211.1(b)(5), FRA proposes to insert the word “Railroad”

before “Safety” into the outdated term “Office of Safety.”

FRA proposes to amend § 211.1(b) to add specific definitions of “in the public interest” and “consistent with railroad safety” for purposes of this part. FRA has long interpreted the standard in 49 U.S.C. 20103(d)(1) of “in the public interest and consistent with railroad safety” as a standard focused on safety, including the safety of rail operations and those directly involved in those operations, as well as the safety and well-being of the public at large. However, neither 49 U.S.C. 20103 nor 49 CFR part 211 defines “in the public interest and consistent with railroad safety.” Thus, in § 211.1(b)(6) and (b)(7), FRA proposes to add definitions of “in the public interest” and “consistent with railroad safety” to clarify the standard and provide transparency and consistency as to how FRA will evaluate whether a petition meets that standard.

Overall, via the proposed definitions in § 211.1(b)(6) and (7), FRA expects requests for waivers, suspensions, and other safety-related proceedings for regulatory relief to maintain or improve railroad safety and to align with one or more of DOT’s priorities and innovation principles or other public interest factors.⁶ DOT’s first innovation principle, to “Serve our policy priorities,” includes a focus “around creating high quality jobs, achieving racial equity and increasing opportunity for all Americans, and tackling the climate crisis” to drive innovation. DOT’s second innovation principle, “Help America win the 21st century,” prioritizes future proofing infrastructure and also bringing legacy systems into the digital age and enabling adaptability and resiliency. Many FRA regulations were established prior to the digital age, providing an opportunity for future requests to show how certain practices can be updated and adapted appropriately consistent with this principle. DOT’s third innovation principle, “Support workers,” involves empowering workers on many levels, including expanding skills and training, as well as ensuring workers have a seat at the table to shape innovation. DOT’s fourth innovation principle, “Allow for experimentation and learn from failure,” supports open data and transparency and the ability to learn from experimentation and failures. DOT’s fifth innovation principle, “Provide opportunities to collaborate,” strives for an outcomes-based approach that is technology neutral, consistent with FRA’s performance-based

regulations. This principle embraces public private partnerships that foster innovation and protect the interests of the public, workers, and communities in a technology-neutral manner. Finally, DOT’s sixth innovation principle, “Be flexible and adapt as technology changes,” also reflects performance-based regulations and interoperability, and the need for a collaborative approach across transportation modes.

For purposes of this part, in § 211.1(b)(7), FRA proposes to define “consistent with railroad safety” to mean the proposal is “at least as safe as or safer than the status quo (*i.e.*, without the proposed relief).” If a proposal would improve railroad safety and/or remove certain railroad operational risks, the prong “consistent with railroad safety” would be satisfied as proposed here. At a minimum, FRA proposes that a petition must document and provide associated qualitative or quantitative analysis that demonstrates that with the regulatory relief, railroad operations would be at least as safe as they would have been without the relief. Under no circumstances could this standard be met if the safety provided under the applicable regulations is not maintained or is reduced. Additionally, consistent with DOT’s policy priorities, “innovations should reduce deaths and serious injuries on our Nation’s transportation network, while committing to the highest standards of safety across technologies.”⁷ Thus, in any petition seeking regulatory relief, petitioners should include safety analysis and any data demonstrating how the request aligns with the proposed definition of “consistent with railroad safety” in § 211.1(b)(7). Generally, FRA expects that a petition that would reduce the level of existing required human visual inspections or that would not meet current FRA requirements would not be consistent with railroad safety under the proposed § 211.1(b)(7). Thus, to demonstrate that a petition is consistent with railroad safety, the petition must show that the proposed process or technology will overcome that expected reduction in safety by being as safe or safer than the existing regulation would require.

For purposes of this part and for understanding the statutory standard, in § 211.1(b)(6), FRA proposes to define “in the public interest” to mean “the proposed request demonstrates positive factors including, but not limited to, empowering workers, ensuring equity, protecting the environment, creating robust infrastructure, enabling

adaptability and resiliency, bringing legacy systems up to current standards, allowing for experimentation consistent with railroad safety, providing opportunities to collaborate, ensuring interoperability integration across transportation modes, and the well-being of the public at large.” FRA proposes that “in the public interest” signifies not only how a proposal for regulatory relief may improve railroad operations, but also how the request may positively affect relevant stakeholders, including workers and communities. FRA notes that a request demonstrating any of these factors in the proposed definition may be seen to be “in the public interest,” because the proposal would align with one or more of DOT’s priorities and innovation principles.

To reflect whether the request is “in the public interest” as proposed in § 211.1(b)(6), FRA notes that petitioners should address these principles directly in their petitions. For example, the petition could explain how the proposal would reduce waste, re-use or recycle certain inputs, or reduce emissions, demonstrating that the proposal is “in the public interest.” Similarly, consistent with the principle to “Help America win the 21st century,” a petitioner could demonstrate how a request may create robust infrastructure, enable adaptability and resiliency, and bring legacy systems up to current standards. Likewise, the petitioner could show how the request would allow for experimentation to enable learning from both successes and failures (while still being consistent with railroad safety). The request could demonstrate how the petitioner has provided (and will continue to provide) opportunities to collaborate with workers and local communities. Moreover, such requests could show how the proposal would empower workers, such as through expanding access to skills, training, and/or the choice of a union. In line with these principles, FRA expects to continue its successful practice of encouraging stakeholder engagement through establishing test committees⁸ as a condition to granting regulatory relief, when appropriate. Historically, FRA has, in certain instances, required the establishment of a test committee as a

⁶ <https://www.transportation.gov/priorities/transformation/us-dot-innovation-principles>.

⁷ <https://www.transportation.gov/priorities/transformation/us-dot-innovation-principles>.

⁸ FRA has traditionally specified the membership of test committees in the conditions to the waiver, if applicable, ensuring that all relevant stakeholders are represented. Test committee membership may include, for example, representatives from equipment manufacturers, affected labor representatives, FRA personnel, railroad representatives, and Association of American Railroads committee members, etc.

condition of regulatory relief related to the use of technology or a new operational process in the railroad industry. As noted in footnote 8, a test committee typically involves a small group of diverse stakeholders that meet periodically to review safety data and consider related challenges and benefits of the relief. To show that a proposal is “in the public interest,” FRA proposes that a petitioner could provide evidence that the regulatory relief requested would not eliminate jobs or eliminate required visual inspections, but would add additional positions, or improve the existing positions. The petitioner could identify opportunities for interoperability among innovations and foster cross-modal integration, if possible. Accordingly, in any petition seeking regulatory relief, petitioners should demonstrate how the request aligns with the proposed definition of “in the public interest” in § 211.1(b)(6).

By incorporating definitions for “in the public interest” and “consistent with railroad safety” into FRA’s Rules of Practice, FRA intends to ensure consistency in how requests are evaluated going forward. For example, when reviewing whether a waiver request is “in the public interest and consistent with railroad safety,” the Board would assess the request’s commitment to both safety and the public interest. A petition showing only that a proposal may improve the efficiency of railroad operations or reduce costs will likely not meet the standard in the proposed definition of “in the public interest” without a separate showing that the request meets additional public interest factors as proposed in § 211.1(b)(6). The petitioner should be able to show there is a benefit to stakeholders, and, as described below, that the stakeholders had been consulted with before filing to ensure any potential concerns are addressed.

Further, if the request for regulatory relief would reduce the number of inspections being performed, the petition may not meet the “in the public interest” definition proposed here. In many cases, technology can be layered on top of the existing regulatory framework without necessitating a reduction in human inspections currently being performed or relief from Federal regulations.⁹ Thus, if a

petitioner proposes to incorporate a new technology or approach, but also requests relief to permit a reduction in the number of inspections, to demonstrate the request is “in the public interest,” the request would need to show both that the relief is necessary and that other factors outweigh the impacts of reduced inspections in the context of potential negative impacts to the “public interest.”

FRA also notes that the same statutory standard applies for initial requests for relief and renewal or modification requests. Generally, waivers or other approvals for regulatory relief are time limited and may be geographically limited, and renewals are discretionary, which means renewals and expansions of a waiver’s geographic scope are never automatic or guaranteed. Further, consistent with 49 U.S.C. 20103(d)(4), FRA reviews waivers or suspensions that have been in continuous effect for a six-year period and determines whether the waiver or suspension should be terminated, renewed, or incorporated into the regulations. Petitioners seeking to renew or expand an existing grant of relief should include in the application evidence of Petitioners’ compliance with the existing conditions of the relief (if any), and how the waiver, suspension, or other approval for relief has satisfied, and will continue to satisfy, the proposed standard of “in the public interest and consistent with railroad safety.” Additionally, FRA proposes (in § 211.9) to require petitions for renewal to contain specific data on the overall effectiveness of the waiver, suspension, or other grant of relief.

Upon review of a petition for regulatory relief, FRA would determine whether the factors in proposed § 211.1(b)(6) and (b)(7) have been addressed and meet the standard of “in the public interest and consistent with railroad safety.” If the factors have not been addressed, FRA may dismiss the petition, primarily because FRA would be unable to evaluate whether the request meets the standard of “in the public interest and consistent with railroad safety.” If the petition addresses the factors proposed in § 211.1(b)(6) and (b)(7), FRA would then consider whether the requested regulatory relief satisfies the “in the public interest” and “consistent with railroad safety” standards as defined and would address these requirements in any decision letter issued.

Given this proposal, which would define and clarify the “public interest” component of the statutory standard, FRA seeks public comment on whether additional changes to the existing

procedures for waivers, suspensions, and other safety-related proceedings for regulatory relief are necessary.

FRA intends the new definitions proposed in § 211.1(b) to be applicable for the evaluation of all waiver and suspension petitions filed pursuant to 49 U.S.C. 20103(d). Historically, FRA has applied the standard of “consistent with railroad safety” to FRA’s review of block signal applications (49 U.S.C. 20502; 49 CFR part 235). FRA does not intend to revise this historical practice, but intends to apply the definition of “consistent with railroad safety,” as proposed in § 211.1(b)(7).

§ 211.7 Filing Requirements

In paragraph (b)(1), FRA proposes to remove the reference to the “FRA Docket Clerk,” and replace with “FRA via email to *FRAWaivers@dot.gov*.” The position of “FRA Docket Clerk” no longer exists. FRA proposes to remove the reference in that section to “grandfathering,” and simply refer to “petitions for approval” under 49 CFR 238.203. Finally, FRA proposes modifying the phrase that the acknowledgment shall state “the date the petition or application was received” to be “the date FRA determined the petition or application was complete.”

§ 211.9 Content of Waiver and Other Safety-Related Proceeding Petitions

First, FRA proposes to make minor editorial amendments to § 211.9(a), (b), and (c) to remove the semi-colons at the end of each paragraph and account for the new proposed paragraphs (d) and (e). FRA also proposes to rename § 211.9 and revise the introductory language to reflect a broader application to waivers, and other safety-related proceedings seeking regulatory relief, such as block signal applications and requests for test programs under § 211.51 and remove the application to rulemakings. Specifically, FRA proposes to apply the new language to “each petition for waiver or other safety-related proceeding for regulatory relief.” FRA proposes to remove rulemaking petitions from the applicability of § 211.9 and add a new § 211.10 dedicated to the content requirements of rulemaking petitions. Additionally, in § 211.9(c), FRA proposes removing the language “each evaluation must include an estimate of resulting costs to the private sector, to consumers, and to Federal, State, and local governments as well as an evaluation of resulting benefits, quantified to the extent practicable.” While petitions for relief must evaluate the impacts of a proposed waiver, the existing language for a

⁹ <https://railroads.dot.gov/about-fra/communications/newsroom/press-releases/usdot-secretary-buttigieg-calls-rail-industry-0> (In a February 21, 2023, press release, Secretary Buttigieg called on the railroad industry to “[d]eploy new inspection technologies without seeking permission to abandon human inspections. . . . We need both [technology and human oversight] to keep our nation’s railroads safe.”).

detailed cost benefit analysis is more applicable to petitions for rulemaking, and thus FRA proposes moving this language into § 211.10(c) pertaining to rulemakings.

Second, FRA proposes to amend § 211.9 to add a new paragraph (d) to require that petitioners must provide evidence that they have consulted with applicable stakeholders prior to submission of the application to FRA for consideration. In this proposal, any petition must contain documentation, such as a certification statement by the petitioner, with accompanying documentation demonstrating that the petitioner engaged in meaningful consultation with stakeholders. Specifically, FRA proposes § 211.9(d) to state that petitions must demonstrate: “meaningful good faith consultation with potentially affected stakeholders, including applicable rail labor stakeholders, on the proposed request for relief, prior to submission to FRA for evaluation and processing.” Should FRA finalize this proposed language, a petition that fails to document meaningful consultation will likely be denied as incomplete. While meaningful consultation will generally entail consultation with rail labor stakeholders, affected stakeholders for a more localized request would likely include communities along the railroad’s right-of-way. If a particular community would be affected, FRA expects the railroad to reach out to the community proactively before filing the request with FRA. If there are no specific localities affected, FRA otherwise expects the public to be informed through FRA’s publication of the notice of the request in the **Federal Register**. The public at-large would then have the opportunity to comment on that notice and collaborate on the request.

FRA has found that incoming petitions frequently do not address the potential impacts of the request on stakeholders other than the petitioner. This too often leads to extensive efforts on the part of both FRA and individual petitioners to work with these stakeholders to understand and address their concerns. FRA discussed this issue in its January 2023 Guidance, recommending that petitioners consult and coordinate with stakeholders prior to filing.¹⁰ This proposed rule would streamline the process by requiring petitioners to consult and coordinate with potentially affected stakeholders prior to filing a petition with FRA, and

then documenting these efforts in their petition. For example, virtually every request from a railroad for a waiver from a safety regulation will impact at least some of that railroad’s employees. Accordingly, prior to filing a petition with FRA, this proposal would require a railroad to meaningfully consult with potentially impacted employees, and the local and general chairmen as well as the State and national legislative levels of any labor organizations that represent them, and document the extent and outcome of its consultation in any petition.

Meaningful consultation prior to submission would serve to educate stakeholders of the proposal and reduce the likelihood of any misunderstandings as to the requested relief. FRA expects petitioners to engage stakeholders in discussions about the relief proposed and genuinely seek stakeholders’ input. FRA expects that consultation will be substantive, and not simply serve to check a box that stakeholders were informed of a proposal, as that would not constitute meaningful consultation. Meaningful consultation involves good faith and the best efforts of railroads to engage stakeholders in discussions about the proposed request for relief, the relief sought, and seek substantive input.¹¹ The intent of consultation is to engage with affected stakeholders at all stages of the proposal’s development and then implementation of the relief, if granted. Ideally, railroads would consider their employees, and organization(s) representing those employees, as partners throughout the process rather than as reviewers of a finished product. Meaningful consultation should involve coordinating, gathering, and discussing employee and railroad input and considering feedback on the development of the proposed request.

To show that a railroad sought feedback from applicable stakeholders, a petition could include a statement with a detailed description of the process the petitioner used to consult with stakeholders as well as written correspondence, identify areas of agreement or non-agreement with the proposal, and include a service list to show which parties were consulted. Additionally, FRA expects that stakeholders would provide factual, well-supported feedback that demonstrates such meaningful collaboration.

Petitions that demonstrate consensus has been achieved with potentially affected stakeholders, including applicable rail labor organizations, would likely provide evidence of one factor that the application is “in the public interest.”

Third, as discussed above, FRA proposes to add a new paragraph (e) to require that renewal and expansion petitions contain data on the overall effectiveness of the existing relief. While § 211.9(c) requires petitions to contain sufficient information to support the action sought, including an evaluation of anticipated impacts of the action sought, FRA notes that a renewal or expansion petition should also be able to demonstrate how effective the waiver or other grant of relief has been prior to the request for renewal or expansion. To assist petitioners in providing data on the effectiveness of a waiver or other relief, FRA proposes revising the last sentence in § 211.9(c) to require each petition pertaining to safety regulations to “contain relevant safety data and analysis to demonstrate the petition is in the public interest and consistent with railroad safety, and outline the metrics to be used to determine effectiveness of the waiver or other relief, if granted.” Given the petitioner’s experience implementing and using the waiver or other relief, a petitioner should have specific data to support the renewal or expansion request. This may include how railroad safety has improved because of the waiver or other grant of relief (e.g., the number of defects decreased, or a reduction in the risk of an infrequent, but catastrophic event), and how the public interest has been served. In § 211.9(e)(1), FRA proposes to make this expectation to provide data of the relief’s effectiveness a requirement for all renewal and expansion petitions. Moreover, in § 211.9(e)(2), FRA proposes to require that a renewal or expansion petition must also demonstrate compliance with any conditions that were included in the previous grant of relief. Finally, in § 211.9(e)(3), FRA proposes to require renewal and expansion requests for relief to “demonstrate how the waiver, suspension, or other approval for relief is, and will continue to be, in the public interest and consistent with railroad safety.”

§ 211.10 Content of Rulemaking Petitions

FRA proposes to establish a new provision, § 211.10, to outline content requirements for rulemaking petitions. As discussed above, FRA proposes to remove rulemaking petitions from § 211.9, and create a standalone § 211.10

¹⁰ <https://railroads.dot.gov/elibrary/guidance-submitting-requests-waivers-block-signal-applications-and-other-approval-requests>.

¹¹ Guidance on Railroad/Employee Consultation Requirements in 49 CFR parts 270 and 271, <https://railroads.dot.gov/elibrary/guidance-railroademployee-consultation-requirements-49-cfr-parts-270-and-271>.

to address rulemaking content requirements. The requirements proposed in § 211.10 are substantively similar to the existing § 211.9. Specifically, FRA proposes to require each petition for rulemaking to (a) “set forth the text or substance of the rule, regulation, standard, or amendment proposed, or specify the rule, regulation, or standard that the petitioner seeks to have repealed” and (b) “explain the interest of the petitioner, and the need for the action requested.” In proposed (c), each petition for rulemaking must “contain sufficient information to support the action sought including an evaluation of anticipated impacts of the action sought; each evaluation must include an estimate of resulting costs to the private sector, to consumers, and to Federal, State, and local governments as well as an evaluation of resulting benefits, quantified to the extent practicable.” In this manner, petitions for rulemaking would be required to evaluate the costs and benefits of the proposal.

§ 211.11 Processing of Petitions for Rulemaking

FRA proposes updating the references in this provision from § 211.9 to § 211.10, to reflect the proposed bifurcation of petitions for waivers and petitions for rulemaking content requirements. In § 211.11(b) and (c),

FRA proposes replacing references to the pronoun “he” with “the Administrator.” In § 211.11(d), FRA proposes to change the word “mailed” to “sent” to reflect the possibility of electronic transmittal of the notice of grant or denial.

§ 211.13 Initiation and Completion of Rulemaking Proceedings

FRA proposes updating the reference in this provision from § 211.9 to § 211.10, to reflect the proposed bifurcation of petitions for waivers and petitions for rulemaking content requirements. FRA proposes replacing references to the pronouns “his” and “he” with “the Administrator’s” and “the Administrator.”

§ 211.41 Processing of Petitions for Waiver of Safety Rules

FRA proposes to update the language in § 211.41(b) to include an explicit standard comment period for notice of a waiver in the **Federal Register** to be 60 days. Moreover, FRA suggests removing the introductory language, “[i]f required by statute or the Administrator or the Railroad Safety Board deems it desirable.” Because publication of a notice is required for all such waiver petitions (*see* 49 U.S.C. 20103(d)(2)(C)), FRA finds this introductory language is unnecessary. The existing provision is silent on the length of an appropriate period of

public comment; however, FRA has customarily used 60 days as a matter of practice. FRA also proposes to specify that any deviation from the proposed standard 60-day comment period will be subject to the Administrator’s approval.

§ 211.43 Processing of Other Waiver Petitions

FRA proposes to update the language in § 211.43(b) to mirror the changes as discussed for § 211.41(b).

III. Regulatory Impact and Notices

A. Executive Order 12866 as Amended by Executive Order 14094 and DOT Regulatory Policies and Procedures

This proposed rule is a non-significant regulatory action within the meaning of Executive Order (E.O.) 12866 as amended by E.O. 14094, Modernizing Regulatory Review¹² and DOT’s Order, “Rulemaking and Guidance Procedures,” DOT 2100.6A (June 7, 2021). FRA concluded that this proposed rule would impart an annualized burden of approximately \$78,000 per year, for an estimated 70 waiver petitions annually, or about \$547,000 present value at 7 percent over 10 years. This estimate assumes an equal number of waiver consultations that take 1 hour and those that may take 4 hours, including administrative time of about 25 percent.

TABLE III–1—SUMMARY OF COSTS AND BENEFITS OVER THE 10-YEAR PERIOD

[2023 Dollars]

Impact	Undiscounted	* PV 7%	PV 3%	PV 2%	** Annualized 7%, 3%, 2%
Data Analysis and Metrics	\$62,392	\$43,821	\$53,221	\$56,044	\$6,239
Consultation and Documentation	676,529	475,166	577,093	607,698	67,653
Waiver Renewal Effectiveness and Conditions Compliance	40,109	28,171	34,214	36,028	4,011
Total Costs	779,030	547,158	664,528	699,770	77,903
FRA Cost	Minimal overall change from baseline. Potentially more time to review additional waiver information may be offset by expected better-organized information explicitly addressing NPRM requirements.				
Qualitative Benefit	In general, addressing incomplete information and facilitating affected stakeholder input expected to better meet statutory standards of “in the public interest” and “consistent with railroad safety.”				

* PV = Present Value.

** Because the schedule of costs by year are the same, the annualized values are the same. Figures in tables may not sum due to rounding.

¹² 88 FR 21879 (Apr. 6, 2023) located at <https://www.federalregister.gov/documents/2023/04/11/2023-07760/modernizing-regulatory-review>.

Overall, FRA expects this rule will lead to higher-quality waiver applications that meet the positive objectives of DOT's innovation principles. Because this rule would apply to a variety of relief applications, it is difficult to quantify the potential benefits from consultation on any particular request for relief.

1. Need for Regulatory Action

a. Inadequate or Asymmetric Information

For convenience, this analysis uses the term “waiver” request to encompass petitions for waiver, or other safety-related proceedings for regulatory relief, including block signal applications (BSAPs), and waiver renewal requests subject to this rulemaking.

As stated in the Section-by-Section analysis for § 211.9 and FRA's Guidance,¹³ FRA has found that some submitted waiver requests on the surface seem to contain the information necessary under part 211 (and are therefore considered “received” by FRA), but in fact do not contain sufficient information for FRA to evaluate if a submitted waiver request meets the applicable legal standards and are therefore incomplete. For these waiver requests containing inadequate information, FRA expends resources to work with the petitioner and affected stakeholders to gather the necessary information. Although waiver requests, including requests for renewal and modification, are published in the **Federal Register** for comment, addressing these information needs early in the waiver development process would potentially result in a more streamlined and efficient waiver request “workflow,” *i.e.*, waiver disposition procedure.

By requiring petitioners and affected stakeholders to consult on a waiver request prior to submission to FRA, this NPRM would provide information to both parties that they may be lacking under the current waiver process. For example, a railroad petitioner may lack information on the full effects of the proposed waiver, and employees may misunderstand how a proposed waiver may be implemented or simply lack awareness of the waiver request. Meaningful consultation could avoid unexpected and unintended effects of the proposed waiver that another party may not have considered. Furthermore, if the waiver would involve several parties, for example, several railroad disciplines (*e.g.*, operating practices, motive power and equipment), or more

than one geographic district, consultation would enhance the distribution of information about the proposed waiver among these parties. Parties that may be potential petitioners, such as railroads and suppliers, and those that may be affected stakeholders, such as labor union representatives and community rail associations, have shown a willingness and ability to provide information through their participation in the Railroad Safety Advisory Committee (RSAC)¹⁴ and submitting comments in notice-and-comment rulemakings. The burden to share information and consult on a proposed waiver rests primarily on the petitioner.

Through this NPRM, FRA is also proposing to define the terms “in the public interest” and “consistent with railroad safety” that are used in the statute, 49 U.S.C. 20103(d), but not previously defined. Defining these terms will help clarify for petitioners and affected stakeholders how FRA will decide whether waiver requests meet the statutory standard. By defining these terms, FRA expects that petitioners will be more likely to submit waiver requests providing the necessary and sufficient information for FRA to evaluate the waiver proposal. That may reduce the chances of a waiver being dismissed because a submitted waiver request did not meet these criteria.

b. Statutory Directive

The NPRM would also facilitate FRA's implementation of 49 U.S.C. 20103(d)(4), requiring review and analysis of a waiver that has been in continuous effect for six years. Specifically, the analysis and metrics required under proposed § 211.9(c), and the data about how effective a waiver has been (when a waiver renewal is requested) under proposed § 211.9(e) will help FRA evaluate whether codifying the waiver is in the public interest and consistent with railroad safety. That is, whether the waiver continues to meet the statutory requirements.

2. Baseline

As background, FRA considers several types of waiver requests under FRA's Rules of Practice and decides whether to grant, conditionally grant, or deny a submitted waiver request. If FRA's preliminary review of a submitted petition for waiver shows it to lack sufficient information for further evaluation, the petition may be denied or returned to the petitioner, who may choose to resubmit it.

This analysis uses the environment without the NPRM as the baseline scenario. Without the NPRM's proposed requirements, FRA would continue to receive some waiver requests that are incomplete because they fail to address the statutory criteria of “in the public interest” and “consistent with railroad safety.” FRA would continue to expend resources to gather the missing information from petitioners and affected stakeholders rather than the petitioner providing the necessary information. Petitioners may face uncertainty about the standards FRA is applying in FRA's waiver petition evaluation, and spend unnecessary resources supplementing a waiver petition the petitioner thought to be complete when initially submitted. When implementing the statutory directive to review waivers in operation for six years, FRA may lack some information to fully evaluate the effectiveness of the waiver.

Some categories of waivers already involve consultation with affected stakeholders and the procedure to evaluate these waivers will remain substantially the same under the baseline and the NPRM. These are waivers involving test committees, hours of service (HS) laws, and train horns.

3. Methodology

The proposed data analysis and consultation requirements apply to individual petitions for waivers. Therefore, this analysis used the additional labor time per waiver request to meet these requirements and the number of waiver requests as the basis to estimate the average per-waiver request cost and the overall costs of the NPRM.

The benefits estimate of potential time savings from “streamlining” the waiver process is qualitative because the benefits will depend on the nature of each waiver. Additionally, FRA does not have history to estimate the impact of the NPRM on FRA's waiver Rules of Practice to date. Although FRA's Guidance described much of the NPRM's provisions as best practices, it was issued recently (2023). FRA notes petitioner and stakeholder experiences with waivers that already involve much consultation, such as those for which test committees were established, have been generally positive. These waiver requests that already involve much consultation are relatively few, numbering about 8 waiver requests from the years 2019 through 2022.

¹³ 88 FR 1448 (Jan. 10, 2023).

¹⁴ <https://rsac.fra.dot.gov/>.

Data and Assumptions

To estimate the number of waivers that may be affected, FRA counted the number of **Federal Register** notices published pertaining to its Railroad Safety Board proceedings. From the years 2020 to 2024, a period of 4 years, there were 280 **Federal Register** notices or an average of 70 notices annually. Furthermore, by applying the percentage of waiver petitions filed by Class 1 railroads,¹⁵ FRA estimated that of these 70 total waiver petitions, 21 were Class I railroad waiver petitions, 28 were small railroad waiver petitions, 17.5 were commuter and passenger service railroad waiver petitions, and 3.5 were blanket waiver petitions (covering more than 1 entity) and other waiver petitions. Based on the waiver petitions that have been submitted to FRA in the past, most petitioners will be railroads and most affected stakeholders will be employees, who may be represented by labor unions. For a small number of waiver petitions, a community adjacent to a rail line segment or rail yard may be an affected stakeholder.

To estimate the additional labor hours per waiver petition, FRA estimated 1 hour per waiver request for petitioners to add the data analysis and metrics required under proposed § 211.9(c), which will support that the waiver would be aligned with the proposed definition of “consistent with railroad safety” in § 211.1(b). For documenting meaningful consultation and the prerequisite consultation with affected stakeholders, FRA estimated an equal number of consultations would take 1 hour and those that would take 4 hours, for simple and more complex waiver requests respectively. FRA also estimated an administrative time of about 25 percent to schedule meetings and other logistics. The 50/50 split between simple and more complex waiver requests reflects the uncertainty around this estimate given that waiver requests vary and that this requirement would be new. The average consultation time is 2.5 hours per waiver request, and the average administrative time is 0.625 hours per waiver request, for a combined average time of 3.125 hours per waiver request. Furthermore, FRA estimated 2 employees from the petitioner and 2 employees from an affected stakeholder would each incur the opportunity cost to engage in the

consultation, for a total of 12.5 hours per waiver request.

To monetize these additional labor hours, FRA used wage rates reported to the Surface Transportation Board (STB) by the Class I railroads, burdened by 75 percent. For this analysis FRA used the STB wage rates for the relevant employee groups. For data analysis and describing metrics costs, FRA used the wage rate of \$89.13, representing the Professional and Administrative employee group. For consultation costs, FRA used the wage rate of \$77.32, representing the total for all groups, because a waiver request can include several different types of employees or railroad disciplines.¹⁶

FRA used a 10-year period for this analysis, allowing for 1 original waiver petition and 1 waiver renewal request after a period of 5 years. FRA has found that some railroads may not seek renewals beyond 10 years, possibly because equipment may be over-age, the waiver codified, or other changes in operations or equipment covered under the waiver. FRA also used 2023 real dollars (*i.e.*, a 2023 base year).

4. Costs

The substantive changes from the baseline are found in following proposed sections:

- § 211.1(b) to add definitions of “in the public interest” and “consistent with railroad safety.”
- § 211.9(c) to require analysis and describe effectiveness metrics.
- § 211.9(d) to include documentation of meaningful consultation.
- § 211.9(e) to require waiver renewal requests to show waiver effectiveness and demonstrate compliance with conditions under which the waiver was granted.

Proposing to clarify the definitions of “in the public interest” and “consistent with railroad safety” in § 211.1(b) have no direct costs except the data analysis and metrics required under proposed § 211.9(c) support demonstrating the waiver request meets these criteria; the sections may be seen to work together. It may take some additional effort to explicitly show how the proposed waiver would meet these criteria, which is reflected in the data analysis, metrics, and consultation cost sections.

The title of § 211.9 is proposed to be revised to include “other safety-related proceedings petitions.” The revision would add proceedings such as those for BSAPs and test programs to this section. FRA has historically held BSAPs to the same safety standards as other waiver petitions. Also, as mentioned, waivers for which test committees are established include much consultation under the baseline. Therefore, this change would be administrative in nature and has no costs.

More significantly, proposed changes to § 211.9(c) would add requirements for (data) analysis and metrics. Although ensuring that a proposed waiver meets safety criteria has always been a part of FRA’s evaluation, the changes in this section emphasize that requirement. Waiver requests would need to include analysis and clearly identify safety impacts. In addition, the specified metrics can be used to determine if the waiver is achieving the intended goals, and meeting the “in the public interest” and “consistent with railroad safety” standards. The metrics need not be complex, for example, accident/incident measures appropriate to the type of waiver proposed (*i.e.*, discipline or railroad operation covered by the waiver), or relevant casualties. FRA estimated this cost as: *Cost of analysis and metrics = time to perform analysis and metrics × wage rate × no. of waivers*. Using 1 hour for the time, and the Professional and Administrative wage rate of \$89.13 per hour, yields an estimated cost of \$89.13 per waiver request, or \$6,239 for the estimated 70 waiver requests per year. The schedule of these costs is shown in the summary table below.

The documentation requirement proposed in § 211.9(d) requires meaningful consultation between the petitioner and affected stakeholders. FRA estimated this cost as: *Cost of consultation and documentation = (hours per waiver × wage rate × no. of employees) × no. of waivers*. The cost is incurred by both the petitioner and affected stakeholders. FRA assumes the cost is equal for both parties. Using an average time (including administrative time) of 3.125 hours per waiver request, a wage rate representing all employee types of \$77.32 per hour, 2 employees each for the petitioner and affected stakeholder(s), and 70 total waiver requests results in a cost of \$33,826 annually for each party. The cost per waiver request is \$483, again for each party. The total costs are shown in the summary table below.

Under the baseline, FRA expends resources to gather missing data from

¹⁵ Separately, FRA reviewed its waiver management systems and found the number of incoming waiver petitions from Class I railroads has remained fairly consistent from the years 2019 through 2023, with a slight decrease only in 2023 (about 24 waiver petitions per year on average).

¹⁶ STB Quarterly Wage A&B Data (2023). Annual composite for All Railroads. Available: <https://www.stb.gov/reports-data/economic-data/quarterly-wage-ab-data/>. Calculations: Group 200 Professional & Administrative employees, \$50.93 per hour STB average straight time rate × 1.75 fringe benefit multiplier = \$89.13 per hour burdened wage rate. Similarly, for Group 700 Total All Groups employees, \$44.18 × 1.75 = \$77.32 per hour burdened wage rate.

the waiver request that the proposed consultation should provide. Thus, some of FRA’s burden and associated cost may be transferred to the petitioner under the proposed requirements in the NPRM. However, FRA assumes that the time spent by FRA post-waiver request submittal is more than the time that would be spent by the petitioner pre-waiver request submittal. FRA reasons that the petitioner has direct knowledge of the subject proposed waiver and ready access to affected stakeholders who may be employees or employee representatives on the petitioner’s worksite or property.

Also under the baseline, petitioners wishing to renew a waiver are expected to provide enough information about its

impacts (and under certain conditions, if so specified) to support its renewal. Proposed § 211.9(e) would require petitioners to show a waiver’s effectiveness over time and compliance with the specified waiver conditions explicitly. FRA expects there will be additional data available by the time a waiver is eligible for extension or renewal to demonstrate its effectiveness; the metrics developed in proposed § 211.9(c) would assist with that effort. FRA notes not all waivers are submitted to FRA for renewal because of the age of the equipment, changes in technology, codification of waivers, or other operational reasons. Based on the Reflectorization of Rail Freight Rolling Stock: Codifying Existing Waivers

NPRM,¹⁷ about 64 percent of waivers are eligible for renewal. Applying that percentage to the 70 waiver requests used in this analysis yields about 45 waivers eligible for renewal annually. The cost is therefore accounted by: *Cost to show renewal effectiveness and compliance = time to provide data × wage rate × no. of renewals*. Using 1 hour for the time, similar to § 211.9(c) for the marginal data analysis and metrics development, \$89.13 to represent Professional and Administrative employees who may perform the data analysis, and 45 renewal requests, produces a cost of \$4,011 annually, or \$89.13 per waiver.

The schedule of NPRM costs is summarized in the table below.

TABLE III–2—SCHEDULE OF NPRM COSTS
[2023 Dollars]

Year	§ 211.9(c) Analysis and metrics	§ 211.9(d) Consultation and documentation	§ 211.9(e) Waiver renewal effectiveness and compliance	Total
1	\$6,239	\$67,653	\$4,011	\$77,903
2	6,239	67,653	4,011	77,903
3	6,239	67,653	4,011	77,903
10	6,239	67,653	4,011	77,903
Total	62,392	676,529	40,109	779,030
PV 7%	43,821	475,166	28,171	547,158
PV 3%	53,221	577,093	34,214	664,528
PV 2%	56,044	607,698	36,028	699,770
Annualized 7%, 3%, 2%	6,239	67,653	4,011	77,903

The figures for analysis of years 4 through 9 repeat and are not shown for brevity. Similarly, the annualized costs using discount rates of 7%, 3%, and 2% are the same.

Government Costs

FRA does not anticipate any additional significant costs under the NPRM. FRA may receive more data and analysis to evaluate, but expects it will be better organized to highlight the information needs addressed by the NPRM. Overall, FRA estimates minimal changes to the time needed for FRA’s evaluation of waiver requests, which are a part of FRA’s customary duties.

FRA invites comment on the inputs used to estimate the costs for the NPRM.

5. Benefits

Because FRA receives a variety of waiver requests covering different areas of the railroading environment, it is difficult to quantify the benefits of the NPRM. The benefits will depend on the increase in the quality of information FRA receives in submitted waiver requests. Generally, FRA expects more and better information that supports a waiver meets the overall statutory standard of safety vis-à-vis the criteria of

“in the public interest” and “consistent with railroad safety.”

6. Other Effects

Distributional Effects

The NPRM may have positive distributional effects. Through consultation and involvement of affected stakeholders, their concerns can be accounted for in evaluating a waiver request and setting conditions for its potential use. That may avoid concentrating the benefits of a waiver in a relatively small number of petitioners, while the costs may be spread among many affected stakeholders.

7. Alternatives

FRA considered two alternatives to the NPRM. First, FRA considered extending the time provided to stakeholders to comment on waiver requests. Second, FRA considered a process in which FRA would facilitate a discussion between a petitioner for waiver and affected stakeholders, in lieu

of the consultation proposed in the NPRM.

For the first alternative, FRA would continue to publish **Federal Register** notices concerning waiver requests as it currently does under FRA’s Rules of Practice. However, FRA could extend the time provided for affected stakeholders to comment on such **Federal Register** notices. The goal would be to expand the opportunity for affected stakeholders to provide information and share their concerns. This option would be a straightforward, low-cost alternative. However, simply extending the comment period time would not achieve FRA’s regulatory objective because FRA would still likely receive waiver requests that lack the in-depth data needed for a thorough evaluation of a waiver request in light of the statutory standard.

FRA also considered an alternative modeled after the RSAC. RSAC membership consists of railroads, suppliers, labor union representatives,

¹⁷ 87 FR 43467 (July 21, 2022).

public interest groups, other governmental agencies, and other interested parties—essentially potential waiver petitioners and affected stakeholders. In the same way that RSAC members discuss assigned regulatory tasks, FRA could host a similar “roundtable” meeting for a petitioner and affected stakeholders to discuss a petitioner’s proposed waiver. FRA would serve as host and facilitator, acting in the same role as it currently does for RSAC meetings. However, this alternative may suggest a perception that FRA is bringing all parties together to eventually approve the waiver petition, rather than FRA serving as the arbiter of the petition. Simultaneously, in this alternative, FRA could also clarify the criteria of “in the public interest” and “consistent with railroad safety” that FRA uses to evaluate waiver requests. Similar to the NPRM, this alternative process could provide clarity, transparency, and input from stakeholders.

To account for the cost of the RSAC-like alternative, FRA reasoned that simple and routine proposed waivers could be discussed through virtual meetings, while more complex waiver requests would benefit from in-person meetings with an option to attend virtually, *i.e.*, hybrid meetings. FRA conducts similar types of virtual and hybrid meetings for the RSAC. The costs for these meetings consist of administrative costs to plan meetings, and opportunity costs for the participants’ time to attend meetings. FRA calculated the average cost of a meeting to discuss a proposed petition and multiplied it by the estimated 70 waiver requests a year for an overall cost for this alternative, as enumerated below.

The administrative costs would vary by whether a meeting is virtual or

hybrid. Based on a discussion with FRA’s RSAC program manager, the tasks for virtual meetings consist of scheduling the meeting, forming an agenda, and posting the meeting details on FRA’s website. In addition, FRA prepares meeting minutes after the meeting. For the scheduling, agenda, and website posting tasks, FRA estimated 1 hour of labor time; for the post-meeting minutes preparation, FRA estimated 3 hours of labor time; for a total of 4 hours. For the hybrid meetings, FRA would need to arrange for meeting space, and audio/visual (A/V) equipment and personnel to operate it. FRA generally pays a fixed price for these services. FRA estimated the cost to rent meeting space, including conference room set-up, to be \$5,000, and the cost for A/V equipment and the operator to be \$5,000 per day, for a total of \$10,000 per meeting (*i.e.*, per complex waiver request). For monetizing FRA time for planning the virtual meeting and for the opportunity cost to attend meetings (see below), this analysis used the General Schedule (GS) pay rate for grade GS–14, step 5 Federal employees in the Washington, DC area. This Federal employee pay rate of \$71.88 was burdened by 75 percent for fringe to yield a pay rate of \$125.79 per hour.¹⁸ The resulting administrative cost for a simple waiver request was estimated at \$503 per waiver request, and \$10,000 for a complex waiver request. For both virtual and hybrid meetings, FRA would bear all the administrative costs.

All parties would incur an opportunity cost to attend the meetings. FRA assumed two representatives from each party to a proposed petition would attend the consultation meeting, specifically two employees each from FRA, the petitioner, and affected

stakeholders. For the petitioners and affected stakeholders, most of whom will be railroad employees, FRA used the same STB wage rates as used in the primary NPRM analysis. In general, the cost for attending a virtual or hybrid meeting is: *Cost to attend meeting = meeting hours × no. of employees × wage rate*, where the meeting hours will vary by type of meeting (virtual or hybrid) and the wage rate varies by type of employee (government or railroad). Using the inputs above, the FRA cost to attend a meeting for a simple waiver request would be \$1,006, and would be \$619 each for petitioners and stakeholders.¹⁹ The cost to attend a hybrid meeting for a complex waiver request is double the cost for virtual meetings because the time is doubled. Therefore, the FRA cost for a complex waiver request would be \$2,013, and the petitioner and stakeholder cost would be \$1,237 each.

Adding in the administrative cost to FRA’s attendance cost resulted in an FRA cost per simple waiver request of \$1,509, and \$12,013 for a complex waiver request (with the majority of complex waiver request costs resulting from conference room rental and A/V equipment and operator fees). The average cost would be \$6,761. For a petitioner and stakeholder that incur only the attendance cost, the average cost would be \$928 per waiver request.²⁰ Next, the respective average cost was multiplied by the estimated 70 waiver requests a year for estimated total costs for FRA, petitioner, and stakeholders. These costs would remain constant over the 10-year period of analysis. The table below shows the present values of these cost schedules. The expected benefit would be the same qualitative benefit as for the preferred NPRM option.

TABLE III–3—ALTERNATIVE OPTION: SUMMARY OF COSTS OVER THE 10-YEAR PERIOD
[2023 Dollars]

Proposed waiver party	Undiscounted	*PV 7%	PV 3%	PV 2%	**Annualized 7%, 3%, 2%
FRA (Gov’t)	\$4,737,742	\$3,324,080	\$4,037,125	\$4,251,226	\$473,274
Petitioner	649,468	456,159	554,009	583,390	64,947
Stakeholder	649,468	456,159	554,009	583,390	64,947
Total Cost	6,031,678	4,236,398	5,145,144	5,418,006	603,168
Total Cost without FRA	1,298,936	912,318	1,108,019	1,166,781	129,894

* PV = Present Value.

¹⁸ Office of Personnel Management (OPM), Salary Table 2023–DCB (Jan. 2023). Available: https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2023/DCB_h.pdf. Calculation: \$71.88 per hour × 1.75 fringe benefit multiplier = \$125.79 per hour burdened rate.

¹⁹ Calculation: Cost to attend virtual meeting (FRA) = 4 hours × 2 employees × \$125.79 per hour = \$1,006.32. The petitioner cost equals the stakeholder cost = 4 hours × 2 employees × \$77.32 per hour = \$618.54.

²⁰ Sample calculation: Cost of simple waiver request (petitioner) = attendance cost only =

\$618.54. Cost of complex waiver request = \$1,237.08. Average cost of waiver request = (\$618.54 + \$1,237.08)/2 = \$927.81 per waiver request. The stakeholder cost is the same as the petitioner cost.

** Because the schedule of costs by year are the same, the annualized values are the same.

To compare the RSAC-like alternative to the preferred NPRM option, the estimated annualized cost is highlighted. The annualized cost (without FRA) for this alternative of \$129,804 exceeds the cost of the NPRM option cost of \$77,903. The cost of the alternative including FRA costs is much greater than the preferred NPRM option cost. Thus, the alternative would not reduce costs in comparison to the NPRM option.

7. Sensitivity Analysis

The costs are dependent on the number of waiver requests per year and the estimate of time to address the proposed requirements. The largest category of costs presented in Table III–2 is for the consultation and documentation provision in proposed § 211.9(d). FRA assumed an equal number of simple and complex waiver requests and therefore used a straight average to estimate the time required. If the stakeholders submit and therefore consult on simple or routine waiver requests more than complex waiver requests, then that cost might be overstated; the converse is true if petitioners and stakeholders consider relatively more complex waiver requests.

FRA's count of 70 waiver petitions a year may underestimate the amount of consultation because when petitioners are added to existing umbrella or blanket waivers, there may not be additional discrete **Federal Register** notices (upon which the estimate of 70 waiver petitions was based). On the other hand, such additional consultations for an existing waiver would be familiar and similar to previous consultations on the same blanket waiver, *i.e.*, they would impose only a small burden. The number of blanket waiver requests is also small (3 waiver requests). Additionally, existing blanket waiver requests include an HS waiver,²¹ for which FRA expects consultation already occurs, mitigating the potential overestimate of costs.

8. Conclusion

In this NPRM, FRA is clarifying terms and proposing changes to provide more complete information for FRA's waiver proceedings. The NPRM addresses proposed waiver petitions received by FRA that lack description of the full range of impacts.

FRA estimated the NPRM would result in costs with a present value of about \$547,000 using a 7 percent discount rate and \$665,000 using a 3 percent discount rate, over a 10-year period of analysis in 2023 dollars. The benefits are described qualitatively because the specific benefits would depend on the waiver under consideration. In general, FRA expects the proposed waivers it receives would include more and better information reflecting the impacts to affected stakeholders. The NPRM would establish a way to gather this information potentially more efficiently before a waiver proposal is submitted to FRA instead of FRA, petitioner, and stakeholders working to gather this information post-waiver request submittal to FRA. The additional information would facilitate FRA determining whether that waiver request meets the statutory standard in 49 U.S.C. 20103(d). FRA would also be better able to balance the interests of a petitioner and stakeholders in the overarching interest of public safety.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act of 1980 ((RFA), 5 U.S.C. 601 *et seq.*) and E.O. 13272 (67 FR 53461, Aug. 16, 2002) require agency review of proposed and final rules to assess their impacts on small entities. When an agency issues a rulemaking proposal, the RFA requires the agency to “prepare and make available for public comment an initial regulatory flexibility analysis” which will “describe the impact of the proposed rule on small entities.” 5 U.S.C. 603(a).

1. Reasons for Considering Agency Action

In this NPRM, FRA is proposing changes to its waiver procedures so waiver petitions submitted to FRA contain more complete information and FRA is informed by sufficient coordination with potential affected stakeholders. As discussed above, this NPRM would apply to waiver requests and other safety-related proceedings for regulatory relief, including BSAPs, and waiver renewal requests. FRA has found that some petitions incompletely describe the impacts of a proposed waiver because they do not address its potential impacts on affected stakeholders. The lack of sufficient information often requires extensive efforts by FRA, the petitioner, and affected stakeholders to gather this information after a waiver petition has

been submitted to FRA or may result in dismissal of a petition due to lack of sufficient information. FRA is therefore proposing that petitioners requesting a waiver consult with affected stakeholders before submitting a waiver request to FRA. Petitioners would also need to provide documentation of consultation with affected stakeholders in their waiver request. See proposed § 211.9(d).

To aid petitioners requesting a waiver in providing the type of information sought by FRA, FRA is proposing to define the terms “in the public interest” and “consistent with railroad safety.” See proposed § 211.1(b)(6) and (7). The statute authorizing FRA to waive or suspend regulatory requirements uses these terms in setting the standard that FRA must use in its decision whether to grant a waiver request. However, these terms are not defined in the statute. 49 U.S.C. 20103(d).

Under the NPRM, a waiver request must contain analysis demonstrating how the proposed waiver would impact the overarching standard of safety. A waiver request also would need to describe the metrics used to measure its effectiveness. See proposed § 211.9(c). A waiver renewal request would be held to same standard, and the petitioner would be required to use data and metrics to show a waiver was effective from approval to request for renewal. See proposed § 211.9(e).

2. A Succinct Statement of the Objectives of, and Legal Basis for, the Proposed Rule

The proposed rule seeks to provide clarity for petitioners requesting a waiver, and result in waiver requests submitted to FRA that provide more in-depth information upon which to base its evaluation. The proposed definitions of “in the public interest” and “consistent with railroad safety” would clarify for the regulated community and the public the criteria FRA uses in deciding whether to grant a waiver request. Furthermore, the proposed requirement to include analysis and metrics in addition to the existing requirement to include relevant safety data would help show how a proposed waiver meets these two criteria. The safety data, analysis, and metrics would ultimately aid FRA in evaluating that a proposed waiver is in the public interest and consistent with railroad safety. Also, the proposed section requiring petitioners to consult with affected stakeholders prior to submitting a waiver request will help ensure the

²¹ Docket Number FRA–2009–0078 (see, *e.g.*, <https://www.regulations.gov/document/FRA-2009-0078-0216>).

petition captures more complete information about a proposed waiver's impacts. FRA intends such a consultation would be a "two-way street," serving to gather information from, but also inform, affected stakeholders who otherwise may have minimal knowledge about the proposed waiver. Finally, the proposed requirements for waiver renewal requests would align with the proposed greater information needs for waiver requests, to show the original waivers were effective.

Regarding the legal basis, this NPRM would define the terms "in the public interest" and "consistent with railroad safety" to help gather information from petitioners facilitating FRA to implement the statutory standard (when determining whether to waive or suspend compliance with rules or regulations). 49 U.S.C. 20103(d). Furthermore, the statute requires FRA to consider issuing rules codifying waivers that have been in effect for 6 years. For codification, these 6-year-old waivers must also meet the criteria of being "in the public interest" and "consistent with railroad safety;" the data and metrics proposed in the NPRM will help FRA determine if these waivers meet the statutory standard. 49 U.S.C. 20103(d)(4).

3. A Description of and, Where Feasible, an Estimate of the Number of Small Entities to Which the Proposed Rule Applies

The RFA requires a review of proposed and final rules to assess their impact on small entities, unless the Secretary certifies that the rule would not have a significant economic impact on a substantial number of small entities. "Small entity" is defined in 5 U.S.C. 601 as a small business concern that is independently owned and operated and is not dominant in its field of operation. The U.S. Small Business Administration (SBA) has authority to regulate issues related to small businesses, and stipulates in its size standards that a "small entity" in the railroad industry includes a for-profit "line-haul railroad" that has fewer than 1,500 employees and a "short line railroad" with fewer than 1,500 employees.²²

Federal agencies may adopt their own size standards for small entities in consultation with SBA and in conjunction with public comment. Under that authority, FRA has published a final statement of agency policy that formally establishes "small

entities" or "small businesses" as railroads, contractors, and hazardous materials shippers that meet the revenue requirements of a Class III railroad as set forth in 49 CFR part 1201, General Instruction 1–1, which is \$20 million or less in inflation-adjusted annual revenues; and commuter railroads or small governmental jurisdictions that serve populations of 50,000 or less.²³ The \$20 million limit is based on the STB's revenue threshold for a Class III railroad carrier. Railroad revenue is adjusted for inflation by applying a revenue deflator formula in accordance with 49 CFR part 1201, General Instruction 1–1. The current threshold is \$46.4 million.²⁴ FRA is using this definition for the proposed rule.

Based on railroads that report to FRA under 49 CFR part 225 (Railroad Accidents/Incidents), FRA estimated the universe of small railroads consists of 812 Class III railroads. Because any railroad may request a waiver, all 812 Class III railroads may be affected by this proposed rule. Considering waiver requests actually submitted to FRA in the year 2023, about 40 percent of petitioners were small railroads, or on average about 28 out of the estimated 70 annual waiver petitions. As mentioned in the regulatory analysis for the NPRM, there are several categories of waiver requests that already require consultation and will mitigate the number of affected railroads. For example, about 215 Class III railroads participate in a waiver granting relief from provisions of 49 U.S.C. 21103(a)(4), regarding the required number of hours off-duty before initiating an on-duty period for train employees. When the association representing Class III railroads, the American Short Line and Regional Railroad Association (ASLRRA), petitioned to add more of its members to this waiver, ASLRRA noted the railroads had sought input from employees.²⁵ In addition, other rulemakings may codify waivers so that a small railroad would not need to submit a waiver request for the regulatory part covered by that rulemaking, making consultation unnecessary. For example, the ReflectORIZATION of Rail Freight Rolling Stock (ReflectORIZATION) NPRM would provide relief to railroads operating

equipment used in Tourist, Historic, Excursion, Educational, Recreational, or Private (THEERP) operations. These are primarily small tourist railroads. As of 2022, FRA had received waiver requests from 12 railroads operating THEERP equipment; these railroads would not need to file waiver renewals under the ReflectORIZATION rule. FRA also estimated the ReflectORIZATION rulemaking could positively affect 123 tourist railroads.²⁶

FRA is also not aware of any commuter railroads that serve cities of less than 50,000 people and would thus qualify as small entities. As noted in the regulatory analysis for the proposed rule, waiver requests to establish a quiet zone under 49 CFR part 222 already would involve extensive discussions between the local public authority and railroad. Therefore, FRA expects few affected communities under the proposed rule. However, there may be situations where small communities adjacent to railroad property for which a railroad requests a waiver, may need to be consulted; FRA expects these situations to be minimal.

Another class of affected small entities may be small railroad suppliers that request a waiver. FRA estimated the North American Industry Classification System (NAICS) code 336510 Railroad Rolling Stock Manufacturing would best represent these suppliers because that classification includes firms engaged in manufacturing rail cars and equipment for both freight and passenger service.²⁷ The SBA size standard for NAICS code 336510 is 1,500 employees.²⁸ Combined with U.S. Census data, in this industry there are 119 out of 137 firms that would qualify as small entities.²⁹ Based on FRA's experience, FRA expects most suppliers that request waivers would be either large manufacturers or associated with large manufacturers that would exceed the employment threshold to qualify as a small entity. For example, suppliers such as Wabtec Corp. and New York Air Brake are a part of the larger firms GE Transportation and Knorr-Bremse, respectively. However, suppliers may include small entities

²⁶ 87 FR 43367 (July 21, 2022).

²⁷ U.S. Census Bureau, NAICS (2022). Available at: <https://www.census.gov/naics/?input=336510&year=2022&details=336510>.

²⁸ U.S. SBA, *Table of Small Business Size Standards Matched to North American Industry Classification Codes* (Mar. 2023). Available at: <https://www.sba.gov/document/support-table-size-standards>.

²⁹ U.S. Census Bureau, *2021 SUSB Annual Data Tables by Establishment Industry, Data by Enterprise Employment Size, U.S. & states, 6-digit NAICS* (Dec. 2023). Available at: <https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html>.

²³ 68 FR 24891 (May 9, 2003) (codified at 49 CFR part 209, appendix C).

²⁴ The Class III railroad revenue threshold is \$46,352,455 or less for 2022, the most recent year available. See STB, *Economic Data*. Available: <https://www.stb.gov/reports-data/economic-data/>.

²⁵ See Docket No. FRA–2009–0078. Available: <https://www.regulations.gov/document/FRA-2009-0078-0217>.

²² "Size Eligibility Provisions and Standards," 13 CFR part 121, subpart A.

such as small electronics equipment manufacturers.

Overall, a substantial number of small railroads may be affected by this NPRM, although that number is reduced by existing consultation requirements and codification of waivers under rulemakings. FRA invites comment on the number of small entities affected.

4. A Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Rule, Including an Estimate of the Class of Small Entities That Will Be Subject to the Requirements and the Type of Professional Skill Necessary for Preparation of the Report or Record

For this NPRM, the compliance costs for affected small entities mirror the costs for all affected entities. The cost categories remain the same as in the regulatory analysis and the cost is represented by: *Cost per waiver = cost of analysis and metrics + cost of consultation and documentation + cost to show waiver renewal effectiveness and compliance.* Using the same assumptions and inputs for time, number of employees, and wage rates as used in the regulatory analysis, the cost per waiver request is calculated by: Cost per waiver = \$89.13 + \$483.24 + 483.24 + \$89.13 = \$1,145 per waiver request. Given that almost all Class III railroads that submit a waiver request submit 1 waiver request per year, the cost per waiver equals the cost per small railroad per year. FRA expects the cost per small railroad supplier will be similar. The cost is the same \$1,145 per waiver request in annualized terms at 7 percent, 3 percent, and 2 percent if the same cost is used over a 10-year period of analysis.

ASLRRRA reports that the average Class III railroad has an annual average revenue of \$4.75 million.³⁰ Thus, the estimated cost of the proposed rule per small entity is less than 0.05 percent of revenues. FRA determined that the cost would not represent a significant

economic impact. FRA realizes the average revenues likely represent a wide variety of Class III railroads in terms of employment and annual revenues. Given these are private firms, it is difficult to further classify or “break down” these railroads by employment and revenue categories to assess the impact of the NPRM in more detail. FRA requests comment on how many Class III railroads may be classified by finer ranges of employees or revenues or both.

5. Identification, to the Extent Practicable, of All Relevant Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rule

Although waiver request notifications are currently published in the **Federal Register** and open for comment, addressing these information needs early in the waiver development process would potentially result in a more streamlined and efficient waiver request “workflow,” *i.e.*, waiver disposition procedure. It would also assist FRA in adhering to the waiver review timeframe as stated in part 211.

FRA has issued guidance to characterize consultation in reference to the regulations for the Risk Reduction Program (RRP), System Safety Program (SSP), and Fatigue Risk Management Program (FRMP).³¹ That guidance refers to the terms “in good faith” and “best efforts” that are specifically noted in the statute requiring those regulations. 49 U.S.C. 20156. The terms referenced for this NPRM, “in the public interest” and “consistent with railroad safety” are different. Also, while the overall intent is for substantive “good” consultations, the information to be discussed in the consultation for this NPRM is different than the information for consultation for RRP, SSP, and FRMP. Therefore, the consultations that would be required in this NPRM would not be duplicative of the consultations described in the guidance.

6. A Description of Significant Alternatives to the Proposed Rule

In the regulatory evaluation, FRA considered an alternative modeled after its Railroad Safety Advisory Committee. In this scenario, FRA would serve as host and facilitator for potential petitioners and affected stakeholders to discuss a waiver request. FRA could clarify the terms “in the public interest” and “consistent with railroad safety” and engage parties to the waiver request for meaningful consultation. However, because FRA would be involved, rather than the petitioner and affected stakeholder communicating directly with each other, the alternative would have higher costs. In addition, for more complex waivers, the rental costs for meeting space and audio/visual equipment to enable a hybrid meeting would increase costs. Thus, the alternative would have higher total costs than the proposed rule.

C. Paperwork Reduction Act

The changes in this proposed rule, if adopted, would result in a burden increase for petitions for regulatory relief under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*). FRA reports burden hours for waivers processed in accordance with part 211 of the CFR in each of the relevant individual information collection submissions. The current number of burden hours reported for waiver submissions over 17 information collections is 674 hours. The additional hours estimated from this NPRM are 164 hours (838 – 674 = 164). The Office of Management and Budget (OMB) control numbers that would have revised requirements, as proposed in this NPRM, are listed in the table below and reflect the revised estimated burden hours. The revised burden requirements for each OMB number listed in the table will be updated in each of the relevant individual information collections, after issuance of the final rule.

OMB control No.	Title	Total annual waiver requests (A)	Average time per waiver (B)	Total annual burden hours (C = A * B)	Wage rate	Total cost equivalent in U.S. dollars (D = C * wage rates)
2130-0010	Track Safety Standards	10	4.25	42.50	89.13	\$3,788.03
2130-0526	Control of Alcohol and Drug Use in Railroad Operations.	3	4.25	12.75	89.13	1,136.41
2130-0524	Railroad Communications	2	3.25	6.50	89.13	579.35
2130-0560	Use of Locomotive Horns at Highway Rail Grade Crossings.	2	6.25	12.50	89.13	1,114.13
2130-0566	ReflectORIZATION of Freight Rolling Stock.	10	10.25	102.50	89.13	9,135.83

³⁰ ASLRRRA, *Short Line and Regional Railroad Facts and Figures* (2019 reprint of 2017 edition), p. 12. Available at: <https://www.aslrra.org/about-us/industry-facts/facts-and-figures-book/>.

³¹ FRA, *Guidance on Railroad/Employee Consultation Requirements in 49 CFR parts 270 and 271* (Oct. 2022). Available at: <https://railroads.dot.gov/elibrary/guidance-railroademployee-consultation-requirements-49-cfr-parts-270-and-271>.

railroademployee-consultation-requirements-49-cfr-parts-270-and-271.

OMB control No.	Title	Total annual waiver requests (A)	Average time per waiver (B)	Total annual burden hours (C = A * B)	Wage rate	Total cost equivalent in U.S. dollars (D = C * wage rates)
2130-0571	Occupational Noise Exposure for Rail- road Operating Employees.	0.3	3.25	0.98	89.13	86.90
2130-0005	Hours of Service	2	26.25	52.50	89.13	4,679.33
2130-0505	Inspection and Maintenance of Steam Locomotives.	1	3.25	3.25	89.13	289.67
2130-0594	Railroad Safety Appliance Standards	3	18.25	54.75	89.13	4,879.87
2130-0008	Brakes Safety Standards	2	166	332.00	89.13	29,591.16
2130-0586	Bridge Safety Standards	0.3	6.25	1.88	89.13	167.12
2130-0544	Passenger Equipment Safety Stand- ards.	12	8.25	99.00	89.13	8,823.87
2130-0545	Passenger Train Emergency Pre- paredness.	1	12.25	12.25	89.13	1,091.84
2130-0533	Certification of Locomotive Engineers	10	3.25	32.50	89.13	2,896.73
2130-0525	Certification of Glazing Materials	1	6.25	6.25	89.13	557.06
2130-0596	Conductor Certification	9	5.25	47.25	89.13	4,211.39
2130-0610	Risk Reduction Program	1	18.25	18.25	89.13	1,626.62
Total		70		838		74,655.29

D. Environmental Impact

FRA has evaluated this proposed rule in accordance with the National Environmental Policy Act (NEPA) (42 U.S.C. 4321 *et seq.*), FRA's regulations implementing NEPA, and other environmental statutes, E.O.s, and related regulatory requirements. FRA has determined that the proposed rule is categorically excluded from detailed environmental review under 23 CFR 711.116(c)(5). FRA has also evaluated this NPRM under 23 CFR 771.116(b) to determine whether the rule would involve unusual circumstances including significant environmental impacts; substantial controversy on environmental grounds; significant impact on certain Federally protected properties; or inconsistencies with any Federal, State, or local law, requirement, or administrative determination related to the environmental aspects of the action. FRA has determined that no unusual circumstances exist with respect to this rule that might trigger the need for a more detailed environmental review. As a result, FRA finds that the proposed rule is not a major Federal action significantly affecting the quality of the human environment.

E. Environmental Justice

E.O. 12898, "Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations," requires DOT agencies to achieve environmental justice as part of their mission by identifying and addressing, as appropriate, disproportionately high and adverse human health or environmental effects, including interrelated social and economic effects, of their programs, policies, and activities on minority populations and low-income

populations. DOT Order 5610.2C ("U.S. Department of Transportation Actions to Address Environmental Justice in Minority Populations and Low-Income Populations") instructs DOT agencies to address compliance with E.O. 12898 and requirements within the DOT Order 5610.2C in rulemaking activities, as appropriate, and also requires consideration of the benefits of transportation programs, policies, and other activities where minority populations and low-income populations benefit, at a minimum, to the same level as the general population as a whole when determining impacts on minority and low-income populations.³² FRA has evaluated this NPRM under E.O.s 12898, 14096, and DOT Order 5610.2C, and has determined it will not cause disproportionate and adverse human health and environmental effects on communities with environmental justice concerns.

F. Federalism Implications

This NPRM will not have a substantial effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Thus, in accordance with E.O. 13132, Federalism (64 FR 43255, Aug. 10, 1999), preparation of a Federalism Assessment is not warranted.

³² E.O. 14096 "Revitalizing Our Nation's Commitment to Environmental Justice," issued on April 26, 2023, supplements E.O. 12898, but is not currently referenced in DOT Order 5610.2C.

G. Unfunded Mandates Reform Act of 1995

This proposed rule will not result in the expenditure, in the aggregate, of \$100,000,000 or more, adjusted for inflation, in any one year by State, local, or Indian Tribal governments, or the private sector. Thus, consistent with section 202 of the Unfunded Mandates Reform Act of 1995 (Pub. L. 104-4, 2 U.S.C. 1532), FRA is not required to prepare a written statement detailing the effect of such an expenditure.

H. Energy Impact

E.O. 13211 requires Federal agencies to prepare a Statement of Energy Effects for any "significant energy action." 66 FR 28355 (May 22, 2001). FRA has evaluated this proposed rule in accordance with E.O. 13211 and determined that this rule is not a "significant energy action" within the meaning of E.O. 13211.

I. Executive Order 13175 (Tribal Consultation)

FRA has evaluated this proposed rule in accordance with the principles and criteria contained in E.O. 13175, Consultation and Coordination with Indian Tribal Governments, dated November 6, 2000. The proposed rule would not have a substantial direct effect on one or more Indian tribes, would not impose substantial direct compliance costs on Indian tribal governments, and would not preempt tribal laws. Therefore, the funding and consultation requirements of E.O. 13175 do not apply, and a tribal summary impact statement is not required.

J. International Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from engaging in any standards or related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as safety, are not considered unnecessary obstacles. The statute also requires consideration of international standards and where appropriate, that they be the basis for U.S. standards. This rulemaking is purely domestic in nature and is not expected to affect trade opportunities for U.S. firms doing business overseas or for foreign firms doing business in the United States.

K. Privacy Act Statement

In accordance with 5 U.S.C. 553(c), DOT solicits comments from the public to better inform its rulemaking process. DOT posts these comments, without edit, to www.regulations.gov, as described in the system of records notice, DOT/ALL-14 FDMS, accessible through www.dot.gov/privacy. To facilitate comment tracking and response, we encourage commenters to provide their name, or the name of their organization; however, submission of names is completely optional. Whether or not commenters identify themselves, all timely comments will be fully considered. If you wish to provide comments containing proprietary or confidential information, please contact the agency for alternate submission instructions.

L. Rulemaking Summary, 5 U.S.C. 553(b)(4)

As required by 5 U.S.C. 553(b)(4), a summary of this rulemaking can be found in the Abstract section of the Department's Unified Agenda entry for this rulemaking at <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202404&RIN=2130-AC97>.

List of Subjects in 49 CFR Part 211

Administrative practice and procedure, Rules of practice.

The Proposed Rule

For the reasons discussed in the preamble, FRA proposes to amend part 211 of chapter II, subtitle B of title 49, Code of Federal Regulations, as follows:

PART 211—RULES OF PRACTICE

■ 1. The authority citation for part 211 continues to read as follows:

Authority: 49 U.S.C. 20103, 20107, 20114, 20306, 20502–20504, and 49 CFR 1.89.

■ 2. Revise § 211.1 to read as follows:

§ 211.1 General.

(a) This part prescribes rules of practice that apply to rulemaking and waiver proceedings, review of emergency orders issued under 49 U.S.C. 20104, and miscellaneous safety-related proceedings and informal safety inquiries. Each proceeding under the Safety Act, as defined at paragraph (b)(3) of this section, shall be disposed of within 12 months after the date it is initiated. A proceeding shall be deemed to be initiated and the time period for its disposition shall begin on the date a petition or application that complies with the requirements of this chapter is confirmed to be complete by FRA.

(b) As used in this part—

(1) *Administrator* means the Federal Railroad Administrator or the Deputy Administrator or the delegate of either of them.

(2) *Waiver* includes exemption.

(3) *Safety Act* means the Federal Railroad Safety Act of 1970, as amended (49 U.S.C. ch. 201 *et seq.*).

(4) *Docket Clerk* means the Docket Clerk, U.S. Department of Transportation, Docket Operations, www.regulations.gov.

(5) *Railroad Safety Board* means the Railroad Safety Board, Office of Railroad Safety, Federal Railroad Administration, Washington, DC 20590.

(6) *In the Public Interest* means the proposed request demonstrates positive factors including, but not limited to, empowering workers, ensuring equity, protecting the environment, creating robust infrastructure, enabling adaptability and resiliency, bringing legacy systems up to current standards, allowing for experimentation consistent with railroad safety, providing opportunities to collaborate, ensuring interoperability, integrating across transportation modes, and the well-being of the public at large.

(7) *Consistent with railroad safety* means the proposal is at least as safe as or safer than the status quo (*i.e.*, without the proposed relief).

(c) Records relating to proceedings and inquiries subject to this part are available for inspection as provided in part 7 of this title.

■ 3. Amend § 211.7 by revising paragraph (b)(1) to read as follows:

§ 211.7 Filing requirements.

* * * * *

(b) * * *

(1) All petitions and applications subject to this part, including applications for special approval under §§ 211.55 and 238.21 of this chapter, petitions for approval under § 238.203

of this chapter, and signal applications under parts 235 and 236 of this chapter, shall be submitted to FRA via email to FRAWaivers@dot.gov. Each petition and application received shall be acknowledged in writing. The acknowledgment shall contain the docket number assigned to the petition or application and state the date FRA determined the petition or application was complete. Within 60 days following receipt, FRA will advise the petitioner or applicant of any deficiencies in its petition or application.

* * * * *

■ 4. Revise § 211.9 to read as follows:

§ 211.9 Content of waiver and other safety-related proceeding petitions.

Each petition for waiver or other safety-related proceeding for regulatory relief must:

(a) Specify the rule, regulation, or standard that the petitioner seeks to have waived.

(b) Explain the interest of the petitioner, and the need for the action requested; explain the nature and extent of the relief sought, and identify and describe the persons, equipment, installations, and locations to be covered by the waiver.

(c) Contain sufficient information to support the action sought including an evaluation of anticipated impacts of the action sought. Each petition pertaining to safety regulations must also contain relevant safety data and analysis to demonstrate the petition is in the public interest and consistent with railroad safety, and outline the metrics to be used to determine effectiveness of the waiver or other relief, if granted.

(d) Include documentation demonstrating meaningful good faith consultation with potentially affected stakeholders, including applicable rail labor stakeholders, on the proposed request for relief, prior to submission to FRA for evaluation and processing.

(e) In any request for renewal or expansion:

(1) provide data on the overall effectiveness of the waiver or other relief;

(2) demonstrate compliance with any conditions that were included in the previous grant of relief; and

(3) demonstrate how the waiver, suspension, or other approval for relief is, and will continue to be, in the public interest and consistent with railroad safety.

■ 5. Add § 211.10 to read as follows:

§ 211.10 Content of rulemaking petitions.

Each petition for rulemaking must:

(a) Set forth the text or substance of the rule, regulation, standard, or

amendment proposed, or specify the rule, regulation, or standard that the petitioner seeks to have repealed.

(b) Explain the interest of the petitioner, and the need for the action requested.

(c) Contain sufficient information to support the action sought including an evaluation of anticipated impacts of the action sought; each evaluation must include an estimate of resulting costs to the private sector, to consumers, and to Federal, State, and local governments as well as an evaluation of resulting benefits, quantified to the extent practicable.

■ 6. Revise § 211.11 to read as follows:

§ 211.11 Processing of petitions for rulemaking.

(a) *General.* Each petition for rulemaking filed as prescribed in §§ 211.7 and 211.10 is referred to the head of the office responsible for the subject matter of the petition to review and recommend appropriate action to the Administrator. No public hearing or oral argument is held before the Administrator decides whether the petition should be granted. However, a notice may be published in the **Federal Register** inviting written comments concerning the petition. Each petition shall be granted or denied not later than six months after its receipt by the Docket Clerk.

(b) *Grants.* If the Administrator determines that a rulemaking petition complies with the requirements of § 211.10 and that rulemaking is justified, the Administrator initiates a rulemaking proceeding by publishing an advance notice or notice of proposed rulemaking in the **Federal Register**.

(c) *Denials.* If the Administrator determines that a rulemaking petition does not comply with the requirements of § 211.10 or that rulemaking is not justified, the Administrator denies the petition. If the petition pertains to railroad safety, the Administrator may also initiate an informal safety inquiry under § 211.61.

(d) *Notification; closing of docket.* Whenever the Administrator grants or denies a rulemaking petition, a notice of the grant or denial is sent to the petitioner. If the petition is denied, the proceeding is terminated and the docket for that petition is closed.

■ 7. Revise § 211.13 to read as follows:

§ 211.13 Initiation and completion of rulemaking proceedings.

The Administrator initiates all rulemaking proceedings on the Administrator's own motion by publishing an advance notice of proposed rulemaking or a notice of

proposed rulemaking in the **Federal Register**. However, the Administrator may consider the recommendations of interested persons or other agencies of the United States. A separate docket is established and maintained for each rulemaking proceeding. Each rulemaking proceeding shall be completed not later than 12 months after the initial notice in that proceeding is published in the **Federal Register**. However, if it was initiated as the result of the granting of a rulemaking petition, the rulemaking proceeding shall be completed not later than 12 months after the petition was filed as prescribed in §§ 211.7 and 211.10.

■ 8. Amend § 211.41 by revising paragraph (b) to read as follows:

§ 211.41 Processing of petitions for waiver of safety rules.

* * * * *

(b) *Notice and hearing.* A notice is published in the **Federal Register**, an opportunity for public comment is provided (with a standard comment period of 60 days), and a hearing is held in accordance with § 211.25, before the petition is granted or denied. Any comment period shorter than 60 days must be authorized by the Administrator.

* * * * *

■ 9. Amend § 211.43 by revising paragraph (b) to read as follows:

§ 211.43 Processing of other waiver petitions.

* * * * *

(b) *Notice and hearing.* A notice is published in the **Federal Register**, an opportunity for public comment is provided (with a standard comment period of 60 days), and a hearing is held in accordance with § 211.25, before the petition is granted or denied. Any comment period shorter than 60 days must be authorized by the Administrator.

* * * * *

Issued in Washington, DC.

Amitabha Bose,

Administrator.

[FR Doc. 2024–24586 Filed 10–28–24; 8:45 am]

BILLING CODE 4910–06–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

50 CFR Part 17

[Docket No. FWS–R4–ES–2024–0051; FXES1113090FEDR–245–FF09E22000]

RIN 1018–BF55

Endangered and Threatened Wildlife and Plants; Removing Chipola Slabshell and Fat Threeridge From the Federal List of Endangered and Threatened Wildlife

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Proposed rule.

SUMMARY: We, the U.S. Fish and Wildlife Service (Service), propose to remove the Chipola slabshell (*Elliptio chipolaensis*) and fat threeridge (*Amblema neislerii*), both freshwater mussels, from the Federal List of Endangered and Threatened Wildlife due to recovery. These species occur in the Apalachicola-Chattahoochee-Flint River Basin of Alabama, Georgia, and Florida. Our review of the best available scientific and commercial data indicates that the threats to the Chipola slabshell and fat threeridge have been eliminated or reduced to the point that both species have recovered and no longer meet the definition of an endangered or threatened species under the Endangered Species Act of 1973, as amended (Act). Accordingly, we propose to delist the Chipola slabshell and the fat threeridge. If we finalize this rule as proposed, the prohibitions and conservation measures provided by the Act, particularly through sections 4 and 7 for the Chipola slabshell and sections 7 and 9 for the fat threeridge, would no longer apply to these species. This proposed rule also serves as the completed status review initiated under section 4(c)(2) of the Act.

DATES: We will accept comments received or postmarked on or before December 30, 2024. We must receive requests for public hearings, in writing, at the address shown in **FOR FURTHER INFORMATION CONTACT** by December 13, 2024.

ADDRESSES:

Written comments: You may submit comments by one of the following methods:

(1) *Electronically:* Go to the Federal eRulemaking Portal: <https://www.regulations.gov>. In the Search box, enter FWS–R4–ES–2024–0051, which is the docket number for this rulemaking. Then, click on the Search button. On the resulting page, in the Search panel on

the left side of the screen, under the Document Type heading, check the Proposed Rule box to locate this document. You may submit a comment by clicking on "Comment." Comments must be received by 11:59 p.m. Eastern Time on the closing date listed in the **DATES** section.

(2) *By hard copy:* Submit by U.S. mail to: Public Comments Processing, Attn: FWS-R4-ES-2024-0051, U.S. Fish and Wildlife Service, MS: PRB/3W, 5275 Leesburg Pike, Falls Church, VA 22041-3803.

We request that you send comments only by the methods described above. We will post all comments on <https://www.regulations.gov>. This generally means that we will post any personal information you provide us (see Information Requested, below, for more information).

Availability of supporting materials: This proposed rule and supporting documents, including the recovery plans, 5-year review, and species status assessment (SSA) reports, are available at <https://ecos.fws.gov/ecp/> and at <https://www.regulations.gov> under Docket No. FWS-R4-ES-2024-0051.

FOR FURTHER INFORMATION CONTACT: Gian Basili, Deputy State Supervisor, Florida Ecological Services Office, 7915 Baymeadows Way, Suite 200, Jacksonville, FL 32256-7517; telephone 904-731-3079; email gianfranco_basili@fws.gov. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States. Please see Docket No. FWS-R4-ES-2024-0051 on <https://www.regulations.gov> for a document that summarizes this proposed rule.

SUPPLEMENTARY INFORMATION:

Executive Summary

Why we need to publish a rule. Under the Act, a species warrants delisting if it no longer meets the definition of an endangered species (in danger of extinction throughout all or a significant portion of its range) or a threatened species (likely to become an endangered species in the foreseeable future throughout all or a significant portion of its range). The Chipola slabshell is listed as a threatened species and the fat threeridge is listed as an endangered species, and we are proposing to delist them. We have determined the Chipola

slabshell and fat threeridge do not meet the Act's definition of an endangered or threatened species. Delisting a species can be completed only by issuing a rule through the Administrative Procedure Act rulemaking process (5 U.S.C. 551 *et seq.*).

What this document does. This rule proposes the removal of the Chipola slabshell and fat threeridge from the List of Endangered and Threatened Wildlife based on their recovery; if we finalize this rule as proposed, the prohibitions and conservation measures provided by the Act, particularly through sections 4 and 7 for the Chipola slabshell and sections 7 and 9 for the fat threeridge, would no longer apply to these species.

The basis for our action. Under the Act, we may determine that a species is an endangered or threatened species because of any of five factors: (A) The present or threatened destruction, modification, or curtailment of its habitat or range; (B) overutilization for commercial, recreational, scientific, or educational purposes; (C) disease or predation; (D) the inadequacy of existing regulatory mechanisms; or (E) other natural or manmade factors affecting its continued existence. The determination to delist a species must be based on an analysis of the same factors.

Under the Act, we must review the status of all listed species at least once every five years. We must delist a species if we determine, on the basis of the best available scientific and commercial data, that the species is neither a threatened species nor an endangered species. Our regulations at 50 CFR 424.11 identify four reasons why we might determine a species shall be delisted: (1) The species is extinct; (2) the species has recovered to the point at which it no longer meets the definition of an endangered species or a threatened species; (3) new information that has become available since the original listing decision shows the listed entity does not meet the definition of an endangered species or a threatened species; or (4) new information that has become available since the original listing decision shows the listed entity does not meet the definition of a species. Here, we have determined that the Chipola slabshell and fat threeridge have recovered to the point at which they no longer meet the definition of an endangered species or a threatened species; therefore, we are proposing to delist them.

Information Requested

We intend that any final action resulting from this proposal will be based on the best scientific and

commercial data available and be as accurate and as effective as possible. Therefore, we request comments or information from other concerned governmental agencies, Native American Tribes, the scientific community, industry, or any other interested parties concerning this proposed rule.

We particularly seek comments concerning:

(1) Reasons we should or should not remove Chipola slabshell or fat threeridge from the List of Endangered and Threatened Wildlife.

(2) Relevant data concerning any threats (or lack thereof) to the Chipola slabshell or fat threeridge, particularly any data on the possible effects of climate change as it relates to habitat, as well as the extent of State protection and management that would be provided to these mussels as delisted species;

(3) Current or planned activities within the geographic range of Chipola slabshell and fat threeridge that may have adverse or beneficial impacts on these species; and

(4) Considerations for post-delisting monitoring, including monitoring protocols and length of time monitoring is needed, as well as triggers for reevaluation.

Please include sufficient information with your submission (such as scientific journal articles or other publications) to allow us to verify any scientific or commercial information you include.

Please note that submissions merely stating support for, or opposition to, the actions under consideration without providing supporting information, although noted, do not provide substantial information necessary to support a determination. Section 4(b)(1)(A) of the Act directs that determinations as to whether any species is an endangered species or a threatened species must be made solely on the basis of the best scientific and commercial data available.

You may submit your comments and materials concerning this proposed rule by one of the methods listed in **ADDRESSES**. We request that you send comments only by the methods described in **ADDRESSES**.

If you submit information via <https://www.regulations.gov>, your entire submission—including any personal identifying information—will be posted on the website. If your submission is made via a hardcopy that includes personal identifying information, you may request at the top of your document that we withhold this information from public review. However, we cannot guarantee that we will be able to do so.

We will post all hardcopy submissions on <https://www.regulations.gov>.

Comments and materials we receive, as well as supporting documentation we used in preparing this proposed rule, will be available for public inspection on <https://www.regulations.gov>.

Our final determinations may differ from this proposal because we will consider all comments we receive during the comment period as well as any information that may become available after this proposal. For example, based on the new information we receive (and if relevant, any comments on that new information), we may conclude that Chipola slabshell should remain listed as a threatened species, or we may conclude that Chipola slabshell should be reclassified from a threatened species to an endangered species. We may conclude that the fat threeridge should remain listed as an endangered species, or we may conclude that the fat threeridge should be reclassified from an endangered species to a threatened species. We will clearly explain our rationale and the basis for our final decision, including why we made changes, if any, that differ from this proposal.

Public Hearing

Section 4(b)(5) of the Act provides for a public hearing on this proposal, if requested. Requests must be received by the date specified in **DATES**. Such requests must be sent to the address shown in **FOR FURTHER INFORMATION CONTACT**. We will schedule a public hearing on this proposal, if requested, and announce the date, time, and place of the hearing, as well as how to obtain reasonable accommodations, in the **Federal Register** and local newspapers at least 15 days before the hearing. We may hold the public hearing in person or virtually via webinar. We will announce any public hearing on our website, in addition to the **Federal Register**. The use of these virtual public hearings is consistent with our regulations at 50 CFR 424.16(c)(3).

Peer Review

Species status assessment (SSA) teams prepared separate SSA reports for the Chipola slabshell and fat threeridge. The SSA teams were composed of Service biologists and staff from Texas

A&M Natural Resource Institute, who consulted with subject area experts for both species. Each SSA report represents a compilation of the best scientific and commercial data available concerning the status of these species, including the impacts of past, present, and future factors (both negative and beneficial) affecting the species.

In accordance with our joint policy on peer review published in the **Federal Register** on July 1, 1994 (59 FR 34270), and our August 22, 2016, memorandum updating and clarifying the role of peer review of listing and recovery actions under the Act, we solicited independent scientific reviews of the information contained in each of the SSA reports. We sent the Chipola slabshell SSA report to three independent peer reviewers and received two responses. We sent the fat threeridge SSA report to four independent peer reviewers and received two responses. Results of these structured peer review processes can be found at <https://www.regulations.gov>. In preparing this proposed rule, we incorporated the results of these reviews, as appropriate, into the final SSA report for each species, which are the foundation for this proposed rule.

Summary of Peer Reviewer Comments

As discussed in Peer Review above, we received comments from two peer reviewers on each of the draft SSA reports. We reviewed all comments we received from the peer reviewers for substantive issues and new information regarding the information contained in the SSA reports. The peer reviewers generally concurred with our methods and conclusions, and provided additional information, clarifications, and suggestions, including clarifications in terminology and discussions of survey information related to detection versus no detection, and other editorial suggestions. Otherwise, no substantive changes to our analysis and conclusions within either of the SSA reports were deemed necessary, and peer reviewer comments are addressed in versions 1.0 of each SSA report (Service 2020, entire; Service 2021, entire).

Previous Federal Actions

On March 16, 1998, the Chipola slabshell was listed as a threatened species (63 FR 12664) and the fat threeridge as an endangered species (63

FR 12664) under the Act. On October 1, 2003, we completed a recovery plan for both species (68 FR 56647). A 5-year review of 37 Southeastern species, including Chipola slabshell and fat threeridge, was completed on September 27, 2006 (71 FR 56545). Critical habitat was designated for the Chipola slabshell in the Chipola River main stem and seven tributaries comprising a stream length of approximately 228 km (142 mi) (72 FR 64286; November 15, 2007). Critical habitat was designated for the fat threeridge in the lower Flint River system (397 km (247 mi)), the Apalachicola River system (161 km (100 mi)), and the Chipola River system (228 km (142 mi)) (72 FR 64286; November 15, 2007). We published notices of initiation of periodic status reviews for both species as required under section 4(c)(2) of the Act in 2018 (83 FR 38320, August 6, 2018); this proposed rule serves as completion of those status reviews. Recovery plan revisions were completed for both species on August 6, 2019 (84 FR 38284). The referenced documents and additional details can be found using our Environmental Conservation Online System (ECOS): <https://ecos.fws.gov/>.

Background

Species Information

Both the Chipola slabshell and fat threeridge are members of the family Unionidae, a large group of freshwater mussels represented by 298 species in North America. Both species are endemic to the Apalachicola-Chattahoochee-Flint River (ACF) River Basin of Alabama, Georgia, and Florida. The ACF River Basin extends approximately 620 kilometers (km) (385 miles (mi)) and spans 50 counties in Georgia, 8 in Florida, and 10 in Alabama (see figure 1, below). For more details about the ACF River Basin, refer to the SSA reports (Service 2020, pp. 12–15; Service 2021, pp. 26–50).

The Chipola slabshell occurs in the mainstem of the Chipola River and several large tributaries. The fat threeridge occurs in the mainstems of the Flint River, Chipola River, and Apalachicola River. Neither species has known occurrences within the Chattahoochee River basin.

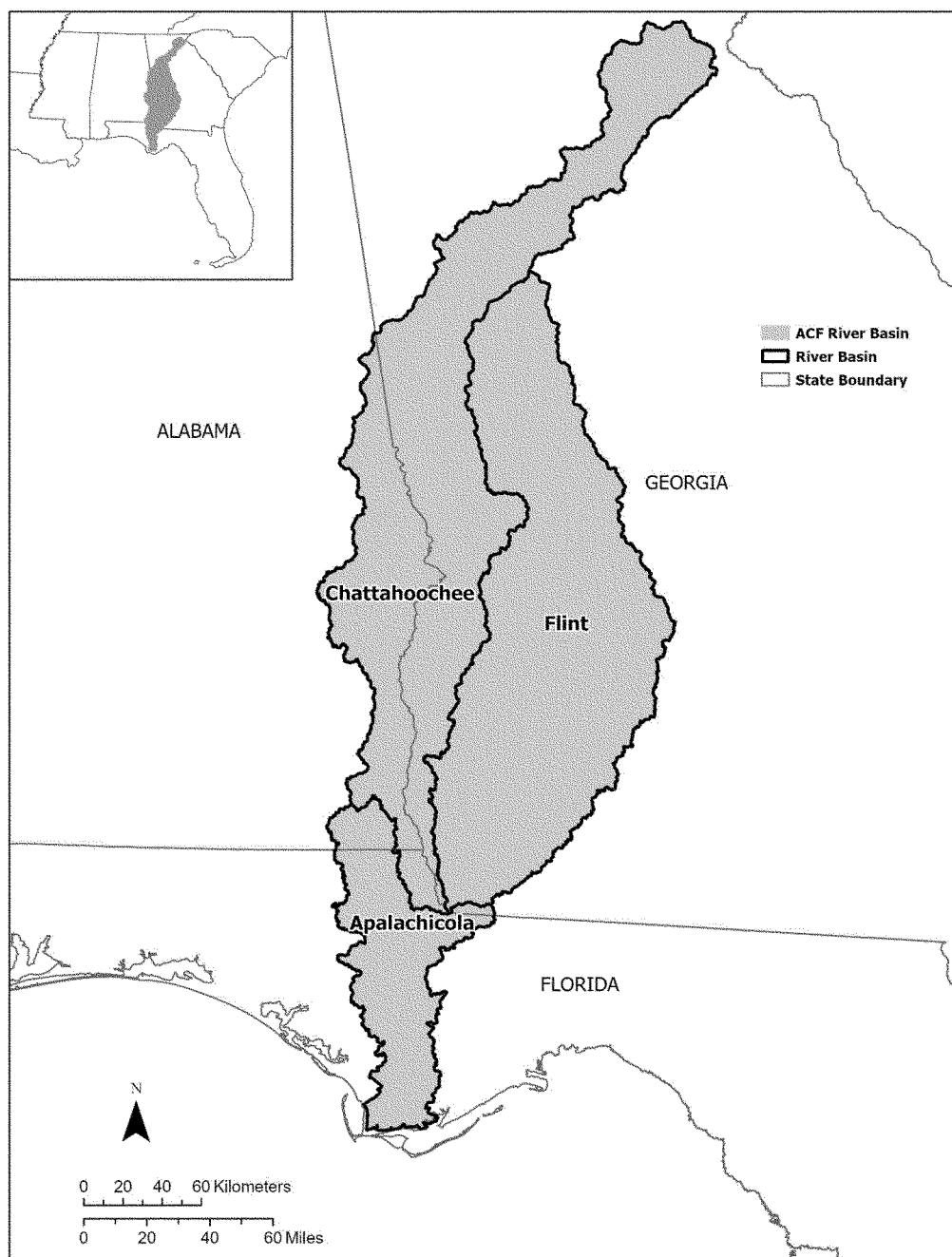


Figure 1. Large river basins within the Apalachicola Drainage of Alabama, Georgia, and Florida. The Apalachicola Basin is commonly referred to by the names of the three largest rivers, the Apalachicola, Chattahoochee, and Flint (ACF River Basin) (Service 2021, p. 27).

General Mussel Biology

Freshwater mussels, including Chipola slabshell and fat threeridge, have a complex reproduction process involving parasitic larvae, called glochidia, that are wholly dependent on host fish. Mussels release sperm into the water column, which is taken in by the

female, wherein fertilization and development of glochidia occurs in a restricted portion of the gills, called the brood pouch or marsupium. When mature, the glochidia are released to the water column to attach on the gills, head, or fins of fishes. Glochidia die if they fail to attach to a host fish, attach

to an incompatible fish species, or attach to the wrong location on a host fish (Neves 1991, p. 254; Bogan 1993, p. 599). Once attached to the host, glochidia draw nutrients from the fish's tissue as they develop (Arey 1932, pp. 214–215). Time to development, from attachment of glochidia to maturation,

ranges from just over 1 week to 6 weeks or more (Parmalee and Bogan 1998, p. 8).

Depending on the species, mussels are either short-term or long-term brooders. In short-term brooders, such as *Chipola* slabshell and fat threeridge, fertilization occurs in the spring or summer and glochidia are released shortly after they are fully developed. In long-term brooders, fertilization occurs in late summer or fall, and developed glochidia are held over winter and released in the following spring or summer (Haag 2012, pp. 39–40). Mature glochidia drop off their hosts and, if they settle in suitable habitat on the stream bottom, continue the remainder of their existence as free-living mussels. Newly released glochidia are juveniles that are reproductively immature but otherwise resemble adults, with both halves (valves) of the shell developed and poised for growth.

Freshwater mussels are relatively sedentary and, under their own power, capable of moving only short horizontal distances, typically up to a few yards or less in a year (Haag 2012, pp. 34–35). Given mussels' limited mobility, host fish are their primary mode of dispersal, and the hosts are essential for maintaining population connectivity. Host specificity varies, with some mussel species being compatible with a few fish species while others can transform from glochidia to juveniles on several fish species.

Chipola Slabshell

A thorough review of the taxonomy, life history, and ecology of the *Chipola* slabshell is presented in chapter 1 of the SSA report (Service 2020, pp. 3–24).

The *Chipola* slabshell is a freshwater mussel that does not exhibit sexual dimorphism in shell characters (Service 2020, p. 4). The species can attain a length of 85 millimeters (mm) (3.35 inches (in)), but typical length is between 47 to 76 mm (1.85 to 2.99 in). The *Chipola* slabshell has a chestnut colored periostracum (outer shell) with 1 to 4 dark annuli (growth) bands (Service 2020, p. 4). Within its range, *Chipola* slabshell is the only species with light and dark bands on periostracum and with salmon-colored nacre (inner layer of shell) inside the shell. The umbos (shell protrusions near the hinge) are prominent, well above the hingeline, thus inside the umbo cavity is deep.

Based on the size, shell characteristics, and traits from similar species in the genus *Elliptio*, the *Chipola* slabshell is thought to reach sexual maturity within 3–5 years and has an average lifespan of 15–20 years

(Service 2020, p. 8). The *Chipola* slabshell is a short-term brooder (tachytictic), meaning immature mussels (*i.e.*, glochidia) are carried in the female's gills for a short time following spawning and released that same season. Females are gravid from early June to early July. The *Chipola* slabshell is a host-fish specialist, requiring a Centrarchid (*i.e.*, sunfish) host.

Currently, the *Chipola* slabshell is widespread within its range and common at some localities. A lack of consistent survey methods across observers and through time limits the discussion of abundance trends for *Chipola* slabshell, however historical data indicate approximately 32 records whereas current records (from 2005 onward) indicate approximately 138 (Service 2020, p. 62). The species' distribution is primarily continuous in one river system, including the *Chipola* River and its tributaries. The species inhabits silty sand substrates of large creeks and the main channel of the *Chipola* River, in slow to moderate current. *Chipola* slabshell appears to be more tolerant of soft sediments than other mussel species in the ACF River Basin. It co-occurs with more silt-tolerant species in stream bank habitats with slower currents, thus it has more available habitat than mid-channel-dwelling species (Service 2020, p. 15).

Fat Threeridge

A thorough review of the taxonomy, life history, and ecology of the fat threeridge mussel is presented in chapter 2 of the SSA report (Service 2021, pp. 14–25).

The fat threeridge is an almost square, inflated, solid, and heavy shelled freshwater mussel that typically reaches up to 102 mm (4 in) in length. Older, larger individuals are quite inflated, where their width approximates their height. The dark brown to black shell is strongly sculptured with seven to eight prominent horizontal parallel ridges. The prominent, parallel ridges and inflated shell (older specimens, especially) distinguish this species from other mussels within its range (Service 2021, p. 15).

The glochidia of fat threeridge, like most freshwater mussels, are obligate parasites on fish, and must attach to a host to transform into juvenile mussels; this parasitism serves as the primary dispersal mechanism for this relatively immobile group of organisms. To facilitate attachment, fat threeridge hookless glochidia are broadcast in a web-like mass that expands and wraps around a host. This method often is seen in host generalists because passive entanglement is nonselective.

Reproductive studies confirm that fat threeridge is a host generalist, completing transformation on 23 species of fishes (Service 2021, p. 17). The fat threeridge is a short-term summer brooder. Females appear to be gravid when water temperatures reach 23.9 degrees Celsius (°C) (75 degrees Fahrenheit (°F)), usually in late May and June.

Because freshwater mussels are relatively long-lived and have limited mobility, habitat stability is a requirement shared by all unionids. Fat threeridge appears to be sensitive to the effects of sediment instability and completely reliant on stable fine sediment habitat patches. Excessive amounts of sediment and particulate matter can interfere with key aspects of mussel biology. The availability of stable sediment patches may help explain the restricted distribution in mainstem versus tributary environments, as the fat threeridge has never been found in a tributary stream. By their nature, tributaries are smaller in size than mainstems and have more dynamic flows and sediment transport (Fritz et al. 2018, p. 6). Thus, the fat threeridge is ecologically restricted/isolated to large river systems in low gradient areas with stable, very fine sediment patches (Service 2021, pp. 22–23).

Within its range in the ACF River Basin, fat threeridge is found in mainstem habitats in the Flint, Apalachicola, and *Chipola* rivers; there are no known collections from the Chattahoochee River (Service 2021, p. 26). At the time the fat threeridge was listed in 1998, there were very few existing records of the species, with the most seen at a site being 6 individuals (63 FR 12666). Current estimates in the middle Appalachicola alone are upwards of 7.7 million individuals (Service 2021, p. 47).

Regulatory and Analytical Framework

Regulatory Framework

Section 4 of the Act (16 U.S.C. 1533) and the implementing regulations in title 50 of the Code of Federal Regulations set forth the procedures for determining whether a species is an endangered species or a threatened species, issuing protective regulations for threatened species, and designating critical habitat for endangered and threatened species. On April 5, 2024, jointly with the National Marine Fisheries Service, the Service issued a final rule that revised the regulations in 50 CFR part 424 regarding how we add, remove, and reclassify endangered and threatened species and what criteria we

apply when designating listed species' critical habitat (89 FR 24300). This final rule is now in effect. The Act defines an "endangered species" as a species that is in danger of extinction throughout all or a significant portion of its range, and a "threatened species" as a species that is likely to become an endangered species within the foreseeable future throughout all or a significant portion of its range. The Act requires that we determine whether any species is an endangered species or a threatened species because of any of the following factors:

- (A) The present or threatened destruction, modification, or curtailment of its habitat or range;
- (B) Overutilization for commercial, recreational, scientific, or educational purposes;
- (C) Disease or predation;
- (D) The inadequacy of existing regulatory mechanisms; or
- (E) Other natural or manmade factors affecting its continued existence.

These factors represent broad categories of natural or human-caused actions or conditions that could have an effect on a species' continued existence. In evaluating these actions and conditions, we look for those that may have a negative effect on individuals of the species, as well as other actions or conditions that may ameliorate any negative effects or may have positive effects. The determination to delist a species must be based on an analysis of the same five factors.

We use the term "threat" to refer in general to actions or conditions that are known to or are reasonably likely to negatively affect individuals of a species. The term "threat" includes actions or conditions that have a direct impact on individuals (direct impacts), as well as those that affect individuals through alteration of their habitat or required resources (stressors). The term "threat" may encompass—either together or separately—the source of the action or condition or the action or condition itself.

However, the mere identification of any threat(s) does not necessarily mean that the species meets the statutory definition of an "endangered species" or a "threatened species." In determining whether a species meets either definition, we must evaluate all identified threats by considering the species' expected response and the effects of the threats—in light of those actions and conditions that will ameliorate the threats—on an individual, population, and species level. We evaluate each threat and its expected effects on the species, then analyze the cumulative effect of all of

the threats on the species as a whole. We also consider the cumulative effect of the threats in light of those actions and conditions that will have positive effects on the species—such as any existing regulatory mechanisms or conservation efforts. The Secretary determines whether the species meets the definition of an "endangered species" or a "threatened species" only after conducting this cumulative analysis and describing the expected effect on the species now and in the foreseeable future.

The Act does not define the term "foreseeable future," which appears in the statutory definition of "threatened species." Our implementing regulations at 50 CFR 424.11(d) set forth a framework for evaluating the foreseeable future on a case-by-case basis which is further described in the 2009 Memorandum Opinion on the foreseeable future from the Department of the Interior, Office of the Solicitor (M-37021, January 16, 2009; "M-Opinion," available online at <https://www.doi.gov/sites/doi.opengov.ibmcloud.com/files/uploads/M-37021.pdf>). The foreseeable future extends as far into the future as the U.S. Fish and Wildlife Service and National Marine Fisheries Service (hereafter, the Services) can make reasonably reliable predictions about the threats to the species and the species' responses to those threats. We need not identify the foreseeable future in terms of a specific period of time. We will describe the foreseeable future on a case-by-case basis, using the best available data and taking into account considerations such as the species' life-history characteristics, threat-projection timeframes, and environmental variability. In other words, the foreseeable future is the period of time over which we can make reasonably reliable predictions. "Reliable" does not mean "certain"; it means sufficient to provide a reasonable degree of confidence in the prediction, in light of the conservation purposes of the Act.

Analytical Framework

The SSA reports document the results of our comprehensive biological review of the best scientific and commercial data regarding the status of the Chipola slabshell and fat threeridge, including assessments of the potential threats to these species. The SSA reports do not represent our decisions on whether these species should be proposed for delisting. However, they do provide the scientific basis that informs our regulatory decisions, which involve the further application of standards within

the Act and its implementing regulations and policies.

To assess Chipola slabshell and fat threeridge viability, we used the three conservation biology principles of resiliency, redundancy, and representation (Shaffer and Stein 2000, pp. 306–310). Briefly, resiliency is the ability of the species to withstand environmental and demographic stochasticity (for example, wet or dry, warm or cold years); redundancy is the ability of the species to withstand catastrophic events (for example, droughts, large pollution events); and representation is the ability of the species to adapt to both near-term and long-term changes in its physical and biological environment (for example, climate conditions, pathogens). In general, species viability will increase with increases in resiliency, redundancy, and representation (Smith et al. 2018, p. 306). Using these principles, we identified each species' ecological requirements for survival and reproduction at the individual, population, and species levels, and described the beneficial and risk factors influencing these species' viability.

The SSA process can be categorized into three sequential stages. During the first stage, we evaluated individual species' life-history needs. The next stage involved an assessment of the historical and current condition of these species' demographics and habitat characteristics, including an explanation of how these species arrived at their current condition. The final stage of the SSA involved making predictions about each species' responses to positive and negative environmental and anthropogenic influences. Throughout all of these stages, we used the best available information to characterize viability as the ability of these species to sustain populations in the wild over time. We use this information to inform our regulatory decisions.

The following is a summary of the key results and conclusions from the SSA reports; the full SSA reports can be found at Docket No. FWS-R4-ES-2024-0051 on <https://www.regulations.gov>.

Summary of Biological Status and Threats

In this discussion, we review the biological condition of each species and their resources, and the threats that influence these species' current and future conditions, in order to assess both species' overall viability and the risks to that viability. In addition, the SSA reports (Service 2020, entire; Service 2021, entire) document our comprehensive biological status review

for each species, including an assessment of the potential threats to each species. The following is a summary of these status reviews and the best available information gathered since that time that have informed these decisions.

Species Needs

Both Chipola slabshell and fat threeridge share similar habitat needs, including stable stream channels; permanently flowing water to adequately deliver oxygen, enable passive reproduction, support host fish, deliver food items to the sedentary juvenile and adult life stages, and remove wastes; and good water quality (*i.e.*, free from harmful toxicants (such as chlorine, unionized ammonia, heavy metals, salts, pesticides), or at low enough concentrations to avoid adverse effects). The Chipola slabshell prefers predominantly sand, gravel, and/or cobble stream substrate with low to moderate amounts of silt and clay (Service 2020, pp. 15–16), whereas the fat threeridge prefers stable fine sediment habitat patches (Service 2021, p. 22).

Analysis Units

The Chipola slabshell consists of a single, panmictic population within the Chipola River basin; we delineated three subpopulations (*i.e.*, management units, MUs) to account for the two natural breaks in connectivity (Service 2020, pp. 64–65). Although these breaks do not prevent dispersal of infected host fish between subpopulations of the Chipola slabshell, we delineated the MUs based on the potential barriers to dispersal and genetic exchange. Since our knowledge of the level of genetic diversity is limited, it is possible MUs exhibit some natural variation in genetic diversity. Each subpopulation was broken into U.S. Geological Survey (USGS) 10-digit hydrologic unit codes (HUC–10s) as MUs (see table 1, below). These units reflect a spatial scale for which mussel survey data were available.

TABLE 1—HUC–10S FOR EACH CHIPOLA SLABSHELL MANAGEMENT UNIT (MU)

MU	HUC–10s
1	River Styx & Douglas Slough.
2	Merritts Mill Pond–South. Mill Creek. Tenmile Creek. Dead Lake.
3	Marshall Creek. Cowarts Creek. Merritts Mill Pond–North.

The fat threeridge also consists of a single population; we delineated six analysis units (HUC–10s) within the Flint, Chipola, and Apalachicola Rivers, based on potential reproductive isolation and/or unique geomorphology, available current occurrence records, and expert input (Service 2021, pp. 51–52).

Threats

The primary threats affecting viability of both mussel species are predominantly related to historical land use practices resulting in the destruction, modification, or curtailment of these species' habitat or range (Factor A), ultimately affecting water quality and flow regime (*i.e.*, water quantity). They are: (1) sedimentation; (2) impoundments; (3) agriculture; and (4) urbanization. Existing regulatory mechanisms (Factor D) and conservation actions have benefited the species, thus ameliorating many threats. Other threats such as invasive species (Factor C) likely have had some negative effects on the two mussel species, as described in the SSA reports, but were not considered primary threats that affect the species' overall viability (Service 2020, pp. 40–41; Service 2021, p. 76). Our analyses also considered the effects of climate change (Factor E), but sea level rise (SLR) was only examined for fat threeridge based upon the potential of SLR to affect the lower portion of its range.

Sedimentation

The primary listing factor for both the Chipola slabshell and fat threeridge was related to habitat modification, specifically the issue of increased sedimentation which causes turbidity from erosion (Service 2020, p. 27; Service 2021, p. 76). Sedimentation is one of the most significant pollution sources for aquatic organisms and is a major factor in overall mussel declines (Service 2020, p. 31), as excessive amounts of sediment and particulate matter can interfere with key aspects of mussel biology (Service 2021, p. 24).

Canopy, or riparian buffers, provide the conditions for stable stream channels, delivery of food items, and improved overall water quality because of their ability to filter runoff. Activities related to dredging, snag removal, agriculture, logging, and urban development are usually common sources of erosion and sedimentation. Dredging was a widespread, intensive, and frequent disturbance within the Apalachicola River that was detrimental to both species at the time of listing. However, over the past 20 years,

dredging practices have been restricted through regulations such that very little dredging has occurred, and future dredging activities are expected to be limited. Following the cessation of widespread dredging, signs of habitat recovery have been observed, indicating improved habitat stability for fat threeridge and other freshwater mussels (including Chipola slabshell) in the Apalachicola River (Service 2021, pp. 58–59).

In 2009, we conducted a basin threats assessment for the Chipola River in order to identify and reduce sedimentation risks to aquatic life. Unpaved roads were identified as primary contributors of sandy materials that are easily eroded and transported to stream corridors. All unpaved road-stream crossing sites were ranked and prioritized for subsequent restoration practices, and proximity to sites of listed species and their habitat was a primary consideration (Service 2020, p. 55). We began unpaved stream crossing restoration efforts in 2013, in partnership with the Florida Fish and Wildlife Commission (FWC), and several projects have reduced sediment inputs (Service 2020, p. 56).

Partnerships and programs have had success in restoring and reducing sediment inputs in priority stream reaches that have been identified as highly erodible. We and our partners, including but not limited to the University of Florida's Institute of Food and Agricultural Sciences Extension, Northwest Florida's Water Management District, Florida Department of Agriculture and Conserver Services, Natural Resources Conservation Service, FWC, the U.S. Forest Service, and many landowners (National Fish Habitat Partnership 2020, unpaginated), have successfully restored over 8 km (5 mi) of streams in the Chipola River Basin and continue to implement stream restoration projects (for example, bank stabilization, solar wells, livestock exclusion fencing, riparian restoration, low-water crossings, and reshaping of spring-fed tributaries) to reduce sediment inputs. The Southeast Aquatic Resources Partnership continues to use a Chipola River Basin threats assessment to reduce sedimentation in the basin and identify potential barriers to fish passage (Service 2020 pp. 55–56).

Impoundments

Impoundments can alter downstream water quality and riverine habitat (Service 2020, p. 28). The most consequential direct effects to Chipola slabshell and fat threeridge from impoundments include upstream and downstream flow effects, as well as the

loss of and fragmentation of riverine habitat. Pre-existing dams that fragment and inundate habitat and alter natural flow are part of existing baseline conditions for these species and are unlikely to change substantially in the near future (Service 2020, pp. 33–36; Service 2021, p. 112). Impoundments remain within tributaries of the Chipola River, but the mainstem, which contains the majority of Chipola slabshell, as well as critical habitat for fat threeridge, is unobstructed (Service 2020, p. 28; Service 2021, p. 107). The main stem of the Chipola River formerly contained one impoundment, the Dead Lake Dam, which was removed in 1987. The final obstructions to natural flow in the channel were removed in 1989. The dam removal returned connectivity and natural flow conditions to the river, but the local sediment and detritus load is likely still high (Service 2021, p. 81). However, even with the accumulated detritus, the number of fish species almost doubled after the dam was removed, with anadromous fish able to travel through the lake to spawn or seek critical thermal refugia in the upper Chipola River (Service 2020, p. 34).

Following the return of connectivity and natural flow regime of Dead Lakes, habitat conditions are anticipated to become more stable over time. Stable stream habitats are formed and maintained by natural flow regimes, channel features (dimension, pattern, and profile), and natural sediment input to the system through periodic flooding. These events help maintain connectivity and interaction with the floodplain, and consistently transport sediment load over time, such that the stream bed neither degrades nor aggrades (Service 2021, p. 22).

Agriculture

Agriculture is the largest groundwater consumer in the ACF River Basin accounting for 35 percent of all water withdrawals in 2010. Of the groundwater withdrawn in the ACF River Basin, 89 percent was withdrawn in Georgia, and about 11 percent was withdrawn in Alabama and Florida during 2010 to provide irrigation for approximately 736,200 acres (ac) (297,930 hectares (ha)) (Service 2021, p. 87). These groundwater withdrawals exacerbate drought conditions during dry years, which can affect both tributaries and main river channels (Service 2021, p. 86).

Water pollutants associated with agricultural activity may also adversely affect mussels. Ammonia is associated with nitrogenous fertilizers, wastewater from animal feedlots (livestock waste), and the effluents of older municipal

wastewater treatment plants. While nitrogen from wastewater inputs originating from septic and sewer sources are also associated with urban centers, other forms of pollution are unique to these agricultural areas (Service 2020, p. 30). Properly implemented agricultural best management practices (BMPs) have improved the water quality in several basins where Chipola slabshell and fat threeridge occur. Implementing BMPs has reduced thousands of pounds of agricultural nitrogen inputs from fertilizers and livestock waste (Service 2020, p. 51).

Agricultural land use is highest in the Lower Flint River, so impacts from stressors associated with agricultural activity could limit fat threeridge in the future. However, land use in the sub-basins with fat threeridge present has remained relatively stable from 2000–2016. A large portion of each sub-basin is also forested, which provides an effective buffer for maintaining sufficient river baseflows, permeability, and reducing overall flooding impacts (Service 2021, p. 87). Fat threeridge will likely maintain resiliency in larger river and mainstem habitats in the ACF River Basin, including the Lower Flint, if adequate water quality and quantity continue at current levels (Service 2021, pp. 129–130).

Urbanization

Urban development not only causes habitat loss and fragmentation, but it also contributes to habitat degradation through storm water runoff and nonpoint source pollution. The term “development” refers to urbanization of the landscape, including (but not limited to) land conversion for residential, commercial, and industrial uses and the accompanying infrastructure. Urbanization effects may include alterations to water quality, water quantity, and instream and streamside habitat (Ren et al. 2003, p. 649; Wilson 2015, p. 424). The effects on habitat also include variability in streamflow, typically increasing the extent and volume of water entering a stream after a storm and decreasing the time it takes for the water to travel over the land before entering the stream (Giddings et al. 2009, p. 1). Freshwater mussel populations experience reduced abundance, species richness, reproduction, growth, and survival stemming from the impacts of urbanization on water and habitat quality (Diamond and Serveiss 2001, p. 4716; Gangloff et al. 2009, p. 198; Cao et al. 2013, pp. 1212–1214; Gillis et al. 2017, pp. 674–679). While there are some parts of both the Chipola

slabshell’s range and the fat threeridge’s range that are affected by urbanization, it does not rise to the level that it is affecting current viability (see *Current Conditions* below).

Additional Water Quality and Quantity Considerations

Influences on the viability of the Chipola slabshell and fat threeridge include habitat factors such as water quantity (flow) (Service 2020, p. 28). Flow impacts are varied between low flow and high flow conditions. When water flows decrease, the concentration of water pollutants increases, thus increasing the adverse effects that can negatively impact the freshwater mussels, such as Chipola slabshell and fat threeridge, and their habitat (Service 2020, p. 32; Service 2021, p. 21).

High-flow volumes can be both harmful and beneficial for freshwater mussels. Floods are often associated with habitat destruction and direct mortality, both to juveniles and adults that are stranded in unsuitable habitats (Service 2020, p. 32; Service 2021, p. 65). Floods can also increase the potential for shear stress events to occur. Shear stress is a critical factor in affecting displacement during high-flow events where substrates are unstable, conditions are generally poor for mussel habitation. However, floods can also help remove accumulated silt deposits, algal growth and harmful organic material from sediments, improving habitat for juvenile mussels. It is likely that large woody debris can also help to potentially stabilize sediments in the Coastal Plains ecoregion where Chipola slabshell and fat threeridge occur, and as a result these areas are expected to be the most stable during high flows (Service 2020, p. 32).

Water quantity can become limited by withdrawals and be exacerbated during extreme drought events and periods of low flow. Groundwater recharge provides water to aquifers and springsheds, and alterations to groundwater removal can alter surface water flow impacting spring flow and available surface water (Service 2020, p. 41). Under moderate-flow conditions, groundwater makes up the majority of the Chipola River’s discharge and the quality of water discharged from the Chipola River springs is predominantly determined by the quality of groundwater in the Floridan Aquifer (Service 2020, p. 19). The Chipola River’s baseflow is derived principally from aquifers, therefore it is not as susceptible to drought conditions. In addition, Chipola slabshell has been found to occupy areas 1 to 2 meters (m) (3.3 to 6.6 feet (ft)) below the water

surface, providing a buffer against the effects of low flow conditions. Fat threeridge has also persisted and arguably increased in abundance through these periods of low flow (Service 2021, pg. 103).

For more information regarding threats, see chapter 3 of the Chipola slabshell SSA report and chapter 5 of the fat threeridge SSA report (Service 2020, pp. 27–140; Service 2021, pp. 76–130).

Climate Change

Impacts of climate changes can have direct effects or be driven by one or more factors working synergistically as indirect effects on species. These effects may be neutral, positive, or negative and they may change over time. Despite the recognition of potential climate effects on ecosystem processes, there is uncertainty about what the exact climate future for the southeastern United States will be and how ecosystems and species in this region will respond. The greatest threat from climate change may come from synergistic effects. That is, factors associated with a changing climate may act as risk multipliers by increasing the risk and severity of more imminent threats, especially for rivers in wide flood plains where stream channels have room to migrate (Elliot et al. 2014, pp. 67–68). As a result, impacts from land use change might be exacerbated under even a mild to moderate climate future. A suite of potential hydrological impacts to waters of the southeastern United States is possible under conditions of climate change, but climate models generally predict increases in extreme rainfall events and droughts of greater duration and intensity (Carter et al. 2018, pp. 745–746).

Flooding

Tropical storms occur across the range of Chipola slabshell and fat threeridge, and they have become more intense during the past 20 years. The wind speeds and rainfall associated with hurricanes are likely to increase as the climate continues to warm (United States Environmental Protection Agency (USEPA) 2016b, p. 1, USEPA 2016c, p. 1). In October 2018, Hurricane Michael substantially impacted northwest Florida. According to a report by the Florida Forest Service (FFS), more than 2.8 million ac (1.13 million ha) of forest land were damaged by storm winds. The Chipola River experienced severe impacts, where 75 percent of upland and bottomland trees were damaged (FFS 2018, pp. 1, 4–5). However, high woody debris loading has greatly

contributed to the formation of stable, fine sediment habitat in the Lower Chipola River (Kaeser et al. 2019, p. 667), resulting in net positive effects of blowdown for Chipola slabshell and fat threeridge assuming forest cover regenerates.

The increased intensity of hurricanes as well as more frequent high-intensity precipitation events could also increase inland flooding. The precipitation received during heavy storms has increased by 27 percent in the Southeast with the trend for increasingly heavy rainfall events likely to continue into the future (USEPA 2016b, p. 2). With these heavy rainfall events comes flooding, as rivers overtop their banks more frequently, and more water accumulates in low-lying areas that drain slowly. Restoring and preserving flood protection and nutrient reduction capabilities of forested lands along the Chipola River is vital (Northwest Florida Water Management District (NFWFMD) 2018, p. 6).

Drought

Long-term climate records suggest that decade-long “mega-droughts” have occurred periodically during the past 700 years in the southeastern United States, including in the ACF River Basin (Stahle et al. 2007, p. 147). Projections for the ACF watershed indicate that future droughts are likely to be more intense (Yao and Georgakakos 2011, entire). This suggests that while the recently observed droughts in 2006–2008 and 2010–2012 were exceptional based on our recent <100-year period of record, they may not be exceptional compared to historic episodes (Pederson et al. 2012, entire).

The duration and severity of droughts may vary within the ranges of Chipola slabshell and fat threeridge. Droughts are likely to be more severe in some locations as periods without rain may be longer and very hot days will be more frequent. Dry spells are expected to be up to 20 days shorter during the cold season in the southern half of Florida, and up to 20 days longer for the same season in Alabama (Keellings and Engstrom 2019, p. 1). While more intense cold season droughts might not be as stressful for mussels as intensification of droughts during the warm season would be, a cool season drought may limit recharge and storage of water in both natural and anthropogenic reservoirs (Engstrom and Keellings 2018, p. 261; Keellings and Engstrom 2019, p. 3). More frequent or severe droughts may reduce streamflow in some areas. In Alabama, the total amount of water running off into rivers or recharging ground water is likely to

decline 2.5 to 5 percent, as increased evaporation offsets the greater rainfall (USEPA 2016b, p. 2). Low flows have decreased in the southeastern United States between 1940 and 2019, meaning streams are carrying less water at low flow than historically recorded (USEPA 2016a, p. 2). Low flows have not gone below 200 cubic feet per second (cfs) in the Chipola River in the recent past (1986 to 2019; USGS National Water Resources, 2019, entire), but may in the future.

The Chipola River is a spring-fed river with baseflow derived principally from aquifers, and therefore is not as susceptible to drought conditions derived from changes in precipitation patterns as it is to alterations in groundwater withdrawals. Mussel sites in the Chipola River generally have slopes greater than 20 percent, which helps to limit mussel mortality to less than 1 percent of the local population during low flow events (Service 2016b, p. 125). In addition, Chipola slabshell have been found to occupy areas 1 to 2 m (3.3 to 6.6 ft) below the water surface, providing a buffer against the effects of low flow conditions (Service 2016b, p. 129). Even during severe drought conditions in 2007, Cowarts Creek (which joins Marshall Creek to form the Chipola River) did not exhibit signs of mussel mortality (Garner et al. 2009, p. 693). Cowarts Creek retained adequate dissolved oxygen (6.5 milligrams per liter (mg/L) (81.5 percent saturation)) and temperature (27 °C (81 °F)), though the flow was sluggish and phytoplankton seemed elevated (Garner et al. 2009, p. 688).

Sea Level Rise

Most freshwater mussels are intolerant of saline conditions. The potential for sea level rise (SLR), and thus intrusion of saline conditions, is considered for the fat threeridge range; however, the Chipola slabshell’s range is not likely to be affected. Exposure to saline conditions (salt at 3 to 6 parts per trillion (ppt)) can decrease the reproduction and survival of freshwater mussels (Blakeslee et al. 2013, p. 2849). The upper limit for exposure of most adult unionid mussels to long-term salinity stress is < 6 ppt, which may be consistent with fat threeridge tolerances. Fat threeridge is not known to occur below the point of tidal influence in the Apalachicola River, where salt exposure is expected to be lethal. An increase in salinity of fresh waters through the intrusion of seawater associated with sea level rise will likely modify community composition of unionids in affected areas, eliminating or at least reducing the abundance of species that

are less adapted to increased salinity (Johnson et al. 2018, p. 67).

Climatic changes, including SLR and shifts in seasonal precipitation, temperature, and storm cycles, are major threats to south Florida. Various studies (University of Florida Geoplan 2015, p. 13; The Nature Conservancy 2011, p. 4–6; Sweet et al. 2017, p. 22–23) have developed scenarios that range from less than 0.3 m to 3.2 m (1 to 10.4 ft) of SLR in the south Florida by 2100. Tidal gauges around Florida have shown 25 cm (10 in) of SLR since 1913, with an increase in SLR of 2.56 mm/year (0.1 inch/year) from 1967 to 2019, equivalent to 25 cm (9.8 inches) in 100 years more locally (NOAA 2021, n.p.). This recent acceleration suggests that the intermediate to high SLR scenarios are more likely to occur than the low and intermediate-low scenarios (Sweet et al. 2022, pp. 20–21). Sea level rise since 2000 has generally been within the trajectory of the Intermediate-High scenario, but it is important to note the trajectory could change throughout the century. Rapid ice sheet collapse in Antarctica could move SLR from the intermediate to the high scenario by the end of the century (Sweet et al. 2022, p. 26). Under the high scenario, some areas supporting fat threeridge (*e.g.*, the Lower Apalachicola) will likely become partially inundated (*i.e.*, under water) at some point during this century (Service 2021, p. 102).

Conservation Efforts and Regulatory Mechanisms

Since the listing of Chipola slabshell as an endangered species and fat threeridge as a threatened species under the Act in 1998, Federal agencies have been required under section 7 of the Act to coordinate with us to ensure actions that they carry out, fund, or authorize will not jeopardize either species' continued existence or destroy or adversely modify the critical habitat designated for these species in 2007. This requirement has protected both Chipola slabshell and fat threeridge throughout most of their ranges. Both Federal and State regulations are relevant to the maintenance of water quality where Chipola slabshell and fat threeridge occur.

Water quantity can become limited by agricultural, irrigation, municipal, and industrial withdrawals. Such withdrawals can be exacerbated during extreme drought events and periods of low flow. Groundwater recharge provides water to aquifers and springheads, and alterations to groundwater removal can alter surface water flow impacting spring flow and available surface water. The State of

Florida establishes minimum flow limits (MFLs) to identify the limit at which withdrawals would be significantly harmful to the water resources or ecology of an area. Water reservation is a legal mechanism in Florida that functions to set aside water from consumptive uses for the protection of fish and wildlife or public health and safety (2023 Florida Statutes at section 373.223). Water reservations and MFLs are both important tools to ensure an adequate supply of water for citizens and environment. There is no known comparable mechanism to protect flows in Alabama. Water reservations were established for the Chipola and Apalachicola rivers in 2006 (Florida Administrative Code, rule 40A–2.223). The magnitude, duration and frequency of observed flows are reserved, essentially in total, for the protection of fish and wildlife of the Chipola River, Apalachicola River, associated floodplains, and Apalachicola Bay.

Federal guidelines are in place to minimize alterations to flow regimes. The Service and USEPA proposed instream flow guidelines for protecting riverine ecosystems under a possible interstate water allocation formula between Alabama, Florida, and Georgia for the ACF Basin. Although the three States failed to agree upon an allocation formula and the ACF compact authorizing their negotiations expired in 2003, the Service has applied the instream flow guidelines in consultations with Federal agencies on actions affecting the species addressed in this proposed rule. At minimum, the Environmental Resource Permit Program within the USEPA regulates the construction, alteration, maintenance, removal, modification and operation of all activities in uplands, wetlands and all other surface waters that alter, divert and change the flow of surface waters. Both State and Federal permits may be required to alter wetlands and other surface waters.

Future water quantity models in the Chipola River Basin have projected adequate water supply for citizens and the environment through 2045, even in drought years (NFWFMD 2023, p. ix). Water flows for most of the Chipola slabshell's and fat threeridge's occupied range are protected through consumptive uses by water reservation (legal protection), while other areas are supported by ground water contributions from springs during drought (Service 2020, pp. 96–139; Service 2021, p. 112). Water quantity models are updated every 5 years to ensure sufficient supply planning.

Regional water plans in Georgia are developed in accordance with the Georgia Comprehensive State-wide Water Management Plan (State water plan), which was adopted by the General Assembly in January 2008. The State water plan requires the preparation of regional water development and conservation plans to manage water resources in a sustainable manner through 2050. A water conservation plan is required of all permit holders operating in the Flint River basin. This requirement will benefit fat threeridge resiliency in the future by ensuring permits are sufficiently protective of necessary water quantity and quality. These plans detail best water management practices to be followed, provide direction for funding conservation practices, describe permit conditions for withdrawal permits, and provide guidance for how to minimize and control water loss (Georgia Department of Natural Resources (GADNR) 2006, pp. 161–163).

Minimum water quality standards have been set by Federal agencies both through the Clean Water Act (CWA; 33 U.S.C. 1251 *et seq.*) and other initiatives. The CWA is a Federal law that regulates the discharge of pollutants into surface waters, including lakes, rivers, streams, wetlands, and coastal areas. USEPA and the Service and National Marine Fisheries Service agreed to a national consultation on the CWA Section 304(a) aquatic life criteria as part of a Memorandum of Agreement regarding interagency coordination under the CWA and the Act (66 FR 11202; February 2, 2001). In 2013, the USEPA released new ammonia criteria that included acute and chronic toxicity testing for 13 freshwater mussels, thus leading to an improved understanding of ammonia toxicity and setting a more protective ammonia criteria value for freshwater mussels (USEPA 2013, p. xi). In 2016, the Florida Department of Environmental Protection (FDEP) adopted the chronic criteria for ammonia as both the acute and chronic values (1.408 mg/L), therefore improving the ammonia standard even further for the conservation of freshwater mussels statewide (USEPA 2016a, entire). Georgia Department of Natural Resources' (GADNR) Environmental Protection Division (EPD) also implements the 2013 ammonia criteria as part of their National Pollutant Discharge Elimination System (NPDES) permitting process (GADNR 2022, pp. A–16–17).

Florida has established water classifications that promote water quality standards that are more stringent than those of the CWA. The Florida

Department of Environmental Protection (FDEP) designates Outstanding Florida Waters (OFWs) under 2023 Florida Statutes section 403.061(27). An OFW is defined by FDEP as a waterbody worthy of special protection because of its natural attributes. In general, FDEP cannot issue permits for direct discharges to OFWs that would lower ambient (existing) water quality. FDEP also may not issue permits for indirect discharges that would significantly degrade a nearby waterbody designated as an OFW. The majority of waterbodies and segments in the range of Chipola slabshell and fat threeridge receive regulatory protection through designation as OFWs in addition to protections under their surface water classification as class III waterbodies, which include designated uses for fish consumption, recreation, and propagation and maintenance of a healthy, well-balanced population of fish and wildlife (Service 2020, appendix B). Further, the Florida Springs and Aquifer Protection Act of 2016 (2023 Florida Statutes at section 373.801–373.813) established Outstanding Florida Springs (OFSs) that require additional protections to ensure their conservation and restoration. Under this act, the State of Florida designated the Jackson Blue Spring within the Chipola River Basin as an OFS.

Section 303(d) of the CWA (33 U.S.C. 1251 *et seq.*) requires states to identify waters that do not fully support their designated use classification, and so are deemed impaired. The most recent assessments within the range of Chipola slabshell and fat threeridge were completed by the FDEP and Alabama Department of Environmental Management (ADEM) as of 2018 and GDNR in 2022. Impaired water bodies are placed on each State's 303(d) list, and a total maximum daily load (TMDL) must be developed for the pollutant of concern. A TMDL is an estimate of the total load of pollutants that a segment of water can receive without exceeding applicable water quality criteria. There are several reasons why an impaired waterbody may be delisted, including but not limited to: a subsequent assessment determining that a waterbody-parameter is no longer impaired based on current water quality standards, if there has been a TMDL completed for the verified impaired parameter; or if a flaw in a previous assessment has been determined.

Impaired waterbodies within watersheds occupied by Chipola slabshell and fat threeridge are largely impacted by fecal coliform. The standards for fecal coliform (*e.g.*,

Escherichia coli) relate to human health and do not necessarily reflect levels that would be harmful to mussels. While some waters are impaired due to nutrients or organic enrichment, these standards are in place to protect human health and do not relate directly to the potential effects of nutrients such as nitrogen on mussels. Monitoring results in Georgia indicate that approximately 60 percent of the streams are impaired for fecal coliform bacteria, with less than 2 percent for ammonia toxicity, which would adversely affect mussels, and those ammonia-impaired streams are not within the range of fat threeridge (GADNR 2022, p. 3–3). The numeric nutrient criteria (NNC) and ammonia standard in Florida reflect nutrient impact thresholds for mussels. This criterion includes total nitrogen (TN) and total phosphorus (TP) for flowing freshwaters. The TN NNC threshold concentrations are 0.67 mg/L for the Chipola River (Panhandle West), which is well below the newly adopted 1.408 mg/L ammonia concentration in Florida (Service 2016a, p. 6). Alabama also has a nitrate/nitrite nitrogen and ammonia standard in addition to other standards that are more representative of the potential harm to mussels than the nutrient or organic enrichment standard, which are no longer used as part of the water quality assessment process (ADEM 2018, pp. 11–14). Many of the delisted waterbodies were previously impaired due to elevated mercury levels in fish, which is also a human-health related standard (FDEP 2013, p. ii) that does not reflect levels that would be harmful to mussels. Given the parameters resulting in impairment and the establishment of TMDLs, water quality within the range of Chipola slabshell and fat threeridge is considered unimpaired in regards to freshwater mussel water quality thresholds.

Current Conditions

Under the SSA framework, we assessed current resiliency, redundancy, and representation for Chipola slabshell and fat threeridge. Resiliency reflects a species' ability to withstand stochastic events (arising from random factors). Resiliency is measured at the population-level using metrics that characterize population health such as demographic rates and population size. We also consider the nature and extent of stressors to a species that could limit resiliency. Populations demonstrating resiliency are better able to withstand perturbations associated with demographic stochasticity (*e.g.*, fluctuations in birth or mortality rates), environmental stochasticity (*e.g.*,

variation in precipitation or temperature), and anthropogenic activities. For the species to be considered viable, there must be adequate redundancy (suitable number, distribution, and connectivity of populations to allow the species to withstand catastrophic events). Redundancy improves with increasing numbers of populations distributed across the species range, and connectivity (either natural or human-facilitated) that allows connected populations to “rescue” each other after catastrophes. We can best gauge redundancy by analyzing the number and distribution of populations relative to the scale of anticipated species-relevant catastrophic events. Representation refers to the genetic and environmental diversity within and among populations that contributes to the ability of the species to respond and adapt to changing environmental conditions over time. The more representation, or diversity, a species has, the more it can adapt to changes (natural or human caused) in its environment. We can best gauge representation by examining the breadth of genetic, phenotypic, and ecological diversity found within a species and its ability to disperse and colonize new areas. For more information, see chapter 4 in each of the SSA reports (Service 2020, pp. 61–92; Service 2021, pp. 51–75).

Chipola Slabshell

Our current condition analysis for the singular Chipola slabshell population describes the conditions of each of the three MUs (see table 1, above). The magnitude and scale of potential impacts to Chipola slabshell or its habitat by a given threat are considered based on the condition of the watershed. Each HUC–10 watershed within the three MUs was rated as currently being in poor, fair, good, or excellent condition for each of the resiliency factors. Resiliency measures included two population factors (occupancy and abundance/recruitment) and two habitat factors (sedimentation and canopy) that were scored to provide overall MU resiliency (table 2, below). The four condition categories were then converted to numerical ranks and then a weighted average of the factor scores was calculated to generate an overall resiliency score. See the SSA report for details on the scoring methodology (Service 2020, pp. 89–91).

TABLE 2—SUMMARY OF CONDITION CATEGORIES AND RESILIENCY FACTORS TO ASSESS CHIPOLA SLABSHELL'S CURRENT RESILIENCY

Condition category	Population factors (since 2005)		Habitat factors	
	Occupancy (proportion of occupied HUC–10s)	Abundance & recruitment (# individuals and evidence of reproduction)	Sedimentation index (a) Density of road crossings and transmission lines, percent non-natural cover, and (b) soil loss potential	Canopy (% 200-ft buffer with ≥50% canopy cover within assessed stream length)
Excellent	Consistent occupation in addition to newly occupied.	>100 (live) during a given sampling event; suggests a healthy population (e.g., likely ongoing recruitment).	0–0.08: (a) minimal; (b) low	>90.
Good	Consistent occupancy	10–100 (live or dead); more than one age class represented.	0.09–0.23: (a & b) low	76 to 90.
Fair	<50% Decreased occupancy	<10 individuals (live or dead); potentially represented only by older individuals with limited recruitment.	0.24–0.36: (a & b) moderate	50 to 75.
Poor	≥50% Decreased occupancy	Only dead observed; population reduction likely not offset by recruitment.	0.37–0.76: (a) maximal; (b) moderate to high.	<50.
Ø	No occupancy in HUC–10	No records	N/A	N/A.

Within the single population for Chipola slabshell, there are currently two MUs that demonstrate moderate to high resiliency and one that has low resiliency (table 3, below). MU 1 has only one watershed, whereas MU 2 and MU 3 are each comprised of several watersheds. Although the range is narrow (*i.e.*, solely within the Chipola

River), current occupancy of the entire range is evident. Sedimentation, a risk to all mussels, is not a threat in the Chipola River Basin, as indicated by good to excellent indices in all but two areas of MU 3. Although the resiliency of MU 3 is overall low, we note that occupancy is excellent throughout this MU. The SSA report noted that the

species is thought to occur in relatively low densities naturally, and the northern part of the range in MU 3 is considered marginal habitat for the slabshell (Service 2020, p. 92). Thus, Chipola slabshell exhibits sufficient resiliency throughout its current range, contributing to overall species viability.

TABLE 3—SUMMARY OF CURRENT RESILIENCY FOR CHIPOLA SLABSHELL MANAGEMENT UNITS (MUS)

MU	HUC–10s	Population factors		Habitat factors		Watershed score	Overall MU resiliency
		Occupancy	Abundance & reproduction	Sedimentation index	Canopy		
1	River Styx & Douglas Slough.	Excellent	Good	Excellent	Excellent	High	High.
2	Merritts Mill Pond—South.	Good	Good	Good	Excellent	Moderate	Moderate.
	Mill Creek	Good	Excellent	Good	Good	Moderate.	
	Tenmile Creek	Good	Excellent	Excellent	Good	High.	
	Dead Lake	Good	Good	Excellent	Good	Moderate.	
3	Marshall Creek	Excellent	Fair	Fair	Good	Low	Low.
	Cowarts Creek	Excellent	Good	Fair	Good	Moderate.	
	Merritts Mill Pond—North.	Excellent	Fair	Good	Excellent	Moderate.	

High redundancy for Chipola slabshell is defined as multiple resilient MUs distributed throughout the species' range. Two-thirds of the species' range has moderate to high levels of resiliency. We considered all three MUs as contributing to redundancy, thus enabling the species to withstand catastrophic events. Most of the population is not currently at risk from habitat modification, indicated by high-ranking habitat factors and watershed

scores (table 3, above), and there is a high degree of land protection where the Chipola slabshell habitat is buffered by forested public lands, protecting water quality and ensuring the viability of the population and ultimately the species as a whole.

Representation, which refers to the breadth of genetic and environmental diversity within and among populations, reflects the species' adaptive capacity. Currently, there is

limited information pertaining to genetic variation and no evidence to support delineating multiple representation units for Chipola slabshell (Service 2020, p. 74). However, the breadth of environmental diversity within the range (*e.g.*, the north-south gradient with headwater streams to mainstems of the Chipola River and the Apalachicola River) is currently occupied. Our knowledge of the level of genetic diversity for Chipola slabshell is

limited; however, it is possible subpopulations exhibit some natural variation in genetic diversity. Chipola slabshell representation has not likely changed over time, but as a narrow endemic, the species' adaptive potential is limited.

Fat Threeridge

Current condition for fat threeridge describes the condition of the six analysis units. Characteristics of

resiliency for fat threeridge include evidence of stable or increasing population trends, and evidence of reproduction (either direct observation of juveniles, or of multiple age classes as inferred by length data). An adequate number of resilient populations should be distributed throughout the species range to both protect adaptive capacity of the species, and protect from catastrophic events. We analyzed the resilience of units within the range of fat

threeridge slightly differently than we did for Chipola slabshell due to differences in habitat use and perceived stressors. We assessed demographic resiliency factors including abundance, recruitment, and occupancy which inform population trends within the population, and we evaluated habitat resiliency factors related to water quality and water quantity to establish a baseline from which to project future condition (table 4, below).

TABLE 4—SUMMARY OF CONDITION CATEGORIES AND RESILIENCY FACTORS TO ASSESS CURRENT RESILIENCY FOR FAT THREERIDGE

Condition category	Population factors			Habitat factors	
	Abundance	Recruitment	Habitat occupancy	Water quality	Water quantity
High	Recent density and population estimate at high end of known range (>1 per square meter (m ²); >1 million). Increasing or stable population trend.	Presence of multiple age classes (individuals > and <50 mm); small individuals (≤35 mm) detected using hydraulic dredge methods.	71–100% or maximal occupancy.	No known or anticipated contaminant or sediment problems given the land cover.	Lower relative risk of direct and indirect impacts to the survival, health, or recruitment of species from low flow events.
Moderate	Recent density and population estimate at lower end of known range (≤1/m ² to 0.11/m ² ; >100k to 1 million). Increasing or stable population trend.	Presence of multiple age classes (individuals > and <50 mm); but no small individuals (≤35 mm) detected using hydraulic dredge methods.	31–70% or intermediate occupancy.	Associated contaminant or sediment issues are likely in some areas.	N/A.
Low	No population estimate, generally known to be present at low density (5–10 individuals minimum and/or ≤0.1/m ²). Possible stable trend since 2000, but undetectable in the past.	Only one size class ≥50 mm; no small individuals (≤35 mm) detected using hydraulic dredge methods.	<30% or minimal occupancy.	Associated contaminant or sediment issues increases the risk of negative impacts throughout habitat.	Higher relative risk of direct and indirect impacts to the survival, health, or recruitment of species from low flow events.
Very Low	Not assessed (N/A)	N/A	N/A	Associated contaminant or sediment levels pose the highest relative risk to habitat; Significant, widespread, or prolonged impacts likely occurring.	N/A.
Ø	None	None	None	N/A	Intermittent flow; no survival.

For each population and habitat factor, we considered whether the analysis units were currently in high, moderate, low, or very low condition

(table 5, below). None of the analysis units are extirpated or in very low condition. The average of factor rankings was used to generate an overall

resiliency score. For more details on the scoring methodology, see chapter 4 of the SSA report (Service 2021, pp. 56–70).

TABLE 5—FAT THREERIDGE RESILIENCY FACTORS AND OVERALL RESILIENCY

Analysis unit	Population factors			Habitat factors		Overall resiliency
	Abundance	Evidence of recruitment	Occupation	Water quality	Water quantity	
Lower Flint	Low	High	High	Low	High	Moderate.
Upper Apalachicola	Moderate	High	Low	Moderate	High	Moderate.
Middle Apalachicola	High	High	High	High	High	High.
Lower Apalachicola	Moderate	High	Moderate	High	High	High.
Lower Chipola	High	High	High	Moderate	High	High.
Chipola NDL *	Low	High	High	Moderate	High	Moderate.

* North of Dead Lakes.

Overall, fat threeridge is more abundant (currently estimated at approximately 12 million individuals) and more widely distributed than when the species was listed (Service 2021, p. 47). When the species was listed in 1998, the most individuals seen at a site

was 6 (63 FR 12666); current estimates across 164 sites in the middle Apalachicola alone are over 7.7 million individuals (Service 2021, p. 47). The positive trends for both population and habitat factors, including relatively large population

sizes, are indicative of populations that are resilient to stochastic factors. Redundancy for the fat threeridge is moderate to high, as currently all analysis units in the species range exhibit moderate to high resiliency. Each unit contributes to overall species

redundancy, or the ability of the species to withstand catastrophic events. Further, the species currently has not had a contraction or disruption of connectivity (such as from an impoundment) within its range and this connectivity corresponds to a lowered risk of extirpation from catastrophic events (Service 2021, p. 72).

The available genetic data for fat threeridge suggests little variation across the species range. This is supported by the absence of notable behavioral, morphological, or life history variation. This suggests genetic variation within the species is low. However, the species maintains ecological diversity in its occupancy of different river “types” (e.g., small and large river systems) and ecoregions (e.g., Southeastern Plains and Southern Coastal Plain). Overall, representation or adaptive capacity of fat threeridge is limited, as supported by little genetic variation within a narrow geographic range.

Future Conditions

The main factor influencing the viability of both Chipola slabshell and fat threeridge is habitat degradation or loss through land use change (e.g., urbanization, agriculture). Land use change can lead to direct impacts on viability through increases in sedimentation and contaminants within waters occupied by each mussel species. Predicting future stream-channel conditions, particularly sedimentation, in the ACF River Basin remains a challenge, as the ongoing remobilization of sediments is difficult to separate from the cumulative effects of climate and land-use change (Elliott et al. 2014, p. 66). An increase in the contaminant load from incompatible land uses is

expected to continue in varying degrees, depending on a combination of factors including the impacts of climate change across the landscape, with habitat degradation or loss likely to be more significant in some MUs/analysis units compared to others. We attempted to discern this variance by analyzing spatially explicit models of future land use and climate change as indicators of associated water quality and water quantity conditions.

We identified the main drivers of change for the future scenario analyses to be human population growth and subsequent urbanization and land use change. Land use change may have synergistic effects with climate change, so several common climate projections are considered in the assessment of future condition. Species and ecosystems are impacted by the habitat degradation and loss associated with population growth, including impacts to water pollution, local climate conditions, and disturbance dynamics.

Chipola Slabshell

Future conditions of the Chipola slabshell were assessed under three plausible future scenarios (lower, moderate, and higher) incorporating a range of conditions associated with climate and land use change (Service 2020, pp. 96–125). The future scenarios were based, in part, on the results of climate-informed land use change (USGS’s FOREcasting SCEnarios of Land-use Change (FORE–SCE)), with special report emissions scenario (SRES) B1 for the lower range, SRES A1B for moderate, and SRES A2 for the higher range, combined with Intergovernmental Panel on Climate Change (IPCC) climate models, with

representative concentration pathway (RCP) 4.5 for the lower range, RCP 6.0 for moderate, and RCP 8.5 for higher range, that projected general changes in habitat used by the Chipola slabshell. The factors that influence resiliency in the species (e.g., occupancy, abundance, sediment, canopy) either change minimally from the current condition (lower range scenario) or worsen to a moderate (moderate range scenario) or greater degree (higher range scenario) based on potential future climate and land use and their impacts on water quality and quantity. The expected future resiliency of each MU was forecasted based on events that were projected to occur under each scenario (Service 2020, pp. 208–133). All scenarios assumed that current conservation efforts, which are in place regardless of listing status, would remain in place but that no new actions would be taken. As with current condition estimates, estimates were scaled up to MU and the population levels (table 6, below).

The three scenarios project Chipola slabshell viability 20 and 40 years into the future, with each timestep representing approximately two generations. This projection was chosen to represent a time frame where climate change impacts may become apparent, while effects of management actions can be implemented and realized on the landscape. The 40-year timeframe, which includes approximately 4 to 5 generations, is also reasonable for this relatively long-lived (15 to 20 years) species, with relatively low fecundity, to respond to potential changes on the landscape.

TABLE 6—RESILIENCY SUMMARY FOR CHIPOLA SLABSHELL MUS INCLUDING CURRENT CONDITION, AND EACH OF THREE FUTURE SCENARIOS (LOWER, MODERATE, HIGHER RANGE) AT THE END OF THE 40-YEAR ASSESSMENT PERIOD

MU	Watershed (HUC–10)	Current		Lower range scenario		Moderate range scenario		Higher range scenario	
		Watershed score	Overall MU resiliency	Watershed score	Overall MU resiliency	Watershed score	Overall MU resiliency	Watershed score	Overall MU resiliency
1	River Styx & Douglas Slough.	High	High	High	High	High	High	Moderate	Moderate.
2	Merritts Mill Pond—South.	Moderate	Moderate	Moderate	Moderate	Low	Moderate	Very Low	Low.
	Mill Creek	Moderate		High		Moderate		Moderate	
	Tenmile Creek	High		High		High		High	
	Dead Lake	Moderate		Moderate		Moderate		Moderate	
3	Marshall Creek	Low	Low	Low	Low	Very Low	Very Low	Very Low	Very Low.
	Cowarts Creek	Moderate		Moderate		Very Low		Very Low	
	Merritts Mill Pond—North.	Moderate		Moderate		Low		Low	

In the lower range scenario, we project no loss in MU resiliency and redundancy compared to the current condition. Management units 1 and 2 would retain resiliency (in high or

moderate resiliency), and MU 3 would remain at low resiliency. For this scenario, the Chipola slabshell population is expected to persist in much the same condition as it is found

currently, with some increases in watershed resiliency through time given positive trends (e.g., future forest cover, recent population expansions).

In the moderate range scenario, a loss of some resiliency and redundancy is expected. Management units 1 and 2 retain resiliency, but MU 3 may become extirpated given its overall very low resiliency. The one watershed in MU 1 is expected to retain high resiliency. The condition of MU 2 is expected to decrease slightly, with reduced resiliency in one (of four) watersheds by 2060. Management unit 2 is expected to retain more than one watershed with moderate or high resiliency, while MU 3 is expected to retain only one occupied watershed (Merritts Mill Pond—North), in low resiliency.

In the higher range scenario, we anticipate impacts to resiliency in all management units. Management unit 1 has moderate resiliency with a reduced capacity to mitigate stochastic events. Management units 2 and 3 exhibit reduced resiliency (low and very low, respectively), with MU 3 likely extirpated. Management unit 2 retains resiliency in the center of the Chipola slabshell range within the Mill Creek and Tenmile Creek watersheds, with sparse to no observable presence in the Merritts Mill Pond—South and Dead Lake watersheds. Similar to the moderate range scenario, redundancy would be reduced to three watersheds with likely extirpation in three of eight currently extant watersheds. Only MU 2 retains more than one watershed with resiliency, and MU 3 retains only one occupied watershed (Merritts Mill Pond—North) with low resiliency.

The northern portion of the species range comprising the Chipola River headwaters (MU 3) was the most susceptible to change through time; MU 3 has low resiliency for current condition and is projected to have very low resiliency under the higher range scenario. It is important to note that the habitat in MU 3 is thought to be inherently variable with regards to sedimentation and has overall low suitability for Chipola slabshell. With

the exception of small portions of MUs 1 and 3, almost the entirety of the Chipola slabshell population is contained within the Chipola River mainstem in MU 2. Management unit 2 is projected to retain moderate resiliency to 2060 under the lower and moderate range scenarios, but resiliency is reduced by 2060 under the higher range scenario. Management unit 2 retains one watershed (Tenmile Creek) at high resiliency through all scenarios and projection periods. Management unit 1 is also projected to retain high to moderate resiliency under all scenarios, benefitting from the presence of extensive protected areas and more suitable large stream habitats for Chipola slabshell.

Fat Threeridge

Based on our review of factors affecting viability of fat threeridge, we focused our evaluation of future conditions on projected habitat degradation associated with two prevalent land uses in the ACF River Basin, agricultural and urban development, and their associated stressors to water quality and quantity. We also assessed potential impacts of SLR in lower portions of the Apalachicola and Chipola Rivers through removal of suitable habitat from projected saltwater inundation. We assessed resiliency, redundancy, and representation for fat threeridge under three SLR threat levels (intermediate, high, and extreme) and two multi-faceted scenarios incorporating variations in future land and water use. We summarized changes in land use within each of the fat threeridge analysis subwatersheds to assess future changes in nonpoint source pollution. We assessed both the change in the percent forested area in riparian buffers, and also the degree of urbanization and agricultural land use within subwatersheds, similar to what we assessed in current condition. To assess

future water quantity, we used the same modeling outputs as in current condition, which provided annual predictions for the time frame 2045–2075. We extracted results for two climate scenarios, RCP 4.5 and RCP 8.5, to bound plausible future outcomes and compared these against a historical simulated state (1950–2005). Annual inputs of both historical and potential future land-cover type and percent impervious area were used to incorporate the effects of changing vegetation and impervious area.

Scenario 1 assumes that conditions in the ACF River Basin continue for the next 50 years along their current trajectory, with climate change trajectories for SRES A2 and RCP 8.5 incorporated. Scenario 2 assumes that conditions in the ACF River Basin continue for the next 50 years along a modified trajectory, with climate change trajectories for SRES B1 and RCP 4.5 incorporated. We analyzed these future threats and their effects on habitat as indicators of directional change in resiliency compared to the current condition (table 7, below). We modeled threats 50 years into the future to project the conditions of analysis units in 2070. This timeframe is biologically appropriate (representing two or three generations) and within the available and reliable modeling timeframe for projecting future threats. The 50-year timeframe, which includes approximately 4 to 5 generations, is also reasonable for this relatively long-lived (15 to 40 years) species, with relatively low fecundity, to respond to potential changes on the landscape. Timeframes earlier than 2070 may be too short to observe a species response (based on a lifespan of at least 30 years) or change in threats, and beyond 2070 were considered too far into the future to reliably account for either. The land and water use threat assessment was completed within the six analysis units.

TABLE 7—SUMMARY OF FAT THREERIDGE CURRENT AND FUTURE RESILIENCY BY ANALYSIS UNIT *

Analysis unit	Current resiliency	Future intermediate sea level rise (SLR)		Future high SLR ²		Future extreme SLR ²	
		Scenario 1 ¹	Scenario 2	Scenario 1	Scenario 2	Scenario 1	Scenario 2
Lower Flint	Mod	Mod	Mod	Mod	Mod	Mod	Mod.
Upper Apalachicola	Mod	Mod	Mod	Mod	Mod	Mod	Mod.
Middle Apalachicola	High	Mod	High	Mod	High	Mod	High.
Lower Apalachicola	High	High	High	Low	Low	Low	Low.
Lower Chipola	High	High	High	High	High	Low	Low.
Chipola NDL	Mod	Mod	Mod	Mod	Mod	Mod	Mod.

* Changes in water quality and quantity inform degree of habitat degradation for scenarios 1 and 2, while NOAA SLR projections (intermediate and high) influence habitat removal by 2070.

¹ Scenario 1 includes changes in water quality for the Middle Apalachicola that result in partial habitat degradation.

² High and Extreme SLR involves partial removal of Lower Apalachicola.

Future habitat degradation associated with land use change is not expected to impact fat threeridge significantly. No analysis units are projected to become extirpated under any scenario, but one high resiliency unit (Lower Apalachicola) may transition to low resiliency in the future primarily due to SLR effects. Redundancy is maintained in the future, regardless of scenario, as most (four of six) analysis units retain moderate to high resiliency under the most severe projections. Even under high SLR, fat threeridge is projected to maintain representation in each river system (*i.e.*, Apalachicola, Chipola, and Flint) and in each ecoregion (*i.e.*, Southeastern Plains and Southern Coastal Plain).

By using the SSA framework to guide our analyses of scientific information documented in the SSA reports, we have analyzed both individual and cumulative effects on each species through characterizing species condition currently and under various plausible future scenarios. We assumed in our modeling of future conditions for both species that increased habitat degradation could result from increased land use or from climate change, or a combination. The impacts of climate change, along with habitat degradation or loss, are likely to be more significant in some MUs/analysis units than others, however, our projections indicate that both species maintain resiliency. Both species are projected to maintain a broad distribution throughout the ACF River Basin, across a variety of habitats and under both continuation and increased threat scenarios, meaning representation and redundancy are not expected to change.

We note that, by using the SSA framework to guide our analysis of the scientific information documented in the SSA reports, we have analyzed the cumulative effects of identified threats and conservation actions on these species. To assess the current and future condition of each species, we evaluate the effects of all the relevant factors that may be influencing the species, including threats and conservation efforts. Because the SSA framework considers not just the presence of the factors, but to what degree they collectively influence risk to the entire species, our assessment integrates the cumulative effects of the factors and replaces a standalone cumulative-effects analysis.

Recovery Criteria

Section 4(f) of the Act directs us to develop and implement recovery plans for the conservation and survival of endangered and threatened species

unless we determine that such a plan will not promote the conservation of the species. Under section 4(f)(1)(B)(ii), recovery plans must, to the maximum extent practicable, include objective, measurable criteria which, when met, would result in a determination, in accordance with the provisions of section 4 of the Act, that the species be removed from the Lists of Endangered and Threatened Wildlife and Plants.

Recovery plans provide a roadmap for us and our partners on methods of enhancing conservation and minimizing threats to listed species, as well as measurable criteria against which to evaluate progress towards recovery and assess the species' likely future condition. However, they are not regulatory documents and do not substitute for the determinations and promulgation of regulations required under section 4(a)(1) of the Act. A decision to revise the status of a species or to delist a species is ultimately based on an analysis of the best scientific and commercial data available to determine whether a species is no longer an endangered species or a threatened species, regardless of whether that information differs from the recovery plan.

There are many paths to accomplishing recovery of a species, and recovery may be achieved without all of the criteria in a recovery plan being fully met. For example, one or more criteria may be exceeded while other criteria may not yet be accomplished. In that instance, we may determine that the threats are minimized sufficiently and that the species is robust enough that it no longer meets the definition of an endangered species or a threatened species. In other cases, we may discover new recovery opportunities after having finalized the recovery plan. Parties seeking to conserve the species may use these opportunities instead of methods identified in the recovery plan. Likewise, we may learn new information about the species after we finalize the recovery plan. The new information may change the extent to which existing criteria are appropriate for identifying recovery of the species. The recovery of a species is a dynamic process requiring adaptive management that may, or may not, follow all of the guidance provided in a recovery plan.

In 2003, we published a recovery plan for seven mussel species, including the Chipola slabshell and fat threeridge (Service 2003, entire). In 2019, we amended the Chipola slabshell and fat threeridge recovery plans to revise the recovery criteria and site-specific recovery actions (Service 2019a, entire;

Service 2019b, entire). Both recovery plans for the Chipola slabshell and fat threeridge provide three criteria for delisting.

Chipola Slabshell

For Chipola slabshell, the criteria to delist are: (1) the one existing population must exhibit a stable or increasing trend, natural recruitment, and multiple age classes; (2) the population from criterion 1 occupies each of the three delineated units to protect against extinction from catastrophic events and maintain adaptive potential; and (3) threats are addressed and/or managed to the extent that the species will remain viable into the foreseeable future.

Criterion 1

Criterion 1 states that the one existing population must exhibit a stable or increasing trend, natural recruitment, and multiple age classes. Currently, the Chipola slabshell is known from one panmictic population within the Chipola River Basin. It is currently widespread throughout its range and common at some localities. The comparison between historical and current distribution shows an expansion north, south, and east of the species' previously known range. Occupancy has increased over time, although the magnitude of this estimate varies with spatial scale. Prior to 1991, the Chipola slabshell occupied 46 km (29 mi) in 6 U.S. Geological Survey (USGS) 10-digit hydrologic unit codes (HUC-10s) watersheds, and its current range has expanded to occupy 112 km (69 mi) in 7 HUC-10 watersheds. This increase in occupancy suggests a robust distribution throughout the known range (Service 2020, p. 62).

Our current condition resiliency analysis examined abundance and reproduction across the range. Currently two HUC-10 watersheds have excellent abundance and reproduction, four HUC-10 watersheds have good abundance and reproduction, and two HUC-10 watersheds have fair abundance and reproduction. While there are some portions of the range with lower abundances and levels of recruitment, overall the Chipola slabshell population has multiple age classes showing natural recruitment, and the species has an expanded range. Thus, we conclude that this criterion has been met for Chipola slabshell.

Criterion 2

Criterion 2 states the population (as identified in criterion 1) occupies each of the three delineated units to protect against extinction from catastrophic

events and maintain adaptive potential. All three delineated units, or subpopulations, of Chipola slabshell are currently occupied, with two of the three having moderate to high resiliency. Thus, we conclude that this criterion has been met for Chipola slabshell.

Criterion 3

Criterion 3 for consideration of delisting Chipola slabshell states that threats have been addressed or managed to the extent that the species will remain viable into the foreseeable future. At the time of listing, Chipola slabshell faced a variety of threats from declines in water quality, loss of stream flow, riparian and instream fragmentation, and deterioration of instream habitats. Additionally, these threats were expected to be exacerbated by climate change and urbanization.

Future water quantity models (updated every 5 years) in the Chipola River Basin have projected adequate water supply for citizens and the environment through 2045, even in drought years (NFWMD 2023, p. ix). Water flows for most of the Chipola slabshell's occupied range are protected through consumptive uses by water reservation (legal protection), while other areas are supported by ground water contributions from springs during drought (Service 2020, pp. 96–139). Urbanization models have projected little growth in the river basin through 2060 (Service 2020, pp. 27–60 and pp. 95–138).

During the most recent status review, there was no documentation of any significant threats to the species or its habitat, as well as no evidence that the species has experienced curtailment of range or habitat, or is affected by disease or predation, commercial or recreational harvest, the inadequacy of existing regulatory mechanisms, or any other natural or manmade factor (Service 2020, p. 140). Thus, we conclude that this criterion has been met for Chipola slabshell.

Fat Threeridge

For fat threeridge, the criteria to delist are: (1) at least four populations exhibit a stable or increasing trend, evidenced by natural recruitment and multiple age classes; (2) at least one population from criterion 1 occupies each of the Flint and Chipola Rivers sub-basins, and one population occupies two of the three delineated units in the Apalachicola River sub-basin for fat threeridge; (3) threats have been addressed or managed to the extent that each species will remain viable into the foreseeable future

(Service 2019a, pg. 4, and Service 2019b, pg. 6).

Criterion 1

Criterion 1 states that at least four populations exhibit a stable or increasing trend, evidenced by natural recruitment and multiple age classes. Since the last 5-year review in 2007, our knowledge of fat threeridge has increased substantially in all three river systems, including what we know about distribution, habitat use, and life history characteristics relevant to species recovery. As a result, we now consider the fat threeridge to consist of one population, with six analysis units. Further, we know that the species occupies most watersheds where it was found historically, and our resiliency analysis indicates that the species maintains moderate to high resiliency in the six analysis units. One of the population factors for resiliency is evidence of recruitment, and all six units exhibit recruitment through observation of small size classes. Its range has expanded in the Chipola and Apalachicola Rivers in Florida. Furthermore, fat threeridge is more abundant and widely distributed among mesohabitats than previously thought, including within deep habitats (Service 2021, pp. 54–55). Thus, fat threeridge has stable trends in all six units, and high levels of recruitment, with an overall indication that multiple age classes exist in each unit throughout the population. For these reasons, we conclude that fat threeridge has met this criterion.

Criterion 2

Criterion 2 for consideration of delisting fat threeridge states that at least one population occupies each of the Flint and Chipola Rivers sub-basins and in the Apalachicola River sub-basin at least one population occupies two of the three delineated units (Service 2019b, p. 6). As described in the SSA report, there are six subpopulations (also referred to as analysis units): one in the Flint, three in the Apalachicola, and two in the Chipola Rivers sub-basins (Service 2021, p. 52). Resiliency is moderate in the Lower Flint, Upper Apalachicola, and Chipola North of Dead Lakes analysis units; it is high in the Middle Apalachicola, Lower Apalachicola, and Lower Chipola analysis units (Service 2021, p. 69). Based on this, we conclude that criterion 2 has been met for fat threeridge.

Criterion 3

Criterion 3 for consideration of delisting fat threeridge states that threats

have been addressed or managed to the extent that the species will remain viable into the foreseeable future. The primary threats to fat threeridge include land use change resulting in reduced water quality and quantity, and effects associated with climate change, including sea level rise (SLR). Our future conditions analysis indicates that at the watershed scale, the amount of land development through 2070 is projected to be low across all scenarios (Service 2021, pp. 115–116). No analysis units are expected to become extirpated, but two high resiliency units (Lower Apalachicola, Lower Chipola) may transition to low resiliency in the future as a result of SLR effects as projected in the high SLR scenarios (Service 2021, p. 127).

Redundancy is maintained under future scenarios, as most (four of six) analysis units retain resiliency under the most severe projections, and no change from the current condition is expected under intermediate SLR. Even under extreme SLR, ecoregion and river representation for fat threeridge is maintained.

Increased sampling efforts and a better understanding of the species' habitat associations indicate a wider distribution of the fat threeridge than previously understood. In general, fat threeridge is more abundant and widely distributed among habitats than previously thought. Habitat mapping and species distribution modeling in the Apalachicola and Lower Chipola Rivers indicates sufficient abundance of habitat for the fat threeridge in these populations; similar habitat mapping has not been done at that scale for the Flint River, but habitat for the population at Newton, Georgia has supported the fat threeridge since 2006 (Service 2021, pp. 41–50). For these reasons, we conclude that this criterion has been met for fat threeridge.

Determinations of Chipola Slabshell and Fat Threeridge Status

Section 4 of the Act (16 U.S.C. 1533) and its implementing regulations (50 CFR part 424) set forth the procedures for determining whether a species meets the definition of an endangered species or a threatened species. The Act defines an “endangered species” as a species that is in danger of extinction throughout all or a significant portion of its range, and a “threatened species” as a species that is likely to become an endangered species within the foreseeable future throughout all or a significant portion of its range. The Act requires that we determine whether a species meets the definition of an endangered species or a threatened

species because of any of the following factors: (A) the present or threatened destruction, modification, or curtailment of its habitat or range; (B) overutilization for commercial, recreational, scientific, or educational purposes; (C) disease or predation; (D) the inadequacy of existing regulatory mechanisms; or (E) other natural or manmade factors affecting its continued existence.

Status Throughout All of Their Range

After evaluating the threats to these species and assessing the cumulative effects of the threats under the Act's section 4(a)(1) factors, we find that both the Chipola slabshell and fat threeridge have expanded distributions with nearly all populations having moderate to high resiliency and projections to maintain resiliency into the future. The primary threat at the time of listing was habitat loss and destruction. Based on our analyses of the current and future condition for the Chipola slabshell and fat threeridge, each species currently has sufficient resiliency and is projected to maintain resiliency into the future such that each species can withstand stochastic and catastrophic effects from existing and future threats. Together the current and future conditions analyses informed our determination as to whether each species is in danger of extinction throughout all of its range (*i.e.*, whether each species meets the definition of an endangered species under the Act) or whether each species is in danger of extinction throughout all of its range in the foreseeable future (*i.e.*, whether each species meets the definition of a threatened species under the Act). Our determinations for each species are discussed below.

Chipola Slabshell—Status Throughout All of Its Range

The Chipola slabshell is currently widespread throughout its range and considered common at some localities. Since the time of listing, surveys indicate expansion of its previously known range. Two-thirds of the range have moderate to high resiliency, and the one MU, or sub-population, that has low resiliency (MU 3) has a high proportion of marginal habitat for the species, and naturally low numbers of Chipola slabshell. Despite this, occupancy is good to excellent throughout the range. To summarize the species' current condition, the Chipola slabshell has sufficient resiliency to withstand stochastic events, as well as sufficient redundancy in the distribution of subpopulations with moderate to high resiliency such that

the species can withstand catastrophic events.

Potential threats to the species, including habitat degradation which led to the species being listed, appear to be well managed or minimized to the greatest extent possible either through protection, implementation of BMPs, and regulations in CWA or State OFW designations. Sedimentation, which is usually a major threat for mussel species, is not a current threat to Chipola slabshell in the Chipola River Basin. Thus, after assessing the best available information, we determine that Chipola slabshell is not in danger of extinction throughout all of its range.

We next evaluate whether the Chipola slabshell is likely to be in danger of extinction throughout its range within the foreseeable future. We considered climate change and land use change as primary stressors influencing habitat degradation and loss, and we developed three scenarios that project Chipola slabshell viability 40 years into the future. This 40-year foreseeable future includes a time frame where both climate change and land use change effects will become apparent on the landscape. The timeframe also includes up to five generations which we consider reasonable for this relatively long-lived (15 to 20 years), low fecundity species to respond to potential changes on the landscape. We are able to reliably predict both the threats to the species and the species' response to those threats within this timeframe.

Almost the entirety of the Chipola slabshell population is contained within the Chipola River mainstem. The core of the population (MU 2) is projected to retain moderate resiliency to 2060 under the Lower and Moderate Range Scenarios, but resiliency could be reduced by 2060 under the higher range scenario. Despite this, two thirds of the watersheds that make up MU 2 retain moderate to high resiliency through all scenarios and projection periods. In addition, MU 1 is also projected to retain moderate to high resiliency under all scenarios, benefitting from the presence of extensive protected areas and available suitable large stream habitats for Chipola slabshell. Thus, species' viability is sustained within two of the three MUs into the future. The species' ability to retain resiliency 40 years into the future supports the determination that the Chipola slabshell is not in danger of extinction throughout all of its range in the foreseeable future.

Thus, after assessing the best available information, we conclude that Chipola slabshell is not in danger of extinction now or likely to become so in the

foreseeable future throughout all of its range.

Chipola Slabshell—Status Throughout a Significant Portion of Its Range

Under the Act and our implementing regulations, a species may warrant listing if it is in danger of extinction or likely to become so in the foreseeable future throughout all or a significant portion of its range. Having determined that the Chipola slabshell is not in danger of extinction or likely to become so in the foreseeable future throughout all of its range, we now consider whether it may be in danger of extinction (*i.e.*, endangered) or likely to become so in the foreseeable future (*i.e.*, threatened) in a significant portion of its range—that is, whether there is any portion of the species' range for which both (1) the portion is significant; and, (2) the species is in danger of extinction or likely to become so in the foreseeable future in that portion. Depending on the case, it might be more efficient for us to address the "significance" question or the "status" question first. We can choose to address either question first. Regardless of which question we address first, if we reach a negative answer with respect to the first question that we address, we do not need to evaluate the other question for that portion of the species' range.

In undertaking this analysis for the Chipola slabshell, we choose to address the status question first. We began by identifying portions of the range where the biological status of the species may be different from its biological status elsewhere in its range. For this purpose, we considered information pertaining to the geographic distribution of (a) individuals of the species, (b) the threats that the species faces, and (c) the resiliency condition of populations.

We evaluated the range of the Chipola slabshell to determine if the species is in danger of extinction now or likely to become so in the foreseeable future in any portion of its range. The range of a species can theoretically be divided into portions in an infinite number of ways. We focused our analysis on portions of the species' range that may meet the definition of an endangered species or a threatened species. For the Chipola slabshell, we considered whether the threats or their effects on the species are greater in any biologically meaningful portion of the species' range than in other portions such that the species is in danger of extinction now or likely to become so in the foreseeable future in that portion.

The Chipola slabshell is found solely in the ACF River Basin, which extends approximately 620 km (385 mi). This

species is a narrow endemic functioning as single, contiguous population and the MUs used do not represent biological populations, rather they were delineated as analysis units. However, these MUs could be considered portions, and one MU (MU 3) may represent a portion of the range that could have a different status. Management unit 3, comprised of marginal habitat and located in the Chipola River headwaters, currently has low resiliency and could possibly become extirpated (projected to have very low resiliency) in the foreseeable future. Thus, this could be a portion of the range that may be in danger of extinction now or within the foreseeable future. Having answered the status question affirmatively for MU 3, we then considered whether this unit is significant.

To assess whether MU 3 is significant, we considered whether the area occupies a relatively large or particularly high-quality or unique habitat. Management unit 3 is not large, as it comprises less than one third of the known range of the species. We also examined whether the unit or characteristics within the unit make the species less susceptible to certain threats than other portions of the species' range, such that it could provide important population refugia in the event of extirpations elsewhere in the species' range. Although MU 3 contributes to the overall species-level representation and redundancy, it does not contain high quality nor high value habitat or any habitat or resources unique to that area. For these reasons, we do not find this portion to be significant. Therefore, this unit does not represent a significant portion of the range, and we find that the species is not in danger of extinction now or likely to become so in the foreseeable future in any significant portion of its range. This does not conflict with the courts' holdings in *Desert Survivors v. Department of the Interior*, 321 F. Supp. 3d 1011, 1070–74 (N.D. Cal. 2018), and *Center for Biological Diversity v. Jewell*, 248 F. Supp. 3d 946, 959 (D. Ariz. 2017) because, in reaching this conclusion, we did not apply the aspects of the Final Policy on Interpretation of the Phrase "Significant Portion of Its Range" in the Endangered Species Act's Definitions of "Endangered Species" and "Threatened Species" (79 FR 37578; July 1, 2014), including the definition of "significant" that those court decisions held to be invalid.

Determination of Status—Chipola Slabshell

Our review of the best scientific and commercial data available indicates that

the Chipola slabshell does not meet the definition of an endangered species or a threatened species in accordance with sections 3(6) and 3(20) of the Act. In accordance with our regulations at 50 CFR 424.11(e)(2) currently in effect, the species has recovered to the point at which it no longer meets the definition of an endangered species or a threatened species. Therefore, we propose to remove the Chipola slabshell from the Federal List of Endangered and Threatened Wildlife.

Fat Threeridge—Status Throughout All of Its Range

Fat threeridge is more abundant and widely distributed than previously thought. Current positive trends for both population and habitat factors, including relatively large population sizes with evidence of recruitment, are indicative of populations that are resilient to stochastic factors. All six analysis units across the species range exhibit moderate to high resiliency. The distribution of each resilient unit contributes to the species' ability to withstand catastrophic events. Further, the species has not experienced a change in connectivity—such as an impoundment—within its range, which is what generally corresponds to a lowered risk of extirpation from catastrophic events. For these reasons, we determined that the fat threeridge is not currently in danger of extinction throughout its range.

We then considered whether the species may be likely to become in danger of extinction within the foreseeable future throughout its range. We considered threats 50 years into the future to project the conditions of the six analysis units to 2070. For fat threeridge, this timeframe is biologically appropriate (representing two or three generations) and within the available and reliable modeling timeframe for projecting future water quality and quantity, threats of urbanization and SLR. Timeframes earlier than 2070 were considered too short to observe a species response (based on a lifespan of at least 30 years) or noticeable change in threats, and beyond 2070 were considered too far into the future to reliably account for species response.

Future water quality and quantity degradation associated with land use change is not expected to impact fat threeridge. Over the 50-year timeframe, no analysis units are projected to become extirpated. Two currently high resiliency units (Lower Apalachicola, Lower Chipola) may transition to low resiliency in the future under the most extreme SLR effects. Species' redundancy is maintained in the future,

regardless of scenario, as most (four of six) analysis units retain moderate to high resiliency under the most severe projections. Even under extreme SLR, fat threeridge is projected to maintain moderate to high resiliency in all but one analysis unit, thus representation is projected to be maintained in each river system (*i.e.*, Apalachicola, Chipola, and Flint Rivers) and in each ecoregion (*i.e.*, Southeastern Plains and Southern Coastal Plain). For these reasons, we conclude that the fat threeridge is not in danger of extinction now or likely to become so in the foreseeable future throughout all of its range.

Fat Threeridge—Status Throughout a Significant Portion of Range

In undertaking this analysis for fat threeridge, we choose to address the status question first. We began by identifying portions of the range where the biological status of the species may be different from its biological status elsewhere in its range. For this purpose, we considered information pertaining to the geographic distribution of (a) individuals of the species, (b) the threats that the species faces, and (c) the resiliency condition of populations.

We evaluated the range of the fat threeridge to determine if the species is in danger of extinction now or likely to become so in the foreseeable future in any portion of its range. The range of a species can theoretically be divided into portions in an infinite number of ways. We focused our analysis on portions of the species' range that may meet the definition of an endangered species or a threatened species. For fat threeridge, we considered whether the threats or their effects on the species are greater in any biologically meaningful portion of the species' range than in other portions such that the species is in danger of extinction now or likely to become so in the foreseeable future in that portion.

The fat threeridge is found solely in the ACF River Basin, which extends approximately 620 km (385 mi). This species is a single, contiguous population and the units delineated for our analysis do not represent biological populations. We determined that two units together, representing the lower portion of the species' range (Lower Apalachicola and Lower Chipola) are a portion of the range that may have a different status due to effects related to SLR. Current resiliency for this portion is high, therefore the fat threeridge is not in danger of extinction now in this portion of the range, but future projections indicate that this portion could change from high resiliency to low resiliency under the high and extreme SLR scenarios within the

foreseeable future. Thus, we considered this a portion of the range that could become in danger of extinction in the foreseeable future.

We next considered whether this portion constitutes a significant portion of the fat threeridge's range. To assess its significance, we evaluated whether the area is relatively large or particularly high-quality, unique habitat. We also examined whether the characteristics within the lower portion of the range make the species less susceptible to certain threats than other portions of the species' range, such that it could provide important population refugia in the event of extirpations elsewhere in the species' range. The Lower Apalachicola and Lower Chipola do not constitute a large geographic area (less than 20 percent of range) nor do they contain habitat of high quality relative to the rest of the range. This portion also does not constitute habitat or resources unique to that area for the species, as similar habitat is found throughout the range. For these reasons, we do not find this portion to be significant. Therefore, the lower portion of the fat threeridge range does not represent a significant portion of the range, and we find that the species is not in danger of extinction now or likely to become so in the foreseeable future in any significant portion of its range. This does not conflict with the courts' holdings in *Desert Survivors v. Department of the Interior*, 321 F. Supp. 3d 1011, 1070–74 (N.D. Cal. 2018), and *Center for Biological Diversity v. Jewell*, 248 F. Supp. 3d 946, 959 (D. Ariz. 2017) because, in reaching this conclusion, we did not apply the aspects of the Final Policy on Interpretation of the Phrase "Significant Portion of Its Range" in the Endangered Species Act's Definitions of "Endangered Species" and "Threatened Species" (79 FR 37578; July 1, 2014), including the definition of "significant" that those court decisions held to be invalid.

Determination of Status—Fat Threeridge

Our review of the best scientific and commercial data available indicates that the fat threeridge does not meet the definition of an endangered species or a threatened species in accordance with sections 3(6) and 3(20) of the Act. In accordance with our regulations at 50 CFR 424.11(e)(2) currently in effect, the species has recovered to the point at which it no longer meets the definition of an endangered species or a threatened species. Therefore, we propose to remove the fat threeridge from the Federal List of Endangered and Threatened Wildlife.

Effects of This Rule

This proposed rule, if made final, would revise 50 CFR 17.11(h) by removing both the Chipola slabshell mussel (*Elliptio chipolaensis*) and the fat threeridge mussel (*Amblema neislerii*) from the Federal List of Endangered and Threatened Wildlife. The prohibitions and conservation measures provided by the Act, particularly through sections 7 and 9, would no longer apply to these species. Federal agencies would no longer be required to consult with the Service under section 7 of the Act in the event that activities they authorize, fund, or carry out may affect these species.

Critical habitat for Chipola slabshell and fat threeridge at 50 CFR 17.95(f) would be removed if this proposal is made final.

Post-Delisting Monitoring

Section 4(g)(1) of the Act requires us, in cooperation with the States, to implement a monitoring program for not less than 5 years for all species that have been recovered. Post-delisting monitoring (PDM) refers to activities undertaken to verify that a species delisted due to recovery remains secure from the risk of extinction after the protections of the Act no longer apply. The primary goal of PDM is to monitor the species to ensure that its status does not deteriorate, and if a decline is detected, to take measures to halt the decline so that proposing it as endangered or threatened is not again needed. If at any time during the monitoring period data indicate that protective status under the Act should be reinstated, we can initiate listing procedures, including, if appropriate, emergency listing.

We will coordinate with other Federal agencies, State resource agencies, interested scientific organizations, and others as appropriate to develop and implement effective PDM plans for the Chipola slabshell and fat threeridge. The PDM plans will build upon current research and effective management practices that have improved the status of each of the species since listing. Ensuring continued implementation of proven management strategies that have been developed to sustain each of the species will be a fundamental goal for the PDM plans. The PDM plans will identify measurable management thresholds and responses for detecting and reacting to significant changes in Chipola slabshell and fat threeridge numbers, distribution, and persistence. If declines are detected equaling or exceeding these thresholds, the Service, in combination with other PDM

participants, will investigate causes of these declines. The investigation will be to determine if the Chipola slabshell or fat threeridge warrants expanded monitoring, additional research, additional habitat protection, or resumption of Federal protection under the Act.

We appreciate any information on what should be included in post-delisting monitoring strategies for these species (see Information Requested, above).

Required Determinations

Clarity of the Rule

We are required by Executive Orders 12866 and 12988 and by the Presidential Memorandum of June 1, 1998, to write all rules in plain language. This means that each rule we publish must:

- (1) Be logically organized;
- (2) Use the active voice to address readers directly;
- (3) Use clear language rather than jargon;
- (4) Be divided into short sections and sentences; and
- (5) Use lists and tables wherever possible.

If you feel that we have not met these requirements, send us comments by one of the methods listed in **ADDRESSES**. To better help us revise the rule, your comments should be as specific as possible. For example, you should tell us the numbers of the sections or paragraphs that are unclearly written, which sections or sentences are too long, the sections where you feel lists or tables would be useful, etc.

Government-to-Government Relationship With Tribes

In accordance with the President's memorandum of April 29, 1994 (Government-to-Government Relations with Native American Tribal Governments; 59 FR 22951), Executive Order 13175 (Consultation and Coordination with Indian Tribal Governments), and the Department of the Interior's manual at 512 DM 2, we readily acknowledge our responsibility to communicate meaningfully with federally recognized Tribes on a government-to-government basis. In accordance with Secretarial Order 3206 of June 5, 1997 (American Indian Tribal Rights, Federal-Tribal Trust Responsibilities, and the Endangered Species Act), we readily acknowledge our responsibilities to work directly with Tribes in developing programs for healthy ecosystems, to acknowledge that Tribal lands are not subject to the same controls as Federal public lands, to remain sensitive to Indian culture, and to make information available to Tribes.

There are no Tribal lands associated with this proposed rule.

References Cited

A complete list of references cited in this rulemaking is available on the internet at <https://www.regulations.gov> and upon request from the Florida Ecological Services Office (see **FOR FURTHER INFORMATION CONTACT**).

Authors

The primary authors of this proposed rule are the staff members of the Fish and Wildlife Service's Species Assessment Team and the Florida Ecological Services Office.

List of Subjects in 50 CFR Part 17

Endangered and threatened species, Exports, Imports, Plants, Reporting and recordkeeping requirements, Transportation, Wildlife.

Proposed Regulation Promulgation

Accordingly, we propose to amend part 17, subchapter B of chapter I, title 50 of the Code of Federal Regulations, as set forth below:

PART 17—ENDANGERED AND THREATENED WILDLIFE AND PLANTS

■ 1. The authority citation for part 17 continues to read as follows:

Authority: 16 U.S.C. 1361–1407; 1531–1544; and 4201–4245, unless otherwise noted.

§ 17.11 [Amended]

■ 2. In § 17.11, amend paragraph (h) by removing the entries for “Slabshell, Chipola” and “Threeeridge, fat” under CLAMS from the List of Endangered and Threatened Wildlife.

■ 3. In § 17.95, in paragraph (f), amend the entry for “Seven mussel species (in four northeast Gulf of Mexico drainages): Purple bankclimber (*Elliptoideus sloatianus*), Gulf moccasinshell (*Medionidus penicillatus*), Ochlockonee moccasinshell (*Medionidus simpsonianus*), oval pigtoe (*Pleurobema pyriforme*), shinyrayed pocketbook (*Hamiota subangulata*), Chipola slabshell (*Elliptio chipolaensis*), and fat threeeridge (*Amblema neislerii*)” by revising the entry's heading, the introductory text of paragraph (2), paragraph (5), the table in paragraph (6), the introductory text of paragraph (8), paragraph (8)(ii), the introductory text of paragraph (13), paragraph (13)(ii), the introductory text of paragraph (14), and paragraph (14)(ii) to read as follows:

§ 17.95 Critical habitat—fish and wildlife.

(f) *Clams and Snails*.

Five mussel species (in four northeast Gulf of Mexico drainages): Purple bankclimber (*Elliptoideus sloatianus*), Gulf moccasinshell (*Medionidus penicillatus*), Ochlockonee moccasinshell (*Medionidus simpsonianus*), oval pigtoe (*Pleurobema pyriforme*), and shinyrayed pocketbook (*Hamiota subangulata*)

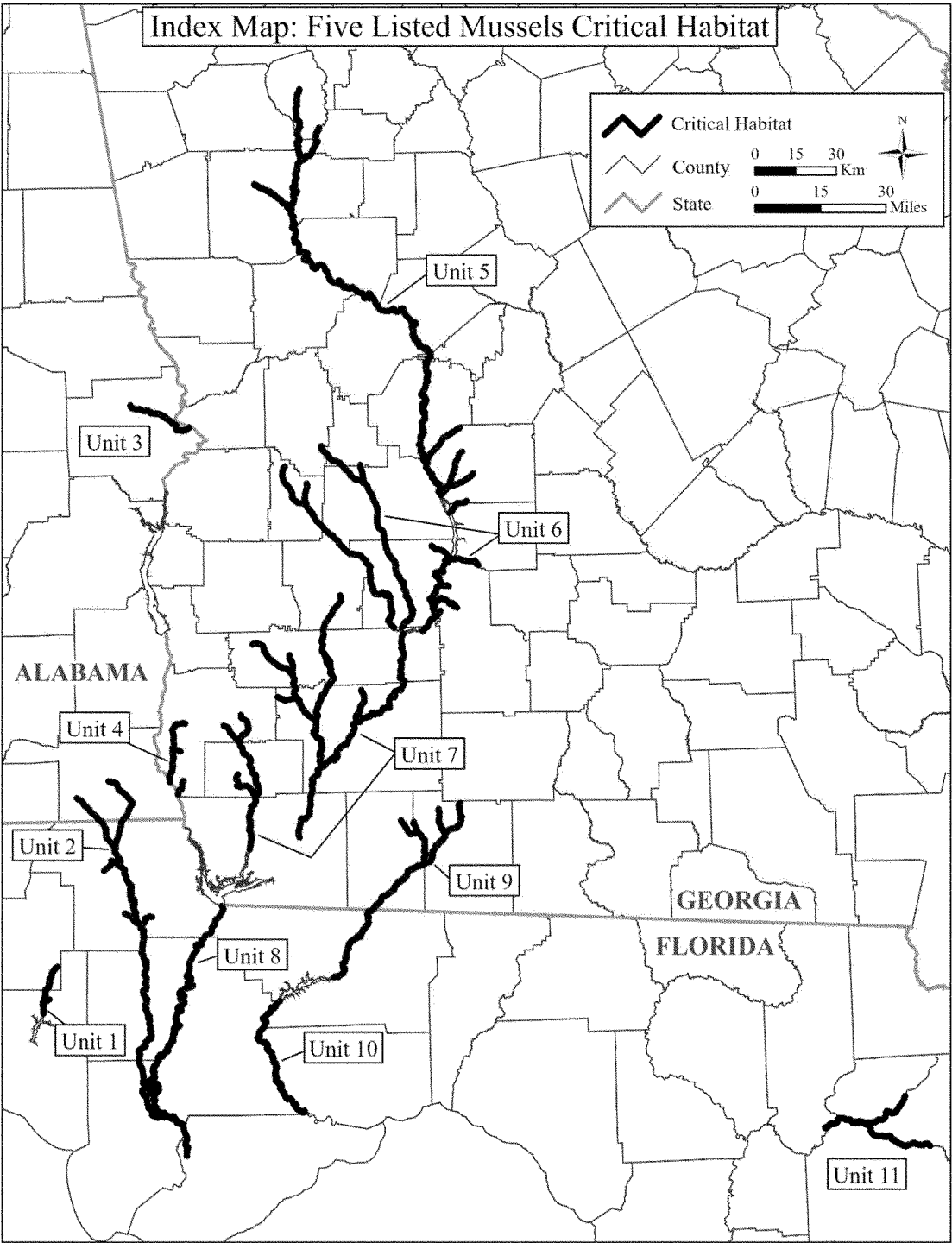
* * * * *

(2) The primary constituent elements of critical habitat for the purple bankclimber (*Elliptoideus sloatianus*), Gulf moccasinshell (*Medionidus penicillatus*), Ochlockonee moccasinshell (*Medionidus simpsonianus*), oval pigtoe (*Pleurobema pyriforme*), and shinyrayed pocketbook (*Hamiota subangulata*), are:

* * * * *

(5) Index map of critical habitat units in the States of Alabama, Florida, and Georgia for the five mussels follows:

Figure 1 to Five mussel species (in four northeast Gulf of Mexico drainages): Purple bankclimber (*Elliptoideus sloatianus*), Gulf moccasinshell (*Medionidus penicillatus*), Ochlockonee moccasinshell (*Medionidus simpsonianus*), oval pigtoe (*Pleurobema pyriforme*), and shinyrayed pocketbook (*Hamiota subangulata*) Paragraph (5)



(6) * * *

Table 1 to Five mussel species (in four northeast Gulf of Mexico drainages):	<i>sloatianus</i>), Gulf moccasinshell (<i>Medionidus penicillatus</i>), Ochlockonee moccasinshell (<i>Medionidus simpsonianus</i>), oval	pigtoe (<i>Pleurobema pyriforme</i>), and shinyrayed pocketbook (<i>Hamiota subangulata</i>) Paragraph (6)
Purple bankclimber (<i>Elliptoideus</i>		
Species	Critical habitat units	States
Purple bankclimber (<i>Elliptoideus sloatianus</i>)	Units 5, 6, 7, 8, 9, 10	AL, FL, GA.
Gulf moccasinshell (<i>Medionidus penicillatus</i>)	Units 1, 2, 4, 5, 6, 7	AL, FL, GA.
Ochlockonee moccasinshell (<i>Medionidus simpsonianus</i>)	Unit 9	FL, GA.
Oval pigtoe (<i>Pleurobema pyriforme</i>)	Units 1, 2, 4, 5, 6, 7, 9, 11	AL, FL, GA.
Shinyrayed pocketbook (<i>Hamiota subangulata</i>)	Units 2, 3, 4, 5, 6, 7, 9	AL, FL, GA.

* * * * *

(8) Unit 2. Chipola River and Dry, Rocky, Waddells Mill, Baker, Marshall, Big, and Cowarts Creeks in Houston County, Alabama, and in Calhoun, Gulf, and Jackson Counties, Florida. This is a critical habitat unit for the shinyrayed

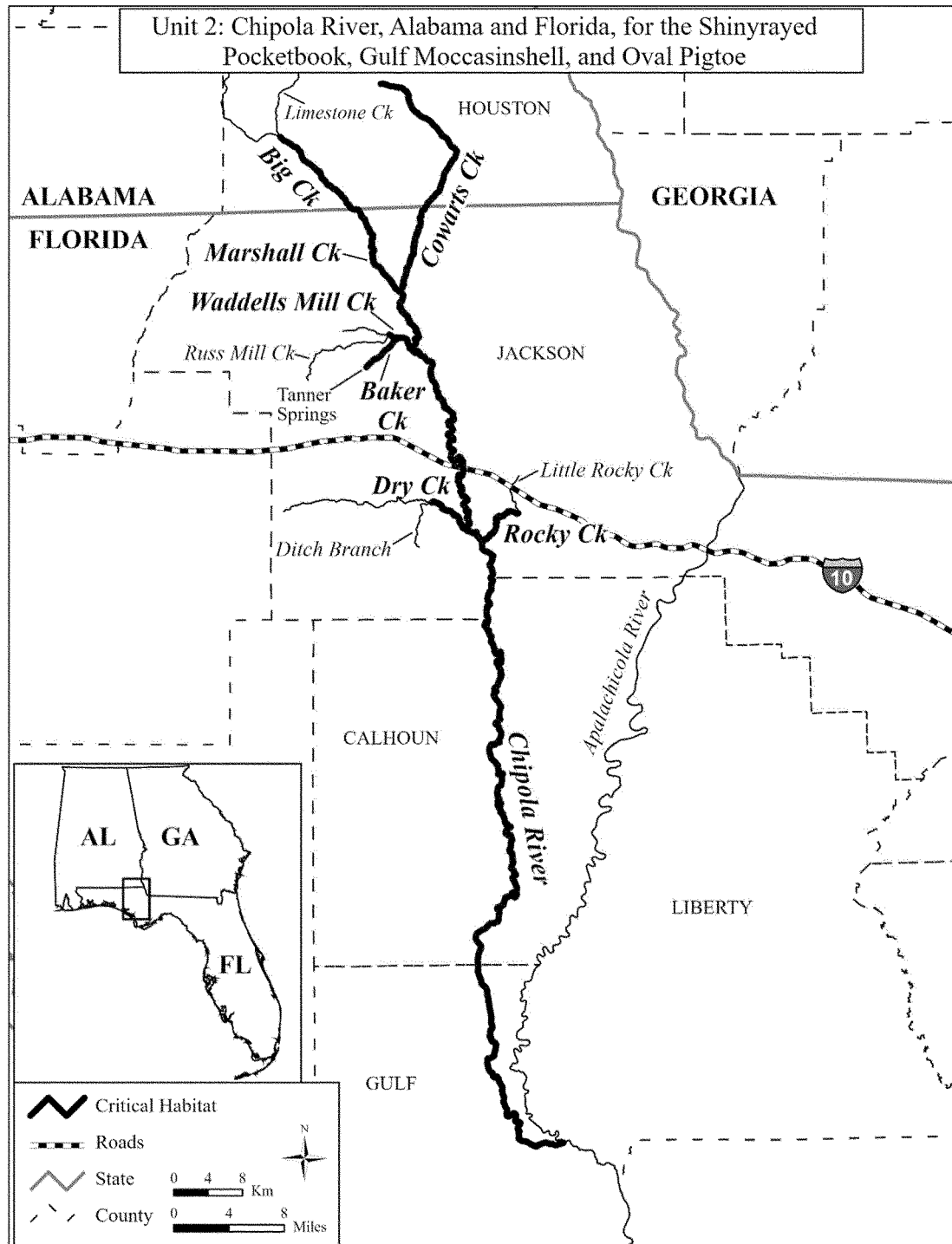
pocketbook, Gulf moccasinshell, and oval pigtoe.

* * * * *

(ii) Unit 2 map follows:

Figure 3 to Five mussel species (in four northeast Gulf of Mexico drainages): Purple bankclimber (*Elliptioideus*

sloatianus), Gulf moccasinshell (*Medionidus penicillatus*), Ochlockonee moccasinshell (*Medionidus simpsonianus*), oval pigtoe (*Pleurobema pyriforme*), and shinyrayed pocketbook (*Hamiota subangulata*) Paragraph (8)(ii)



* * * * *

(13) Unit 7. Lower Flint River and Spring, Aycocks, Dry,

Ichawaynochaway, Mill, Pachitla, Little Pachitla, Chickasawhatchee, and Cooleewahee creeks in Baker, Calhoun,

Decatur, Dougherty, Early, Miller, Mitchell, and Terrell Counties, Georgia. This is a critical habitat unit for the

shinyrayed pocketbook, Gulf moccasinshell, oval pigtoe, and purple bankclimber.

* * * * *

(ii) Two maps of Unit 7—western part of unit 7 and eastern part of unit 7—follow:

Figure 10 to Five mussel species (in four northeast Gulf of Mexico drainages): Purple bankclimber (*Elliptoideus sloatianus*), Gulf moccasinshell (*Medionidus penicillatus*), Ochlockonee moccasinshell (*Medionidus simpsonianus*), oval

pigtoe (*Pleurobema pyriforme*), and shinyrayed pocketbook (*Hamiota subangulata*) Paragraph (13)(ii)

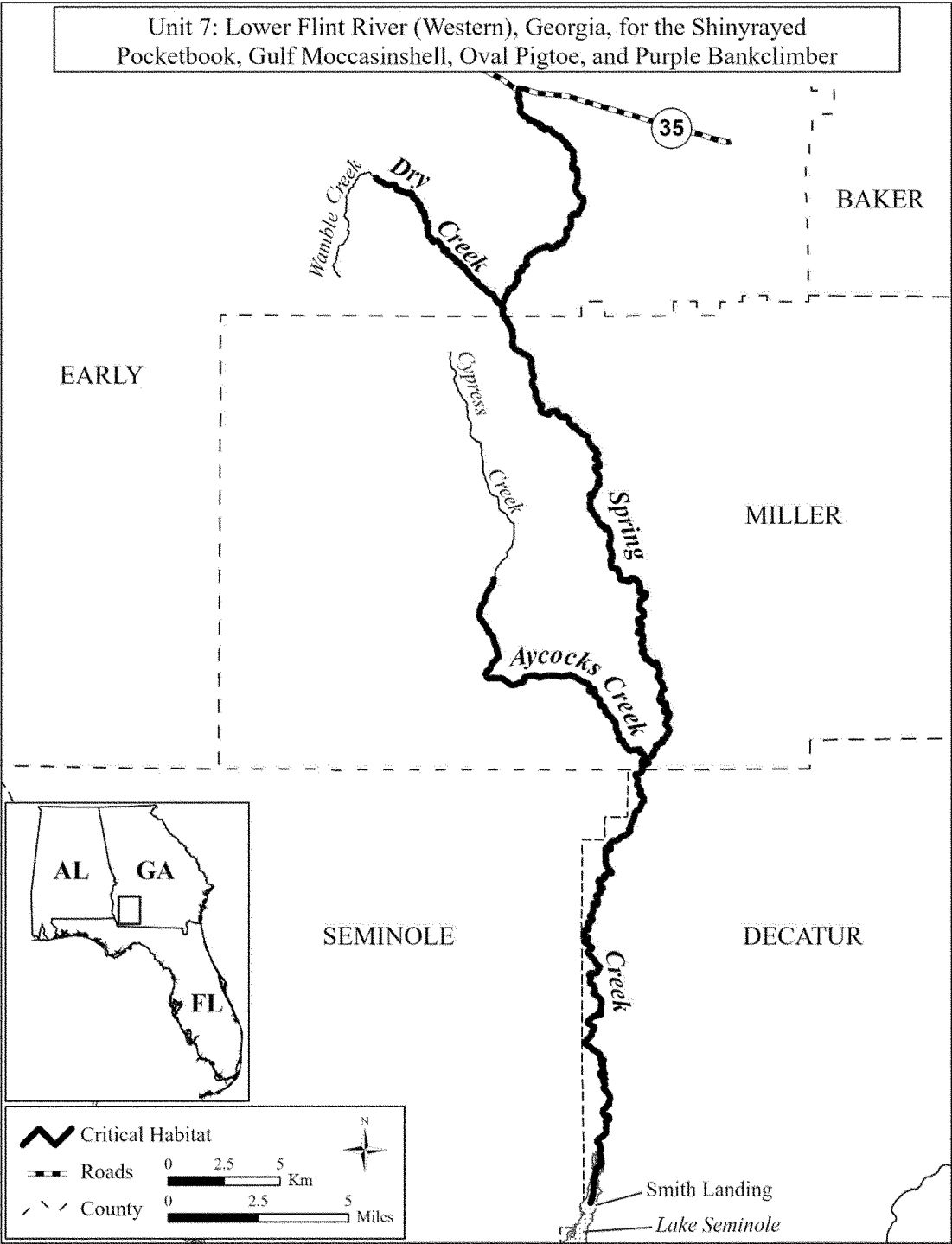


Figure 11 to Five mussel species (in four northeast Gulf of Mexico drainages): Purple bankclimber (*Elliptoideus*

sloatianus), Gulf moccasinshell (*Medionidus penicillatus*), Ochlockonee moccasinshell

(*Medionidus simpsonianus*), oval pigtoe (*Pleurobema pyriforme*), and

shinyrayed pocketbook (*Hamiota subangulata*) Paragraph (13)(ii)



(14) Unit 8. Apalachicola River, Chipola Cutoff, Swift Slough, River Styx, Kennedy Slough, and Kennedy Creek in Calhoun, Franklin, Gadsden, Gulf, Jackson, and Liberty Counties,

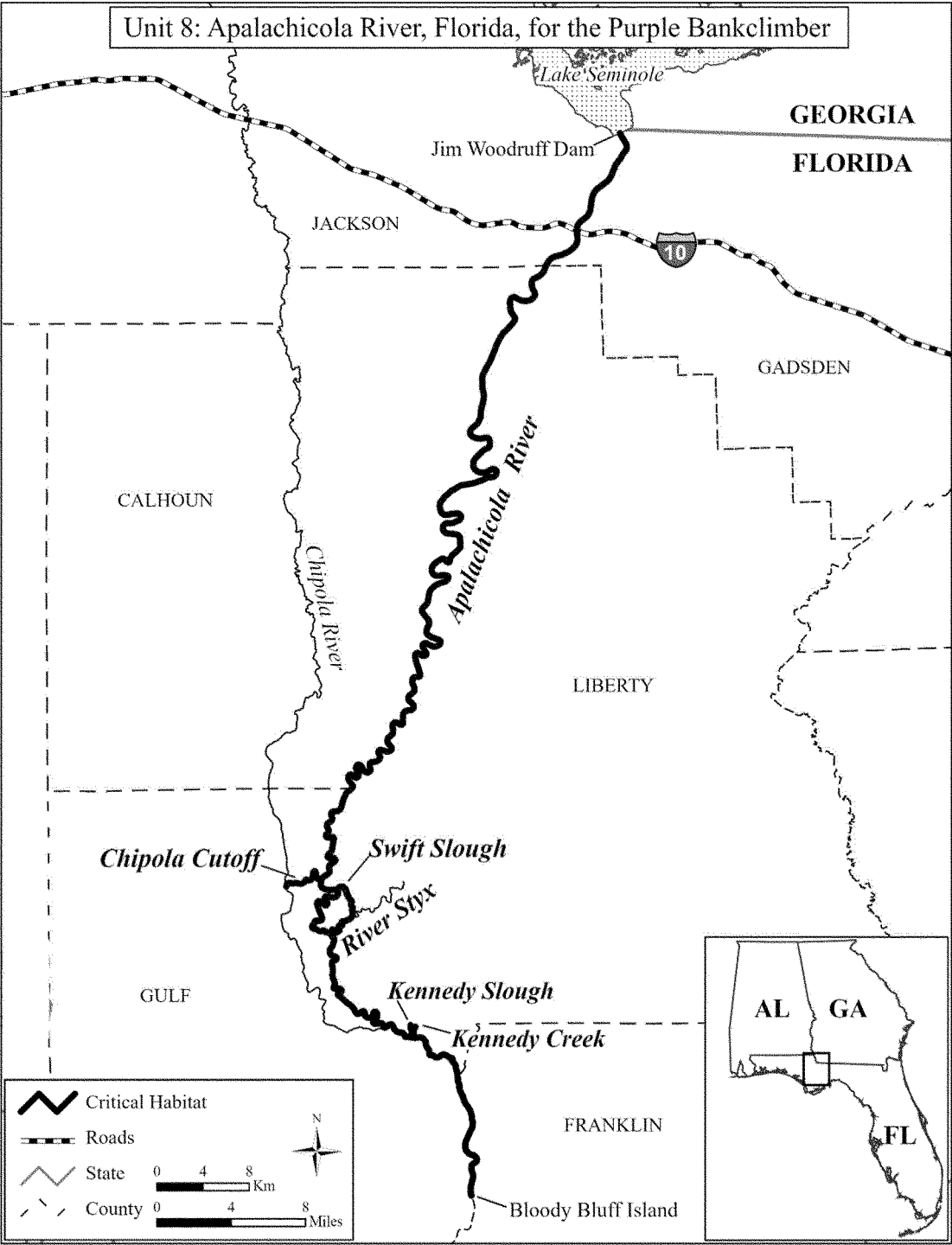
Florida. This is a critical habitat unit for the purple bankclimber.

* * * * *

(ii) Unit 8 map follows:

Figure 12 to Five mussel species (in four northeast Gulf of Mexico drainages): Purple bankclimber (*Elliptioideus*

sloatianus), Gulf moccasinshell (*Medionidus penicillatus*), Ochlockonee moccasinshell (*Medionidus simpsonianus*), oval pigtoe (*Pleurobema pyriforme*), and shinyrayed pocketbook (*Hamiota subangulata*) Paragraph (14)(ii)



* * * * *

Martha Williams,
Director, U.S. Fish and Wildlife Service.
[FR Doc. 2024-23929 Filed 10-28-24; 8:45 am]
BILLING CODE 4333-15-P

Notices

Federal Register

Vol. 89, No. 209

Tuesday, October 29, 2024

This section of the FEDERAL REGISTER contains documents other than rules or proposed rules that are applicable to the public. Notices of hearings and investigations, committee meetings, agency decisions and rulings, delegations of authority, filing of petitions and applications and agency statements of organization and functions are examples of documents appearing in this section.

DEPARTMENT OF AGRICULTURE

Animal and Plant Health Inspection Service

[Docket No. APHIS–2019–0013]

Importation of Fresh Soursop Fruit (*Annona muricata*) From Mexico Into the Continental United States

AGENCY: Animal and Plant Health Inspection Service, USDA.

ACTION: Notice.

SUMMARY: We are advising the public of our decision to authorize the importation of fresh soursop fruit (*Annona muricata*), also known as guanabana, from Mexico into the continental United States. Based on findings of a pest risk analysis, which we made available to the public for review and comment through a previous notice, we have determined that the application of one or more designated phytosanitary measures will be sufficient to mitigate the risks of introducing or disseminating plant pests or noxious weeds via the importation of fresh soursop fruit from Mexico.

DATES: Imports may be authorized beginning October 29, 2024.

FOR FURTHER INFORMATION CONTACT: Mr. Marc Phillips, Senior Regulatory Policy Specialist, PPQ, APHIS, USDA, 4700 River Road, Unit 133, Riverdale, MD 20737; (301) 851–2114; marc.phillips@usda.gov.

SUPPLEMENTARY INFORMATION:

Background

Under the regulations in “Subpart L—Fruits and Vegetables” (7 CFR 319.56–1 through 319.56–12, referred to below as the regulations), the Animal and Plant Health Inspection Service (APHIS) prohibits or restricts the importation of fruits and vegetables into the United States from certain parts of the world to prevent plant pests from being

introduced into or disseminated within the United States.

Section 319.56–4 contains a performance-based process for approving the importation of commodities that, based on the findings of a pest risk analysis (PRA), can be safely imported subject to one or more of the designated phytosanitary measures listed in paragraph (b) of that section. Under that process, APHIS proposes to authorize the importation of a fruit or vegetable into the United States if, based on findings of a PRA, we determine that the measures can mitigate the plant pest risk associated with the importation of that fruit or vegetable. APHIS then publishes a notice in the **Federal Register** announcing the availability of the PRA that evaluates the risks associated with the importation of a particular fruit or vegetable. Following the close of the 60-day comment period, APHIS will issue a subsequent **Federal Register** notice announcing whether or not we will authorize the importation of the fruit or vegetable subject to the phytosanitary measures specified in the notice.

In accordance with that process, we published a notice ¹ in the **Federal Register** on May 2, 2019 (84 FR 18764–18765, Docket No. APHIS–2019–0013), in which we announced the availability, for review and comment, of a PRA that evaluated the risks associated with the importation of fresh soursop ² (*Annona muricata*) fruit from Mexico into the continental United States. The PRA consisted of a pest list identifying pests of quarantine significance that could follow the pathway of the importation of fresh soursop fruit into the continental United States from Mexico and a risk management document (RMD) identifying phytosanitary measures to be applied to that commodity to mitigate the pest risk.

We solicited comments on the notice for 60 days, ending on July 1, 2019. Based on a public request to extend the comment period, APHIS did so, and the extended comment period closed on August 2, 2019. We received 28 comments by the close of the comment period. They were from the national

plant protection organization (NPPO) of Mexico, an industry group representing Mexican fruit packers, State departments of agriculture within the United States, a county government, a committee representing domestic avocado producers, a trade association representing domestic citrus producers, an agricultural extension agent, domestic soursop producers, and private citizens.

We have categorized the comments according to topic areas, summarizing and responding to each comment below.

General Comments

One commenter stated that Mexico’s NPPO and authorities lack the expertise necessary to implement the systems approach, particularly phytosanitary inspections.

We consider the NPPO of Mexico to have sufficient training to conduct phytosanitary inspections, which are required for the importation of many commodities from Mexico, and which are conducted routinely.

Several commenters stated that Mexico lacked sufficient personnel to conduct phytosanitary inspections.

APHIS will require that a phytosanitary inspection is conducted by the NPPO of Mexico and a phytosanitary certificate is issued in order for the shipment of soursop to be allowed to enter the United States for irradiation treatment; shipments that lack this phytosanitary certificate will be refused entry. However, we have no reason to believe that Mexico lacks sufficient personnel to perform this task. As noted above, phytosanitary inspections are performed routinely within Mexico, and the NPPO of Mexico has not expressed concerns about insufficient resources to perform them.

Several commenters stated that the NPPO lacked the integrity and incentives for adequate phytosanitary inspection; they alleged a history of lying and cheating within the NPPO.

Mexico is a signatory to the World Trade Organization’s Sanitary and Phytosanitary Agreement. As such, it has agreed to respect the phytosanitary measures the United States imposes on the importation of plants and plant products from Mexico when the United States demonstrates the need to impose these measures in order to protect plant health within the United States. The pest list that accompanied the initial

¹ To view the notice, the supporting documents, and the comments received, go to www.regulations.gov. Enter APHIS–2019–0013 in the Search field.

² Soursop is also commonly referred to as guanabana.

notice provided evidence of such a need.

With that being said, all shipments of soursop are subject to inspection at ports of entry, and an inspector will monitor all irradiation treatments of soursop from Mexico and may inspect articles prior to irradiation for quarantine pests.

Four comments cited concerns that market access to the United States of fresh produce from Mexico provides a vehicle for illegally transporting drugs, money, and/or people.

The commenters provided no evidence to substantiate these concerns. However, as noted above, all shipments of soursop are subject to inspection at ports of entry.

Several commenters expressed concern that APHIS did not describe the Mexican chemical control measures in its assessment of market access for soursop. One of the commenters asked whether APHIS has determined that the chemicals Mexican producers may use on soursop are harmonized with those that U.S. producers may use, while another asked who will monitor to ensure that only chemicals approved for use in the United States are applied. One of the commenters asked how APHIS will ensure that chemicals that are harmful to human health are not used.

The United States does not have direct control over pesticides that are used on food commodities such as soursop in other countries, and it will fall to the NPPO of Mexico to monitor which chemicals are used at registered places of production.

However, there are regulations in the United States concerning the importation of food to ensure that commodities do not enter the United States containing illegal pesticide residues. Through section 408 of the Federal Food, Drug, and Cosmetic Act, the Environmental Protection Agency (EPA) has the authority to establish, change, or cancel tolerances for food commodities. These EPA-set tolerances are the maximum levels of pesticide residues that have been determined, through comprehensive safety evaluations, to be safe for human consumption. Tolerances apply to both food commodities that are grown in the United States and food commodities that are grown in other countries and imported into the United States. The EPA tolerance levels are enforced once the commodity enters the United States. Chemicals such as DDT that are banned in the United States do not have tolerances on food commodities. Federal Government food inspectors are responsible for monitoring food

commodities that enter the United States to confirm that tolerance levels are not exceeded and that residues of pesticide chemicals that are banned in the United States are not present on the commodities.

Several commenters stated that, since the notice was issued, Mexico had experienced a significant and widespread outbreak of Mediterranean fruit fly (*Ceratitis capitata*, Medfly) in the State of Colima, indicating a breakdown of trapping and control measures at production sites. One other commenter stated that fruit fly outbreaks in the area of Mexico bordering Texas had become more frequent.

Mexico worked with the United Nations Food and Agriculture Organization (FAO) and the International Atomic Energy Agency's (IAEA's) technical cooperation program and more than 200 technicians to employ sterile insect techniques (SIT) after a Medfly detection in Colima. Mexican authorities, who imposed a quarantine on the region during eradication efforts, declared the Medfly completely eradicated. APHIS determined that no fruit fly host material was exported to the United States from the incident.

Sterile male medflies in the SIT initiative were produced at a facility in Mexico, with a design that benefited from IAEA expertise, inaugurated in 2021. It is the second largest in the world with a production capacity of 1,000 million sterile medflies every week. The new facility, located in the state of Chiapas, focuses on mass production of sterile insects. Together with the El Pino facility in Guatemala, it helps maintain the containment barrier that prevents the introduction and spread of the pest to northern Guatemala, Mexico, and the United States.

Several commenters stated that irradiation, the primary mitigation, is not failsafe in the event of high infestation levels. Several other commenters echoed this last point and stated that other measures should be included in the systems approach to ensure that irradiation is effective at neutralizing quarantine pests. One commenter, the NPPO of Mexico, stated that in order to be eligible to export, soursop producers in Mexico must be registered with the NPPO, and that such registration is associated with integrated pest management at the place of production, including monitoring for and control of fruit flies.

We agree with the commenters who stated that fruit fly trapping at places of production is warranted in order to

reduce pest pressures and help ensure that the soursop fruit to be irradiated is not infested with fruit flies. We have added a requirement for pest management for fruit flies and other pests to the final RMD. We will also require places of production to be registered with the NPPO of Mexico so that the NPPO may monitor the placement and servicing of traps; as noted by the NPPO of Mexico, this is currently a requirement for all soursop producers in Mexico who wish to be eligible to export soursop.

Several commenters stated that they believe that the introduction of quarantine pests from the importation of soursop from Mexico is likely because the climate in Florida and, especially, south Florida is especially suitable to the establishment and spread of quarantine pests.

We have determined, for the reasons described in this final notice as well as the RMD that accompanies this final notice, that the measures specified in the RMD will effectively mitigate the risk associated with the importation of soursop from Mexico.

One commenter asked that APHIS employ additional databases in Spanish and English to assess pest introduction risk.

APHIS notes that sources in both Spanish and English were consulted in preparing the quarantine pest list for the soursop market access request.

To facilitate comments from Spanish-speaking members of the public without internet access, two commenters requested that APHIS provide: Spanish translations of APHIS' website, pest risk assessments, and economic documents, as well as a means of submitting an official comment that did not rely on internet access, email access, or access to an online portal. The commenters also asked that comments received in Spanish be translated and taken into consideration.

APHIS affirms the U.S. Department of Agriculture's (USDA's) overarching commitment to environmental justice as regards its actions and activities, and, to the extent practicable, we do make our outreach materials available in languages other than English when we are aware of stakeholder groups who are not native English speakers and who are particularly impacted by or interested in our actions. We also note that there are a variety of free internet tools available that will translate documents and web pages from one language to another, often without charge. However, given the more than 7,000 languages currently in existence, it is not logistically feasible nor equitable to expect the Agency to

translate all of its documents into any one language.

Regarding submission of comments, consistent with the requirements of the eGovernment Act of 2022, APHIS allows comments on all of its **Federal Register** documents to be submitted through postal mail and considers such comments to be official comments, regardless of the language of the submission. APHIS already endeavors and will continue to try to translate comments received in languages other than English in its consideration of comments. However, in order to ensure the best or most accurate characterization and response to comments, APHIS suggests that all submissions be made in English.

Pest List Comments

As we mentioned previously in this document, the initial notice made available a pest list that identified pests of quarantine significance that could follow the pathway of the importation of fresh soursop fruit into the continental United States from Mexico. These were *Optatus palmaris* Pascoe, the Annonaceae fruits weevil, *Neosilba glaberrima*, a lance fly, *Anastrepha fraterculus* (Wiedemann), the South American fruit fly, *Anastrepha striata* Schiner, the guava fruit fly, *Ceratitidis capitata*, Mediterranean fruit fly or Medfly, *Nipaecoccus viridis*, the spherical mealybug, *Bephratelloides pomorum* (Fabricius), the soursop wasp, *Oenomaus ortygnus*, the aquamarine hairstreak butterfly, *Cerconota anonella*, the Annona fruit borer, and *Talponia batesi* Heinrich, a moth. No introduction of a new quarantine pest has occurred in Mexico that would infest soursop fruit since APHIS' analysis was completed.

One commenter faulted the pest list for not including *Frankliniella diffilis* among pests it evaluated for the importation, noting that the insect is impervious to irradiation and has been reported as a persistent pest of mamey sapote and avocado in Morelos, Mexico.

While *Frankliniella diffilis* is present in Mexico and while it is a quarantine pest for the continental United States, APHIS has found no evidence to suggest that it is a pest of soursop. For these reasons, APHIS did not include it in the pest list.

Another commenter stated that the pest list did not include five pests of soursop that pose risks to California's agriculture and environment, *Aleurodicus dispersus*, *Paracoccus marginatus*, *Pseudococcus jackbeardsleyi*, *Russellaspis pustulans*, and *Bephratelloides cubensis*. APHIS regards all five of these pests as

nonactionable, meaning that they are none of the following: (1) Quarantine pests that are not present in the United States; (2) regulated non-quarantine pests that are not present in the United States; (3) pests that are in the United States in limited distribution and under official control or are candidates for official control; or (4) pests that require evaluation for regulatory action. Because they are non-actionable, they were not included in the pest list.

A commenter also stated that numerous fruit flies attack soursop, specifically citing *Neosilba glaberrima*, *N. pendula*, *Anastrepha fraterculus*, *A. ludens*, *A. obliqua*, *A. striata*, and *Ceratitidis capitata*.

As noted above, *Neosilba glaberrima*, *Anastrepha fraterculus*, *A. striata*, and *Ceratitidis capitata* were included in the pest list as quarantine pests that could follow the pathway of the importation of soursop from Mexico and thus require mitigation. This mitigation is first and foremost the irradiation treatment required under the systems approach. *Neosilba pendula*, *Anastrepha ludens*, and *A. obliqua* are listed in Section 1.1 of the pest list as quarantine pests. However, the section indicates that there is inadequate evidence for a host association of these pests with soursop. Hence, we did not develop mitigations specific to these pests. Nonetheless, it should be noted that all fruit fly species are sterilized at 150 Gy, and the dose required for this importation will be 400 Gy.

The same commenter expressed concern that *Optatus palmaris*, the Annonaceae fruits weevil, is a significant pest of soursop.

We included *Optatus palmaris* in the pest list as a quarantine pest that could follow the pathway of the importation of soursop from Mexico and thus requires mitigation.

The same commenter specifically requested inclusion of Lance fly (*Neosilba batesi*); also, the fungal diseases black canker (*Phomopsis* spp.), purple blotch (*Phytophthora palmivora*), brown rot (*Rhizopus stolonifera*), burning string (*Corticium koleroga*), and zoned spot (*Sclerotium coffeicolum*), citing references specific to soursop in Mexico in support of this request.

Neosilba batesi (Curran) is present in Florida and not under official control, and it is therefore non-actionable and not a quarantine pest for the continental United States. Hence, it was not included in the pest list.

With regard to the fungi referenced by the commenter, these fungi have been reported on other Annona species such as *A. cherimola*, but APHIS found no

evidence of them on *A. muricata*. These fungi are also ubiquitous in the United States, and they are thus both non-actionable and not quarantine pests.

Another commenter asked APHIS to define the basis for its assertion that *Parlatoria cinerea* Hadden, armored scale, is not an actionable pest as regards soursop importation. The commenter asserted that the pest does occur on fruit and that no economic analysis has been made of its potential cost to U.S. producers if it is introduced here.

APHIS acknowledges that *Parlatoria cinerea* Hadden is present in Mexico, and it has been reported as a pest of *Annona muricata*. Although it is a quarantine pest for the continental United States, APHIS has determined that fruit for consumption is an unlikely pathway for the introduction of diaspidid scales, such as *Parlatoria cinerea*, due to their very limited ability to disperse to new host plants. Hence, it is not an actionable pest at U.S. ports of entry.

A commenter expressed concern that APHIS had not assessed the economic effect of non-actionable insects, such as several scales or mealy bugs that are in the United States but not present in Florida or south Florida. The commenter stated that detection probabilities prior to shipment have not been determined, also that inspection of all fruit loads upon arrival in a locale are impossible. The commenter stated that, in light of this, there is a possibility of introduction of non-actionable pests, and that non-actionable pests have impacts on farmers.

As noted in a previous response, a pest must be considered actionable if it is a pest of quarantine significance that is not present in the United States or if it is a pest of quarantine significance that is in the United States in limited distribution and under official control or is a candidate for official control. Therefore, non-actionable pests do not meet either our or the International Plant Protection Convention's definition of a quarantine pest, and we do not consider specific mitigation measures necessary for them.

However, APHIS has developed a program, the Federally Recognized State Managed Phytosanitary Program (FRSMP), to afford protections to States when commodities are determined at a port of entry to harbor a plant pest that is not a quarantine pest but is of concern to a particular State. Information regarding the petition process for FRSMP is found here: https://www.aphis.usda.gov/plant_health/plant_pest_info/frsmp/downloads/petition_guidelines.pdf.

Comments on the RMD

In the RMD, we proposed that soursop from Mexico would have to be commercially produced and part of a commercial consignment. We further indicated that, in order to be considered commercially produced, culling of fruit prior to shipment would need to occur.

One commenter questioned culling process effectiveness for *Opatus palmaris*, four fruit fly species, and three lepidoptera species. The commenter stated that, at various stages of the pests' development, these pests are internal feeders and may not cause visible damage that would result in culling.

The purpose of the irradiation treatment described in the RMD is to mitigate the risk of internally feeding pests, other than lepidoptera, that are not detected during a visual inspection. Moreover, APHIS disagrees with the commenter that these pests may not cause visible damage; damage from these internal feeders is visible and often conspicuous and would lead to culling of the fruit by the time it reaches a packinghouse.

We proposed that the soursop would have to be irradiated with a minimum absorbed dose of 400 Gy and follow the requirements of 7 CFR part 305 with treatments approved as effective at neutralizing quarantine pests.

One commenter stated that soursop should be allowed to be irradiated in the continental United States, citing a bilateral agreement with Mexico. The commenter interpreted the RMD to limit irradiation treatment to prior to the fruit's arrival at a port of entry into the United States.

The RMD stated that fruit must be irradiated with a minimum absorbed dose of 400 Gy and follow the requirements of part 305. That part contains APHIS' regulations governing phytosanitary treatments. Section 305.9 contains APHIS' irradiation treatment regulations. The commenter appears to be referring to one of the requirements for irradiation of imported commodities within the United States, which is for the NPPO of a country from which articles are to be imported into the United States to sign a framework equivalency workplan with APHIS.

The commenter is correct that the NPPO of Mexico has signed such a workplan and met other preconditions for domestic irradiation of part 305. The RMD therefore allows irradiation of soursop at approved facilities within the United States.

Several commenters challenged the efficacy of APHIS' irradiation dosage, stating that it may not kill the moth

lepidoptera pupae and larvae inside the soursop fruit. They stated that this is acknowledged in the USDA treatment manual. The commenters also noted that several lepidopteran species, including *Cerconota anonella*, infest soursop in Mexico.

While it is true that irradiation at a minimum absorbed dose of 400 Gy may not neutralize lepidoptera, irradiation was not intended within the RMD as a specific mitigation for lepidoptera. As noted in the RMD, the lepidoptera of quarantine significance listed in the pest list, while internal feeders, cause visible damage to the fruit that renders it unmarketable and would result in it being culled. Thus, it is expected that the visual inspection required in culling would detect the pupal and larval stages of the three lepidoptera pests in soursop.

One commenter noted a discrepancy between this provision of the RMD and the economic effects abstract, or economic effects assessment (EEA), that accompanied the initial notice. In the EEA, we indicated that "most shipments" will be irradiated, which the commenter pointed out could be as little as 51 percent of total shipments. The commenter also asserted that the EEA did not provide any context about which shipments would be subject to irradiation and which would not, or who would adjudicate whether irradiation should be administered to the shipment.

The initial EEA did not clearly state, but the initial RMD, our final RMD, and this notice all affirm, that all shipments will have to be irradiated.

One commenter questioned Mexico's ability to administer irradiation treatment and stated that this should be verified through test protocols before we allow it to occur for soursop intended for export to the United States. In contrast, the NPPO of Mexico pointed out that they have irradiation facilities that have been approved by APHIS and have used these facilities to irradiate commodities in accordance with part 305 for more than a decade. Two other commenters stated that approval of the facilities occurred in November 2008, and that pests have not been identified on irradiated commodities following treatment. These latter commenters cited this as evidence that the irradiation program in Mexico is well established.

For the reasons cited by the NPPO of Mexico and the latter commenters, we do not consider it necessary to conduct test protocols of irradiation treatment in Mexico. However, we must here underscore that § 305.9 (a) through (o) lays out in detail the provisions

required for irradiation treatment of any imported regulated articles (*i.e.*, fruits, vegetables, cut flowers, and foliage), as well as such regulated articles moved interstate from Hawaii and U.S. territories. Protocols and conditions for irradiation facilities and their certification; compliance, monitoring, and interagency agreements; treatment framework equivalency workplans; related packaging, container, dosage, records, inspection; and other requirements are all specified therein.

We proposed that soursop from Mexico imported into the United States would be subject to inspection at ports of arrival into the United States.

Several commenters stated that port-of-entry inspections were insufficient in frequency and sampling size to detect quarantine pests, particularly fruit fly larvae, that may be present in soursop from Mexico.

The RMD prescribes a systems approach for the mitigation of plant pests of soursop imported from Mexico into the United States. As noted previously, port-of-entry inspections are just one type of inspection of soursop within the systems approach and will be required for all shipments entering into the United States. Additionally, the NPPO of Mexico must inspect all shipments prior to issuing a phytosanitary certificate, and an inspector may inspect shipments prior to or after irradiation treatment. To that end, we reiterate that all shipments will have to be treated with irradiation treatment for fruit flies.

Several commenters indicated that port-of-entry inspection had failed to detect oriental fruit fly (OFF)-infestations in imported products, leading to a significant outbreak in Florida.

APHIS has no evidence that the OFF outbreak was due to insufficient port-of-entry inspections of imported fruit.

One commenter requested that specific eradication and research programs, as well as commitments of resources, be in place to mitigate potential pest introduction impact. Another commenter stated that treatment of soursop for pests upon entry to the United States, as well as within Mexico, should be allowed.

The comments presume a likelihood that APHIS' prescribed systems approach will fail to mitigate pest introduction to the United States. APHIS would not entertain the market access for soursop if it lacked confidence that a systems approach would prevent quarantine pests from following the pathway of importation into the United States. APHIS does not find that the comments provided

evidence that contravenes the efficacy of the systems approach or supports denial of the market access to soursop.

Finally, a commenter asked APHIS to have laboratories test soursop fruit before it is taken for supply to the United States. Specifically, the commenter asked that the fruit be required to ripen and overripen in laboratories in Mexico before being allowed to be shipped to the United States, citing a protocol for durian from Mexico that the commenter asserted to be operational and effective as a precedent.

We are uncertain what protocol the commenter is referring to. The import requirements for durian from Mexico are that it must be accompanied by a permit issued by APHIS and is subject to inspection at ports of entry into the United States. Nonetheless, we do not consider such testing necessary for soursop from Mexico to be warranted. For the reasons set forth in the initial RMD, the revised RMD, and this notice, we consider the mitigations of the revised RMD to be sufficient to address the plant pest risk associated with the importation of soursop from Mexico.

Economic Comments

Three commenters noted that the EEA that accompanied the initial notice had stated that there was no domestic production of soursop in the United States. The commenters stated that there were in fact domestic producers, and that APHIS has not conducted analysis of imported soursop impact on domestic grower wellbeing. The commenters provided information from local surveys and grower contacts, as well as the status of soursop production in Florida.

APHIS has updated the EEA for the soursop market access based on information the public provided during the comment period.

Public comments APHIS received in 2019 suggested a presence of 11 acres of commercial soursop production area in Florida's Miami-Dade County, the only region in the continental United States that has a tropical climate suitable for soursop production. Among other findings of the revised EEA, Florida's soursop acreage is increasing within this limited production area in Miami-Dade County, in part because soursops are considered as a potential alternative cash crop to avocados, the production of which has been declining since the outbreak of Laurel Wilt disease in 2011. Assuming an average yield of 3.2 to 3.6 tons per acre, APHIS estimates that approximately 35 to 40 tons of soursop were produced in Florida in 2018.

The revised EEA, most recently updated in 2024, also examines the

growth of Mexico's soursop production, the relatively stable fresh soursop imports from Grenada to the United States (presently only Grenada is authorized to export fresh soursops to the United States), the total acreage available for all domestic tropical fruit tree production in southern Florida in 2018, and available economic census data for U.S. tropical fruit production and commerce to indicate potential production areas of soursops in Florida.

Several commenters stated that imports of soursop from Mexico will adversely impact the domestic market for soursop in Florida. Five commenters stated that domestic acreage is slowly growing, and the market is niche and sensitive to quantity and price fluctuations. These latter commenters stated that Mexico's projected shipment quantity will disproportionately cut soursop prices and pressure the U.S. domestic producers to compete with one another.

As noted above, APHIS has revised the EEA to take domestic production—as well as current import volume from Grenada, the only country currently authorized to ship fresh soursop to the United States—into consideration. However, the estimated domestic production is only 30 to 35 tons annually in southern Florida. In this regard, we note that this notice provides Mexico with market access to the entire continental United States, including major metropolitan areas where fresh soursop is currently not available. While it is possible soursop from Mexico will be imported for distribution to Florida, it is also possible that it will be imported for distribution to other areas of the continental United States. Additionally, given the currently limited scope of the market, allowing soursop importation may increase consumer awareness of soursop, spurring an increase in demand.

One of the commenters characterized APHIS' assessment as indifferent toward domestic soursop producers in that it views the market access as only harming small entities and merchants. Commenters also expressed concern that the import will have a negative impact on the domestic growers, whom the commenters stated are small, family-owned businesses, for a very modest and localized domestic demand for soursop, which, the commenters stated, domestic growers are presently meeting. They stated that even with time, education, and diversification, demand for soursop in the United States could not increase to levels justifying this imported volume. They stated that the domestic supply is seasonally met, and APHIS had not conducted an analysis of

the impacts of additional import volume on seasonal or counter-seasonal demand. Similarly, one commenter characterized domestic production as in an “incubator stage,” in which demand increases very slowly and influxes of product could significantly adversely impact the domestic market.

We cannot with certainty determine that consumers will favorably respond to fresh soursops with which they are not presently familiar. We have thus not been able to substantiate the commenters' concerns that domestic demand throughout the continental United States is localized, seasonal, or modest, particularly given that it is not currently available in most major metropolitan areas in the United States.

Two commenters stated that domestic grower costs are much greater than in Mexico for the same crops and that cheaply produced soursop imports in increased volume will be harmful to domestic growers. They believed that Mexico's big scale production at lower production costs will overwhelm domestic production.

A commodity's production costs abroad, broadly construed, do not necessarily equate to costs of production for that commodity when it is required to meet stringent standards for importation to the United States. In this regard, we note that the NPPO of Mexico indicated that their export program for soursop imposes additional requirements on producers that are not required of soursop producers that sell domestically within Mexico. We also note that the other standards of the RMD, particularly irradiation, will impose other logistics costs to retain freshness for soursops' short shelf-life, costs that domestic producers would not encounter.

Ten commenters stated that in assessing economic impact of the market access request from Mexico, APHIS cannot ignore possible pest eradication costs, nor effects past introductions of pests and diseases have had on U.S. growers. They cited unintentional pest and disease introductions at great, documented quarantine expense. Among impacts they noted, domestic commercial citrus packinghouses have been cut from 88 to 14. Five commenters in a related concern maintained that this importation is much more broadly economically significant because the listed quarantine-able pests pose potential risk to Florida's \$120 billion agricultural industry. These commenters feared a spill-over effect on large numbers of avocado growers and their \$100 million related industry, as they are exposed to the same pest and

disease risks as soursop growers in this importation.

We have determined, for the reasons described in this final notice, as well as the RMD that accompanies this final notice, that the measures specified in the RMD will effectively mitigate the risks associated with the importation of soursop from Mexico. Thus, we do not believe that the economic losses due to pest or disease introduction that the commenters feared will materialize, and therefore do not need to be analyzed.

One commenter stated that each time the Mediterranean fruit fly has been detected in Florida, fewer control methods have been available, as the pest has been increasingly resistant to aerial pesticide spraying. The commenter cited one recent eradication cost estimate ranging widely from \$24 to \$56 million.

APHIS acknowledges the severity of past fruit fly outbreaks in its revised EEA, but APHIS reiterates that the provisions of the revised RMD will address the plant pest risk associated with the importation of soursop from Mexico, for the reasons set forth in the initial RMD, the revised RMD, and this document. If we considered those mitigations insufficient, we would not approve such importation.

Another commenter asserted that meeting soursop demand with domestic production is safer and returns dollars to the local economy, rather than draining the local economy.

As indicated above, APHIS has no information indicating that domestic demand for fresh soursop throughout the continental United States is met by domestic production and distribution, which is currently limited and localized. Notwithstanding this, under the Plant Protection Act (7 U.S.C. 7701 *et seq.*), APHIS cannot base its determinations on economic cost competitiveness considerations or economic impacts.

Another commenter asked APHIS to conduct an income impact study of domestic grower prices in the event of soursop importation, especially if the importation is at volumes stated in the proposed market access.

APHIS does not have, nor did commenters provide, data that would allow us to complete such an analysis. However, such an analysis is not warranted. The commenter's stated assumption was that imports of soursop would directly compete with domestic production in areas of current domestic distribution. As noted above, we have no data suggesting this will occur, particularly given the scope of the market access and the absence of fresh

soursop in most major metropolitan areas.

As stated in the revised EEA, we evaluated whether it would have an impact high enough to trigger a Major designation under the Congressional Review Act and concluded that it would not. In this particular case, the entire domestic industry has a market value of far less than \$100 million. Thus, even a complete collapse in the domestic soursop price would not be sufficient to trigger such a designation. APHIS finds no evidence such a collapse will occur, and it is possible that soursop imports could expand access to other metropolitan areas (e.g., cities in Arizona, California, and Texas), leading to more market access rather than additional competition for domestic growers.

In addition to considering the total value of the market effects, the revised EEA also noted that many of the soursop producers are small entities. Precise income effects on these growers would be difficult for APHIS to determine exactly due to the absence of detailed data.

Mexico is a major producer of soursops. The production of soursops increased rapidly in Mexico up to 2021, when Mexican producers grew 39,905 tons of soursops on 10,012 planted acres. That reflected a 380 percent increase in production and a 260 percent increase in planted acreage from 2000, when 8,321 tons of soursops were produced on 2,792 planted acres. In 2023, this moderated as Mexican producers grew 30,121 tons of soursops on 8,080 planted acres. That still reflected a 262 percent increase in production and a 190 percent increase in planted acres from 2000. Mexico's NPPO estimates that 200 metric tons of fresh soursops would initially be exported to the continental United States each year if exports were authorized. From 2017 to 2023, the United States imported an average of 256 tons of fresh soursops per year from Grenada, with an average value of \$1.2 million in Customs value³ and \$1.6 million in Cost, Insurance, Freight import (CIF) value,⁴ respectively.

Due to fresh soursop's short shelf-life, all soursops are air-shipped to the United States, mainly to Miami.

³ Customs value is generally defined as the price actually paid for merchandise when sold for exportation to the United States and excludes U.S. import duties, freight, insurance and other charges. (International Trade Definitions (*census.gov*).

⁴ CIF value represents the landed value of the product at the first port of arrival in the United States. It is computed by adding import charges to the Customs value and excludes U.S. import duties. (International Trade Definitions (*census.gov*).

However, as already noted, as more soursops are imported into the United States, the market may expand outside the Miami area to other metropolitan regions. In the event of such an expansion, domestic soursop producers might even be at a slight competitive harvest and timely shipping advantage for the delicate fruit within the United States, over longer imported distances.

Therefore, in accordance with § 319.56–4(c)(3)(iii), we are announcing our decision to authorize the importation into the continental United States of fresh soursop fruit from Mexico subject to the phytosanitary measures identified in the RMD that accompanies this final notice.

These conditions will be listed in the USDA, APHIS Agricultural Commodity Import Requirements (ACIR) database (<https://acir.aphis.usda.gov/s/>).⁵ In addition to these specific measures, each shipment must be subject to the general requirements listed in § 319.56–3 that are applicable to the importation of all fruits and vegetables.

Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), the recordkeeping and burden requirements associated with this action are included under the Office of Management and Budget control number 0579–0049.

E-Government Act Compliance

The Animal and Plant Health Inspection Service is committed to compliance with the E-Government Act to promote the use of the internet and other information technologies, to provide increased opportunities for citizen access to Government information and services, and for other purposes. For information pertinent to E-Government Act compliance related to this notice, please contact Mr. Joseph Moxey, APHIS' Paperwork Reduction Act Coordinator, at (301) 851–2533.

Authority: 7 U.S.C. 1633, 7701–7772, and 7781–7786; 21 U.S.C. 136 and 136a; 7 CFR 2.22, 2.80, and 371.3.

Done in Washington, DC, this 23rd day of October 2024.

Donna Lalli,

Acting Administrator, Animal and Plant Health Inspection Service.

[FR Doc. 2024–25085 Filed 10–28–24; 8:45 am]

BILLING CODE 3410–34–P

⁵ On September 30, 2022, the APHIS Fruits and Vegetables Import Requirements (FAVIR) database was replaced by the ACIR database.

DEPARTMENT OF AGRICULTURE**Forest Service****Modoc Resource Advisory Committee**

AGENCY: Forest Service, Agriculture (USDA).

ACTION: Notice of meeting.

SUMMARY: The Modoc Resource Advisory Committee (RAC) will hold a public meeting according to the details shown below. The committee is authorized under the Secure Rural Schools and Community Self-Determination Act (the Act) and operates in compliance with the Federal Advisory Committee Act. The purpose of the committee is to improve collaborative relationships and to provide advice and recommendations to the Forest Service concerning projects and funding consistent with Title II of the Act, as well as make recommendations on recreation fee proposals for sites on the Modoc National Forest within Modoc County, consistent with the Federal Lands Recreation Enhancement Act.

DATES: An in-person and virtual meeting will be held on November 13, 2024, 3 p.m. to 7 p.m. Pacific Standard Time.

Written and Oral Comments: Anyone wishing to provide in-person or virtual oral comments must pre-register by 11:59 p.m. Pacific Standard Time on November 8, 2024. Written public comments will be accepted by 11:59 p.m. Pacific Standard Time on November 8, 2024. Comments submitted after this date will be provided by the Forest Service to the committee, but the committee may not have adequate time to consider those comments prior to the meeting.

All committee meetings are subject to cancellation. For status of the meeting prior to attendance, please contact the person listed under **FOR FURTHER INFORMATION CONTACT**.

ADDRESSES: This meeting will be held in-person at the Modoc National Forest Supervisor's Office Conference Room, located at 225 West 8th Street Alturas, California 96101. The public may also join the meeting virtually via webcast, teleconference, videoconference, or Homeland Security Information Network virtual meeting online at: www.fs.usda.gov/main/modoc/workingtogether/advisorycommittees. RAC information and meeting details can be found on the website or by contacting the person listed under **FOR FURTHER INFORMATION CONTACT**.

Written Comments: Written comments must be sent by email to samantha.jager@usda.gov or via mail

(postmarked) to RAC Coordinator, 225 West 8th Street, Alturas, California, 96101. The Forest Service strongly prefers comments be submitted electronically.

Oral Comments: Persons or organizations wishing to make oral comments must pre-register by 11:59 p.m. Pacific Standard Time, November 8, 2024, and speakers can only register for one speaking slot. Oral comments must be sent by email to samantha.jager@usda.gov or via mail (postmarked) to USFS RAC Coordinator, 225 West 8th Street, Alturas, California, 96101.

FOR FURTHER INFORMATION CONTACT: Ian Reid, Designated Federal Officer, by phone at (530) 233-5811 or email at ian.reid2@usda.gov; or Samantha Jager, RAC Coordinator, by phone at (530) 708-7291 or email at samantha.jager@usda.gov.

SUPPLEMENTARY INFORMATION: The purpose of the meeting is to:

1. Discuss any old business from last year;
2. Finalize award amounts on chosen proposals;
3. Discuss committee vacancies;
4. Approve meeting minutes;
5. Schedule the next meeting.

The agenda will include time for individuals to make oral statements of three minutes or less. Individuals wishing to make an oral statement should make a request in writing at least three days prior to the meeting date to be scheduled on the agenda. Written comments may be submitted to the Forest Service up to 14 days after the meeting date listed under **DATES**.

Please contact the person listed under **FOR FURTHER INFORMATION CONTACT**, by or before the deadline, for all questions related to the meeting. All comments, including names and addresses when provided, are placed in the record and are available for public inspection and copying. The public may inspect comments received upon request.

Meeting Accommodations: The meeting location is compliant with the Americans with Disabilities Act, and the USDA provides reasonable accommodation to individuals with disabilities where appropriate. If you are a person requiring reasonable accommodation, please make requests in advance for sign language interpretation, assistive listening devices, or other reasonable accommodation to the person listed under the **FOR FURTHER INFORMATION CONTACT** section or contact USDA's TARGET Center at (202) 720-2600 (voice and TTY) or USDA through the Federal Relay Service at (800) 877-8339.

Additionally, program information may be made available in languages other than English.

USDA programs are prohibited from discriminating based on race, color, national origin, religion, sex, gender identity (including gender expression), sexual orientation, disability, age, marital status, family/parental status, income derived from a public assistance program, political beliefs, or reprisal or retaliation for prior civil rights activity, in any program or activity conducted or funded by USDA (not all bases apply to all programs). Remedies and complaint filing deadlines vary by program or incident.

Equal opportunity practices in accordance with USDA's policies will be followed in all appointments to the committee. To ensure that the recommendations of the committee have taken into account the needs of the diverse groups served by the USDA, membership shall include, to the extent practicable, individuals with demonstrated ability to represent the many communities, identities, races, ethnicities, backgrounds, abilities, cultures, and beliefs of the American people, including underserved communities. USDA is an equal opportunity provider, employer, and lender.

Dated: October 16, 2024.

Cikena Reid,

USDA Committee Management Officer.

[FR Doc. 2024-24375 Filed 10-28-24; 8:45 am]

BILLING CODE 3411-15-P

COMMISSION ON CIVIL RIGHTS**Notice of Public Meeting of the Colorado Advisory Committee to the U.S. Commission on Civil Rights**

AGENCY: Commission on Civil Rights

ACTION: Notice of public meeting.

SUMMARY: Notice is hereby given, pursuant to the provisions of the rules and regulations of the U.S. Commission on Civil Rights (Commission) and the Federal Advisory Committee Act that the Colorado Advisory Committee (Committee) to the U.S. Commission on Civil Rights will convene a monthly virtual business meeting on Wednesday, November 20, 2024, at 3 p.m. Mountain Time. The purpose of the meeting is to review the final version of its report on public school attendance zones in Colorado. The committee will vote on the report and discuss next steps.

DATES: Wednesday, November 20, 2024, at 3 p.m. Mountain Time.

ADDRESSES: The meeting will be held via Zoom.

Meeting Link (Audio/Visual): <https://tinyurl.com/279ffjudv>; password: USCCR-CO.

Join by Phone (Audio Only): 1-833 435 1820; Meeting ID: 160 614 2807#.

FOR FURTHER INFORMATION CONTACT:

Barbara Delaviez, Designated Federal Official, at bdelaviez@usCCR.gov, or by phone at 202-539-8246.

SUPPLEMENTARY INFORMATION: These committee meeting is available to the public through the meeting link above. Any interested member of the public may listen to the meeting. At the meeting, an open comment period will be provided to allow members of the public to make a statement as time allows. Per the Federal Advisory Committee Act, public minutes of the meeting will include a list of persons who are present at the meeting. If joining via phone, callers can expect to incur regular charges for calls they initiate over wireless lines, according to their wireless plan. The Commission will not refund any incurred charges. Callers will incur no charge for calls they initiate over land-line connections to the toll-free telephone number. Closed captioning will be available for individuals who are deaf, hard of hearing, or who have certain cognitive or learning impairments. To request additional accommodations, please email ebohor@usCCR.gov at least 10 business days prior to the meeting.

Members of the public are entitled to submit written comments; the comments must be received in the regional office within 30 days following the meetings. Written comments may be emailed to Barbara Delaviez at bdelaviez@usCCR.gov. Persons who desire additional information may contact the Regional Programs Coordination Unit at 1-312-353-8311.

Records generated from these meetings may be inspected and reproduced at the Regional Programs Coordination Unit Office, as they become available, both before and after the meetings. Records of the meeting will be available via www.facadatabase.gov under the Commission on Civil Rights, Colorado Advisory Committee link. Persons interested in the work of this Committee are directed to the Commission's website, <http://www.usCCR.gov>, or may contact the Regional Programs Coordination Unit at ebohor@usCCR.gov.

Agenda

- I. Welcome and Roll Call
- II. Report Stage: Discuss and Vote on Report—Public School Attendance Zones

III. Discuss Next Steps

IV. Public Comment

V. Adjournment

Dated: October 24, 2024.

David Mussatt,

Supervisory Chief, Regional Programs Unit.

[FR Doc. 2024-25095 Filed 10-28-24; 8:45 am]

BILLING CODE P

COMMISSION ON CIVIL RIGHTS

Notice of Public Briefing of the Hawai'i Advisory Committee to the U.S. Commission on Civil Rights

AGENCY: U.S. Commission on Civil Rights.

ACTION: Notice of Public Briefing.

SUMMARY: Notice is hereby given, pursuant to the provisions of the rules and regulations of the U.S. Commission on Civil Rights (Commission) and the Federal Advisory Committee Act (FACA), that the Hawai'i Advisory Committee (Committee) to the U.S. Commission on Civil Rights will convene by ZoomGov on Wednesday, November 6, 2024, from 9:00 a.m. to 11:00 a.m. HST, to collect testimony on their topic "Examining Hawaii's Child Welfare System and the Overrepresentation of Native Hawaiian Children and Families."

DATES: Wednesday, November 6, 2024, from 9:00 a.m.–11:00 a.m. Hawai'i Standard Time.

ADDRESSES: The briefing will be held via Zoom Webinar.

Registration Link (Audio/Visual): <https://www.zoomgov.com/webinar/register/WN/8NxGTECqQ2qhiUoUnfx2Q>.

Join by Phone (Audio Only): (833) 435-1820 USA Toll Free; Webinar ID: 160 656 2501.

FOR FURTHER INFORMATION CONTACT:

Kayla Fajota, Designated Federal Officer (DFO) at kfajota@usCCR.gov or (434) 515-2395.

SUPPLEMENTARY INFORMATION:

Committee meetings are available to the public through the videoconference link above. Any interested member of the public may listen to the meeting. An open comment period will be provided to allow members of the public to make a statement as time allows. Per the Federal Advisory Committee Act, public minutes of the meeting will include a list of persons who are present at the meeting. If joining via phone, callers can expect to incur regular charges for calls they initiate over wireless lines, according to their wireless plan. The Commission will not refund any incurred charges. Closed captions will

be provided for individuals who are deaf, hard of hearing, or who have certain cognitive or learning impairments. To request additional accommodations, please email Angelica Trevino, Support Services Specialists, at atrevino@usCCR.gov at least 10 business days prior to the meeting. Members of the public are entitled to make comments during the open period at the end of the meeting. Members of the public may also submit written comments; the comments must be received in the Regional Programs Unit within 30 days following the meeting. Written comments may be emailed to Kayla Fajota (DFO) at kfajota@usCCR.gov.

Records generated from this meeting may be inspected and reproduced at the Regional Programs Coordination Unit Office, as they become available, both before and after the meeting. Records of the meetings will be available via www.facadatabase.gov under the Commission on Civil Rights, Hawai'i Advisory Committee link. Persons interested in the work of this Committee are directed to the Commission's website, <http://www.usCCR.gov>, or may contact the Regional Programs Coordination Unit at atrevino@usCCR.gov.

Agenda

- I. Welcome and Roll Call
- II. Chair Remarks
- III. Panelists Presentations
- IV. Committee Q&A
- V. Public Comment
- VI. Adjournment

Dated: October 24, 2024.

David Mussatt,

Supervisory Chief, Regional Programs Unit.

[FR Doc. 2024-25094 Filed 10-28-24; 8:45 am]

BILLING CODE 6335-01-P

DEPARTMENT OF COMMERCE

International Trade Administration

Massachusetts Institute of Technology, et. al; Application(s) for Duty-Free Entry of Scientific Instruments

Pursuant to Section 6(c) of the Educational, Scientific and Cultural Materials Importation Act of 1966 (Pub. L. 89-651, as amended by Pub. L. 106-36; 80 Stat. 897; 15 CFR part 301), we invite comments on the question of whether instruments of equivalent scientific value, for the purposes for which the instruments shown below are intended to be used, are being manufactured in the United States.

Comments must comply with 15 CFR 301.5(a)(3) and (4) of the regulations and

be postmarked on or before November 18, 2024. Address written comments to Statutory Import Programs Staff, Room 41006, U.S. Department of Commerce, Washington, DC 20230. Please also email a copy of those comments to Dianne.Hanshaw@trade.gov.

Docket Number: 24–026. Applicant: Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139. Instrument: Narrow line width laser, FL–SF–1695–0.5–CW. Manufacturer: Shanghai Precilaser Technology, Co., Ltd., China. Intended Use: The instrument is intended to be used as a single frequency laser system at 1695 nm that will be used in quantum physics experiments at MIT for improved optical atomic clocks and precision measurement using ytterbium (^{171}Yb). The 1695nm frequency is the Yb optical transition between the ground state $4f^{14}6s6p\ ^3P_0$ and the metastable state $4f^{13}6s^25d(J=2)$, where J represents the total angular momentum. This transition allows the possibility of dual-mode optical lattice clocks to further reduce the uncertainty from external level shifts, as well as physics beyond the standard model (for example investigating a potential mediating particle for forces between electron and neutron). Justification for Duty-Free Entry: According to the applicant, there are no instruments of the same general category manufactured in the United States. Application accepted by Commissioner of Customs: August 8, 2024.

Docket Number: 24–027. Applicant: Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02114. Instrument: Low noise laser system. Manufacturer: Shanghai Precilasers Technology Co., Ltd., China. Intended Use: The instrument is intended to be used for Sodium potassium molecules confined in optical dipole traps. Sodium potassium molecules are fermionic molecules possessing large electric dipole moment. Clouds of sodium-23 and potassium-40 atoms are first laser-cooled into suitable ultracold temperatures and loaded into optical dipole traps. A two-photon Raman process using the laser system to be imported then binds pairs of sodium-23 and potassium-40 atoms into deeply bound molecules in their absolute ground state. Direct control of quantum states of molecules is difficult owing to the structural complexity of molecules. Binding molecules from laser-cooled and well-controlled atoms provides a more feasible alternative to controlling and manipulating quantum states of molecules. Justification for Duty-Free Entry: According to the applicant, there are no instruments of the same general

category manufactured in the United States. Application accepted by Commissioner of Customs: August 27, 2024.

Docket Number: 24–029. Applicant: Harvard University, 1033 Massachusetts Avenue, Cambridge, MA 02138. Instrument: Narrow Line-width laser. Manufacturer: Shanghai Precilasers Technology Co., Ltd., China. Intended Use: The narrow linewidth (<2kHz), ultralow noise (intensity and phase), large tuning range (>1nm) seed laser at 1591 nm will be used as a seed to be doubled down to 795 nm. The seed laser will be used in a quantum physics experiment at Harvard for laser cooling and trapping experiments for Rubidium atoms to explore quantum physics research. The research work enabled by this system is part of the training of graduate students, undergraduate students, and postdoctoral research fellows. Justification for Duty-Free Entry: According to the applicant, there are no instruments of the same general category manufactured in the United States. Application accepted by Commissioner of Customs: August 23, 2024.

Docket Number: 24–030. Applicant: University of Michigan, Naval Architecture and Marine Engineering, West Hall RM 126, 1085 S University Avenue, Ann Arbor, MI 48109. Instrument: Wave Generator System. Manufacturer: Van Halteren Technologies Boxtel BV, Netherlands. Intended Use: The instrument is intended to be used to study ship motions in water waves. Ship models in fresh water are to be investigated. The experiments to be conducted will involve the creation of model scale ocean waves. The objective is an engineering understanding of wave mechanics and the response of ship metrics. Justification for Duty-Free Entry: According to the applicant, there are no instruments of the same general category manufactured in the United States. Application accepted by Commissioner of Customs: April 10, 2024.

Docket Number: 24–031. Applicant: University of Chicago, 929 E 57th Street, GCIS ESB41, Chicago, IL 60637. Instrument: Fiber Laser. Manufacturer: PreciLasers, China. Intended Use: The instrument is intended to be used to study the Cold molecular Nuclear Time-Reversal Experiment (CeNTREX), a collaborative physics experiment between University of Massachusetts Amherst, Columbia University, Yale University, University of Chicago, and Argonne National Laboratory. The goal of the CeNTREX project is to shed light on the reasons for why there is more

matter than antimatter in the Universe through the measurement of properties of the thallium-205 nucleus.

Justification for Duty-Free Entry: According to the applicant, there are no instruments of the same general category manufactured in the United States. Application accepted by Commissioner of Customs: August 27, 2024.

Docket Number: 24–032. Applicant: University of California, Santa Barbara, 2509 Broida Hall, Santa Barbara, CA 93106–9530. Instrument: Low Noise Laser Amplifier. Manufacturer: Shanghai Precilaser Technology Co., Ltd., China. Intended Use: The instrument is intended to be used in a cold atom experiment at the University of California, Santa Barbara, for optical trapping and manipulation of cold lithium-7 atoms. It will be seeded by 100 nW 1064 laser and will produce 100 W output power. The low relative intensity noise (RIN) of this laser amplifier is critical, because the intensity noise contributes a lot to the stability of the optical traps, and the atom interferometry experiment is very sensitive to the noise of the optical traps. Justification for Duty-Free Entry: According to the applicant, there are no instruments of the same general category manufactured in the United States. Application accepted by Commissioner of Customs: September 17, 2024.

Docket Number: 24–033. Applicant: Harvard University, 17 Oxford Street, Jefferson 158, Cambridge, MA 02138. Instrument: High Power Single Frequency Fiber Amplifier. Manufacturer: Connet Laser Technology Co., Ltd., China. Intended Use: The high power (30 W), single frequency fiber amplifier system 1908 nm will be used in a quantum physics experiment at Harvard for optical tweezer trapping of rubidium-87 atoms. The available laser power will allow many more of these atoms (thousands) to be controlled than previously demonstrated (hundreds). This platform will allow the study of larger quantum systems with properties and fidelities far exceeding smaller systems. Justification for Duty-Free Entry: According to the applicant, there are no instruments of the same general category manufactured in the United States. Application accepted by Commissioner of Customs: September 18, 2024.

Dated: October 23, 2024.

Gregory W. Campbell,
Director, *Subsidies and Economic Analysis,*
Enforcement and Compliance.

[FR Doc. 2024–25091 Filed 10–28–24; 8:45 am]

BILLING CODE 3510-DS-P

DEPARTMENT OF COMMERCE

International Trade Administration

[A–201–831]

Prestressed Concrete Steel Wire Strand From Mexico: Final Affirmative Determination of Circumvention of the Antidumping Duty Order; Correction

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: The U.S. Department of Commerce (Commerce) published notice in the **Federal Register** of September 27, 2024, in which Commerce published the final determination in the circumvention inquiry of the antidumping duty (AD) order on prestressed concrete steel wire strand (PC strand) from Mexico. This notice omitted the section ordering the liquidation of entries of merchandise subject to the AD order on PC strand from Mexico as a result of the affirmative determination of circumvention.

DATES: Applicable October 29, 2024.

FOR FURTHER INFORMATION CONTACT: Jonathan Schueler, AD/CVD Operations, Office VIII, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482–9175.

SUPPLEMENTARY INFORMATION:**Background**

On September 27, 2024, Commerce published in the **Federal Register** the final determination in the circumvention inquiry for the AD order on PC strand Mexico.¹ In the *Final Determination*, we inadvertently omitted the “Liquidation of Entries” section announcing our intent to order the liquidation of entries of merchandise subject to the AD order on PC strand from Mexico that entered during the prior administrative review period for the AD order on PC strand from Mexico. Specifically, Commerce did not receive a request to conduct an administrative review for the AD order on PC strand from Mexico for the period from January 1, 2023, to December 31, 2023,² thus entries of subject

¹ See *Prestressed Concrete Steel Wire Strand from Mexico: Final Affirmative Determination of Circumvention of the Antidumping Duty Order*, 89 FR 79252 (September 27, 2024) (*Final Determination*), and accompanying Issues and Decision Memorandum.

² See *Antidumping or Countervailing Duty Order, Finding, or Suspended Investigation; Opportunity to Request Administrative Review and Join Annual*

merchandise during this period were automatically liquidated pursuant to 19 CFR 351.212(c). However, following the *Preliminary Determination*, Commerce instructed U.S. Customs and Border Protection (CBP) to collect cash deposits and suspend the liquidation of entries of merchandise covered by the inquiry that were entered, or withdrawn from warehouse, for consumption on or after July 31, 2023, until specific instructions for liquidation were issued.³

Correction

In the **Federal Register** of September 27, 2024, in FR Doc 2024–22113, on page 79253, in the third column, correct the text by adding the following section below the “Final Circumvention Determination” section:

Liquidation of Entries

For all entries of merchandise subject to the AD order on PC strand from Mexico, entered or withdrawn from warehouse for consumption on or before December 31, 2023, Commerce intends to instruct U.S. Customs and Border Protection (CBP) to liquidate those entries at the applicable AD rates for those entries.⁴

Commerce intends to issue liquidation instructions to CBP no earlier than 41 days after the date of publication of this notice in the **Federal Register**. If a timely notice of intent to contest this final determination is filed at the U.S. Court of International Trade, the assessment instructions will direct CBP not to liquidate relevant entries until the time for parties to file a request for a statutory injunction has expired (*i.e.*, within 90 days of publication).

Notification to Interested Parties

This notice is issued and published in accordance with section 781(a) of the Act and 19 CFR 351.226(g)(2).

Inquiry Service List, 89 FR 63, 64 (January 2, 2024); see also *Initiation of Antidumping and Countervailing Duty Administrative Reviews*, 89 FR 15827 (March 5, 2024).

³ See *Antidumping Duty Order on Prestressed Concrete Steel Wire Strand from Mexico: Preliminary Affirmative Determination of Circumvention*, 89 FR 22668 (April 2, 2024) (*Preliminary Determination*), and accompanying Preliminary Decision Memorandum.

⁴ Commerce is not conducting an administrative review of the AD order on PC strand from Mexico for the period ending on December 31, 2023. Therefore, Commerce will instruct CBP to liquidate all entries through the end of the last administrative review period.

Dated: October 23, 2024.

Ryan Majerus,

Deputy Assistant Secretary for Policy and Negotiations, performing the non-exclusive functions and duties of the Assistant Secretary for Enforcement and Compliance.

[FR Doc. 2024–25075 Filed 10–28–24; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XE185]

Takes of Marine Mammals Incidental to Specified Activities; Taking Marine Mammals Incidental to the Atlantic Shores South Project Offshore of New Jersey

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice; issuance of letter of authorization.

SUMMARY: In accordance with the Marine Mammal Protection Act (MMPA) as amended, and implementing regulations, notification is hereby given that a Letter of Authorization (LOA) has been issued to Atlantic Shores Offshore Wind Project 1, LLC (Project Company 1), for the taking of marine mammals incidental to the construction of the Atlantic Shores South Project (hereafter known as the “Project”).

DATES: The LOA is effective from January 1, 2025 through December 31, 2029.

ADDRESSES: The LOA and supporting documentation are available online at: <https://www.fisheries.noaa.gov/permit/incidental-take-authorizations-under-marine-mammal-protection-act>. In case of problems accessing these documents, please call the contact listed below (see **FOR FURTHER INFORMATION CONTACT**).

FOR FURTHER INFORMATION CONTACT: Kelsey Potlock, Office of Protected Resources, NMFS, (301) 427–8401.

SUPPLEMENTARY INFORMATION:**Background**

The MMPA prohibits the “take” of marine mammals, with certain exceptions. Sections 101(a)(5)(A) and (D) of the MMPA (16 U.S.C. 1361 *et seq.*) direct the Secretary of Commerce (as delegated to NMFS) to allow, upon request, the incidental, but not intentional, taking of small numbers of marine mammals by U.S. citizens who engage in a specified activity (other than commercial fishing) within a specified

geographical region if certain findings are made, regulations are promulgated (when applicable), and public notice and an opportunity for public comment are provided.

An authorization for incidental takings shall be granted if NMFS finds that the taking will have a negligible impact on the species or stock(s) and will not have an unmitigable adverse impact on the availability of the species or stock(s) for taking for subsistence uses (where relevant). If such findings are made, NMFS must prescribe the permissible methods of taking; “other means of effecting the least practicable adverse impact” on the affected species or stocks and their habitat, paying particular attention to rookeries, mating grounds, and areas of similar significance, and on the availability of the species or stocks for taking for certain subsistence uses (referred to as “mitigation”); and requirements pertaining to the monitoring and reporting of such takings. The MMPA defines “take” to mean harass, hunt, capture, or kill, or attempt to harass, hunt, capture, or kill any marine mammal (16 U.S.C. 1362(13); 50 CFR 216.103). Level A harassment is defined as any act of pursuit, torment, or annoyance which has the potential to injure a marine mammal or marine mammal stock in the wild (16 U.S.C. 1362(18); 50 CFR 216.3). Level B harassment is defined as any act of pursuit, torment, or annoyance which has the potential to disturb a marine mammal or marine mammal stock in the wild by causing disruption of behavioral patterns, including, but not limited to, migration, breathing, nursing, breeding, feeding, or sheltering (16 U.S.C. 1362(18); 50 CFR 216.3). Section 101(a)(5)(A) of the MMPA and the implementing regulations at 50 CFR part 216, subpart I authorize NMFS to propose and, if appropriate, promulgate regulations and issue an associated LOA. NMFS promulgated regulations on January 23, 2024 (89 FR 4370) for the taking of marine mammals incidental to the construction of the Atlantic Shores South Project offshore of New Jersey. The LOA authorizes Project Company 1, and those persons it authorizes or funds to conduct activities on its behalf, to take marine mammals incidental to specified activities during the construction of the Project and requires them to implement mitigation, monitoring, and reporting requirements.

Summary of Request

In response to their petition to promulgate incidental take regulations and issue an associated Letter of Authorization, on September 24, 2024,

NMFS promulgated a final rule (89 FR 77972) establishing a framework for authorizing the taking of marine mammals by Project Company 1. Specifically, the rule allows for take of 16 species of marine mammals comprising 17 stocks by Level B harassment (all 17 stocks) and by Level A harassment (9 stocks) incidental to construction activities occurring in Federal and State waters off of New Jersey, specifically within and around the Bureau of Ocean Energy Management (BOEM) Commercial Lease of Submerged Lands for Renewable Energy Development on the Outer Continental Shelf (OCS) Lease Areas OCS-A 0499 and OCS-A-0570 (collectively, “Lease Area”) and along two export cable routes to sea-to-shore transition points (collectively referred to as the “Project Area”), over the course of 5 years (January 1, 2025 through December 31, 2029). The final rule included the following specified activities: the installation of up to 200 wind turbine generators (WTGs) on jacket and/or monopile foundations using impact pile driving; the installation of up to 10 offshore substations (OSSs) on multi-legged jacket foundations using pin piles using impact pile driving; the installation of one meteorological tower (Met Tower) on a monopile using impact pile driving; nearshore cable landfall work comprising of the installation and subsequent removal of nearshore temporary cofferdams at the sea-to-shore transition points located in Sea Girt, New Jersey (the Monmouth landfall site) and in Atlantic City, New Jersey (the Atlantic City landfall site) by vibratory pile driving; high-resolution geophysical (HRG) marine site characterization surveys using active acoustic sources; fishery and ecological monitoring surveys; the deployment of up to four temporary meteorological and oceanographic (metocean) buoys; the placement of scour protection; the installation of the export cable routes from OSSs to shore-based converter stations and inter-array cables between turbines by trenching, laying, and burial activities; vessel transit within the specified geographical region to transport crew, supplies, and materials; and WTG operation.

Marine mammals exposed to elevated noise levels during foundation impact pile driving may be taken by Level A harassment, and marine mammals exposed to elevated noise levels during impact and vibratory pile driving and HRG site characterization surveys may be taken by Level B harassment. No

mortality or serious injury of any marine mammal is anticipated or authorized.

Authorization

In accordance with the MMPA, as amended, NMFS has issued a LOA to Project Company 1 authorizing the take, by harassment, of marine mammals incidental to specified activities within the specified geographical region. As previously stated, no mortality or serious injury of any marine mammal species is anticipated or authorized. The incidental takes authorized herein are the same as those analyzed and authorized in the final rule (89 FR 77972, September 24, 2024). The number of takes, by species, authorized may be found in table 1 in the LOA, which is available at <https://www.fisheries.noaa.gov/permit/incidental-take-authorizations-under-marine-mammal-protection-act>.

Takes of marine mammals will be minimized through the following required mitigation and monitoring measures, as applicable for each specified activity: (1) implementation of seasonal/time of day work restrictions; (2) use of multiple NMFS-approved Protected Species Observers to visually observe for marine mammals (with any detection within specifically designated zones triggering a delay or shutdown, as applicable); (3) use of NMFS-approved passive acoustic monitoring (PAM) operators to acoustically detect marine mammals, with a focus on detecting baleen whales (with any detection within designated zones triggering a delay or shutdown, as applicable); (4) implementation of clearance and shutdown zones; (5) use of soft-start upon commencement of impact pile driving and ramp-up of certain acoustic sources during HRG surveys; (6) use of noise attenuation technology during foundation pile driving; (7) use of situational awareness monitoring for marine mammal presence; (8) use of sound field verification monitoring; (9) use of PAM within the vessel transit corridor for Project vessels to travel over 10 knots (11.5 miles per hour); (10) implementation of several vessel strike avoidance measures to avoid vessel strikes, including but not limited to, vessel speed restrictions and separation zones between marine mammals and project vessels; and (11) requirements for personal training, gear use, and actions required to be undertaken for trawl surveys during fishery monitoring surveys. Additionally, NMFS may modify the LOA’s mitigation, monitoring, or reporting measures, based on new information. Project Company 1 is also required to submit

frequent and situational reports, as specified in the LOA.

Based on the findings discussed in the preamble of the final rule, NMFS has determined that the take authorized in the LOA is of small numbers, will have a negligible impact on marine mammal stocks, will not have an unmitigable adverse impact on the availability of the affected marine mammal stock for subsistence uses, and the mitigation measures provide a means of affecting the least practicable adverse impact on the affected stocks and their habitat.

Dated: October 24, 2024.

Kimberly Damon-Randall,

*Director, Office of Protected Resources,
National Marine Fisheries Service.*

[FR Doc. 2024–25090 Filed 10–28–24; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Transmittal No. 23–66]

Arms Sales Notification

AGENCY: Defense Security Cooperation Agency, Department of Defense (DoD).

ACTION: Arms sales notice.

SUMMARY: The DoD is publishing the unclassified text of an arms sales notification.

FOR FURTHER INFORMATION CONTACT:

Pamela Young at (703) 953–6092, pamela.a.young14.civ@mail.mil, or dsca.ncr.rsrcmgmt.list.cns-mbx@mail.mil.

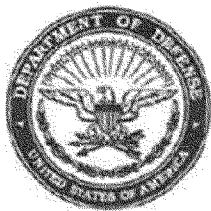
SUPPLEMENTARY INFORMATION: This 36(b)(1) arms sales notification is published to fulfill the requirements of section 155 of Public Law 104–164 dated July 21, 1996. The following is a copy of a letter to the Speaker of the House of Representatives with attached Transmittal 23–66, Policy Justification, and Sensitivity of Technology.

Dated: October 24, 2024.

Aaron T. Siegel,

*Alternate OSD Federal Register Liaison
Officer, Department of Defense.*

BILLING CODE 6001–FR–P



DEFENSE SECURITY COOPERATION AGENCY
2800 Defense Pentagon
Washington, DC 20301-2800

September 1, 2023

The Honorable Kevin McCarthy
Speaker of the House
U.S. House of Representatives
H-209, The Capitol
Washington, DC 20515

Dear Mr. Speaker:

Pursuant to the reporting requirements of Section 36(b)(1) of the Arms Export Control Act, as amended, we are forwarding herewith Transmittal No. 23-66, concerning the Army's proposed Letter(s) of Offer and Acceptance to the Government of the Republic of Bulgaria for defense articles and services estimated to cost \$1.5 billion. We will issue a news release to notify the public of this proposed sale upon delivery of this letter to your office.

Sincerely,

James A. Hursch
Director

Enclosures:

1. Transmittal
2. Policy Justification
3. Sensitivity of Technology

BILLING CODE 6001-FR-C

Transmittal No. 23-66

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act, as amended

(i) Prospective Purchaser: Government of the Republic of Bulgaria

(ii) Total Estimated Value:

Major Defense Equipment * ..	\$1.0 billion
Other	\$.5 billion

TOTAL \$1.5 billion

Funding Source: National Funds

(iii) Description and Quantity or Quantities of Articles or Services under Consideration for Purchase: The Government of the Republic of Bulgaria has requested to buy one hundred eighty-three (183) Stryker Family of Vehicles, including:

Major Defense Equipment (MDE):
Ninety (90) XM1296 Infantry Carrier Vehicles—Dragoon (ICVD)
Seventeen (17) M1126 Infantry Carrier Vehicles (ICV)
Nine (9) M1132 Engineer Squad Vehicles (ESV)

Thirty-three (33) M1130 Command Vehicles (CV)
Twenty-four (24) M1133 Medical Evacuation Vehicles (MEV)
Ten (10) M1135 Nuclear, Biological, Chemical Reconnaissance Vehicles (NBCRV)
Five (5) Heavy Expanded Mobility Tactical Truck (HEMTT) Light Equipment Transport (LET)
Five (5) Modular Catastrophic Recovery System (MCRS)
Two (2) M1120A4 HEMTT Load Handling System
Five (5) M984A4 Wrecker HEMTT

One hundred seven (107) M240 Coaxial 7.62mm Machine Guns
Non-MDE:

The following are also included: support service equipment; M-153A4 Common Remote Operated Weapons Stations (CROWS); Forward Repair Systems (FRS); M2A1 .50 caliber machine guns; M6 smoke grenade launchers and associated spares; Harris radios; AN/VAS-5 Driver's Vision Enhancer (DVE); DVE-Wide; communications equipment; RS6 (LW30) Remote Weapon Systems; TACFLIR 280 HDEP systems; Ranger R20SS Radar; ROVER6Si transceivers; spare parts; Basic Issue Items (BII), Components of End Items (COEI), and Additional Authorized List (AAL); Special Tools and Test Equipment (STTE); technical manuals; OCONUS Deprocessing Service; OCONUS contractor provided training and Field Service Representatives (FSR); component assembly in-country; and other related elements of logistics and program support.

(iv) Military Department: Army (BU-B-UCP, BU-B-UCS)

(v) Prior Related Cases, if any: None

(vi) Sales Commission, Fee, etc., Paid, Offered, or Agreed to be Paid: None

(vii) Sensitivity of Technology Contained in the Defense Article or Defense Services Proposed to be Sold: See Attached Annex

(viii) Date Report Delivered to Congress: September 1, 2023

* As defined in Section 47(6) of the Arms Export Control Act.

POLICY JUSTIFICATION

Bulgaria—Stryker Vehicles

The Government of the Republic of Bulgaria has requested to buy one hundred eighty-three (183) Stryker Family of Vehicles. The proposed sale would consist of: ninety (90) XM1296 Infantry Carrier Vehicles—Dragoon (ICVD); seventeen (17) M1126 Infantry Carrier Vehicles (ICV); nine (9) M1132 Engineer Squad Vehicles (ESV); thirty-three (33) M1130 Command Vehicles (CV); twenty-four (24) M1133 Medical Evacuation Vehicles (MEV); ten (10) M1135 Nuclear, Biological, Chemical Reconnaissance Vehicles (NBCRV); five (5) Heavy Expanded Mobility Tactical Truck (HEMTT) Light Equipment Transports (LET); five (5) Modular Catastrophic Recovery Systems (MCRS); two (2) M1120A4 HEMTT Load Handling Systems; five (5) M984A4 Wrecker HEMTTs; and one hundred seven (107) M240 Coaxial 7.62mm machine guns. Also included is support service equipment; M-153A4 Common Remote Operated Weapons Stations

(CROWS); Forward Repair Systems (FRS); M2A1 .50 caliber machine guns; M6 smoke grenade launchers and associated spares; Harris radios; AN/VAS-5 Driver's Vision Enhancer (DVE); DVE-Wide; communications equipment; RS6 (LW30) Remote Weapon Systems; TACFLIR 280 HDEP systems; Ranger R20SS Radar; ROVER6Si transceivers; spare parts; Basic Issue Items (BII), Components of End Items (COEI), and Additional Authorized List (AAL); Special Tools and Test Equipment (STTE); technical manuals; OCONUS Deprocessing Service; OCONUS contractor provided training and Field Service Representatives (FSR); component assembly in-country; and other related elements of logistics and program support. The estimated total cost is \$1.5 billion.

This proposed sale will support the foreign policy and national security objectives of the United States by helping to improve the security of a North Atlantic Treaty Organization ally that is a force for political stability and economic progress in Europe.

The proposed sale will improve Bulgaria's rapid infantry deployment and force projection capability. Bulgaria will use this enhanced capability to strengthen its homeland defense and deter regional threats. Bulgaria will have no difficulty absorbing this equipment and services into its armed forces.

The principal contractor will be General Dynamics Land Systems, Anniston, AL. There are no known offset agreements proposed in connection with this potential sale.

Implementation of this proposed sale will require twenty (20) Stryker contractor representatives to travel to Bulgaria for twenty-four (24) months to conduct contractor logistics support, training, and component assembly support.

There will be no adverse impact on U.S. defense readiness as a result of this proposed sale.

Transmittal No. 23-66

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act

Annex

Item No. vii

(vii) *Sensitivity of Technology:*

1. The Stryker Family of Vehicles (FoV) are all derived from the Flat Bottom Infantry Carrier Vehicle (ICV). The ICV supplies the common suspension (except for the ICVD), drive line, major C4 components, and hull to the FoV. The FoV is powered by a 350 horsepower C7 Caterpillar diesel engine and runs on eight wheels that feature

run flat capability and a central tire inflation system (CTIS). It contains a vehicle height management system to aid in transportability. The FoV is supported by a communications suite that integrates the Single Channel Ground and Airborne Radio System (SINCGARS) radio family and Global Positioning System (GPS) and their commercially exportable equivalents, and has a Mission Equipment Package that add to the ICV common capabilities. The Stryker is deployable by C-130 aircraft and is combat capable upon arrival; it is also capable of self-deployment by highway and can conduct self-recovery. It has a low noise level that reduces crew fatigue and enhances survivability. It moves about the battlefield quickly and is optimized for close, complex, or urban terrain. The Stryker program leverages non-developmental items with common subsystems and components to quickly acquire and field these systems.

2. The XM914E1 is a single feed chain gun that fires linked, percussion-primed 30mm x 113mm ammunition. The gun is powered by a 1 horsepower 28V (volt) direct current (DC) motor and incorporates hang fire safety protection. Actual operation of the gun is accomplished via the platform's fire control system in conjunction with and through the dedicated Gun Control Unit (GCU). The GCU provides all electrical power to the gun, including operational and sensor level 28V DC power. The weapon has a cyclic firing rate of 200 ± 25 shots per minute. Actual firing rate varies within the specification range due to system level characteristics, such as inputted voltage and ammunition feed system loads.

3. The RS6 Remote Weapon System (RWS) is an externally mounted weapon mounting and control system that allows the gunner to remain inside the vehicle protected by armor while firing a variety of crew-served weapons, including the XM914E1 chain gun. The RS6 allows for remote day and night sighting and ballistic control capability, providing first-burst engagement of targets at maximum effective weapon range while on the move.

4. The AN/VAS-5 Driver's Vision Enhancer (DVE) is compact thermal camera providing armored vehicle drivers with day or nighttime visual awareness in clear or reduced vision (fog, smoke, dust, etc.) situations. The system provides the driver a 50-degree viewing angle using a high-resolution infrared sensor and image stabilization to reduce the effect of shock and vibration. The viewer and monitor are ruggedized for operation in tactical environments.

5. The Driver's Vision Enhancer (DVE-Wide) mounted on the XM1296 ICVD, is a compact thermal camera providing armored vehicle drivers with day or nighttime visual awareness in clear or reduced vision (fog, smoke, dust, etc.) situations. The system provides the driver a 180-degree viewing angle using a high-resolution infrared sensor and image stabilization to reduce the effect of shock and vibration. The viewer and monitor are ruggedized for operation in tactical environments.

1. The Common Remote Operated Weapon Station (CROWS) is an externally-mounted weapon mounting and control system that allows the gunner to remain inside the vehicle protected by armor while firing a variety of crew-served weapons. The CROWS allows for remote day and night sighting and ballistic control capability, providing first-burst engagement of targets at maximum effective weapon range while on the move.

2. hC2 BMS solution—the hC2 Software Suite is a complete COMMAND and Control (C2) solution that offers clarity, simplicity, and high performance to address real world C2 challenges at all echelon levels. The hC2 Suite connects the headquarters all the way down the echelon to the tactical edge. At the core of the hC2 Suite is hC2 Tactical Communications, which enables full integration and interoperability of the three hC2 components: COMMAND, PATROL and

DISMOUNT. hC2 Tactical Communications provides networked COMMAND and control and shared situational awareness, allowing for information exchange across echelons. hC2 Tactical Communications is operable on limited bandwidth, high latency tactical radio data communications frequencies. hC2 also supports IP and non-IP radios and can handle different types of radios, even within the same vehicle.

3. The highest level of classification of defense articles, components, and services included in this potential sale is SECRET.

4. If a technologically advanced adversary were to obtain knowledge of the specific hardware and software elements, the information could be used to develop countermeasures that might reduce weapon system effectiveness or be used in the development of a system with similar or advanced capabilities.

5. A determination has been made that Bulgaria can provide the same degree of protection for the sensitive technology being released as the U.S. Government. This sale is necessary in furtherance of the U.S. foreign policy and national security objectives outlined in the Policy Justification.

6. All defense articles and services listed in this transmittal have been authorized for release and export to the Republic of Bulgaria.

[FR Doc. 2024–25117 Filed 10–28–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Transmittal No. 23–59]

Arms Sales Notification

AGENCY: Defense Security Cooperation Agency, Department of Defense (DoD).

ACTION: Arms sales notice.

SUMMARY: The DoD is publishing the unclassified text of an arms sales notification.

FOR FURTHER INFORMATION CONTACT:

Pamela Young at (703) 953–6092, pamela.a.young14.civ@mail.mil, or dsca.ncr.rsrcmgmt.list.cns-mbx@mail.mil.

SUPPLEMENTARY INFORMATION: This 36(b)(1) arms sales notification is published to fulfill the requirements of section 155 of Public Law 104–164 dated July 21, 1996. The following is a copy of a letter to the Speaker of the House of Representatives with attached Transmittal 23–59, Policy Justification, and Sensitivity of Technology.

Dated: October 24, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

BILLING CODE 6001–FR–P



DEFENSE SECURITY COOPERATION AGENCY
 2800 Defense Pentagon
 Washington, DC 20301-2800

August 18, 2023

The Honorable Kevin McCarthy
 Speaker of the House
 U.S. House of Representatives
 H-209, The Capitol
 Washington, DC 20515

Dear Mr. Speaker:

Pursuant to the reporting requirements of Section 36(b)(1) of the Arms Export Control Act, as amended, we are forwarding herewith Transmittal No. 23-59, concerning the Army's proposed Letter(s) of Offer and Acceptance to the Government of Australia for defense articles and services estimated to cost \$975 million. We will issue a news release to notify the public of this proposed sale upon delivery of this letter to your office.

Sincerely,

James A. Hursch
 Director

Enclosures:

1. Transmittal
2. Policy Justification
3. Sensitivity of Technology

BILLING CODE 6001-FR-C

Transmittal No. 23-59

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act, as Amended

(i) *Prospective Purchaser:* Government of Australia

(ii) *Total Estimated Value:*

Major Defense Equipment * ..	\$902 million
Other	\$ 73 million
TOTAL	\$975 million

(iii) *Description and Quantity or Quantities of Articles or Services under Consideration for Purchase:*

Major Defense Equipment (MDE):

Up to twenty-two (22) M142 High Mobility Artillery Rocket Systems (HIMARS)

Sixty (60) M30A1 Guided Multiple Launch Rocket System (GMLRS) Alternative Warhead (AW) Pods with Insensitive Munitions Propulsion System (IMPS)

Forty (40) M31A1 GMLRS Unitary (GMLRS-U) High Explosive (HE) Pods with IMPS

Sixty-six (66) M30A2 Extended Range (ER)-GMLRS AW Pods

Twenty-four (24) M31A2 ER GMLRS Unitary (HE) Pods

Non-MDE:

Also included are Reduced Range Practice Rocket (RRPR) Pods; intercom systems to support the HIMARS Launcher; M1084A2 HIMARS Re-Supply Vehicles (RSV); trailers; 9300-SL60TN Forklift, Side Loader; radio/

communication mounts; machine gun mounts; wheel guards; ruggedized laptops; training; training equipment; publications for HIMARS and its munitions and spares; services; other support equipment; and other related elements of program and logistic support.

(iv) *Military Department: Army (AT-B-UNP)*

(v) *Prior Related Cases, if any: AT-B-UMJ, AT-B-UMK, AT-B-UKI*

(vi) *Sales Commission, Fee, etc., Paid, Offered, or Agreed to be Paid: None known at this time*

(vii) *Sensitivity of Technology Contained in the Defense Article or Defense Services Proposed to be Sold: See Attached Annex*

(viii) *Date Report Delivered to Congress: August 18, 2023*

* As defined in Section 47(6) of the Arms Export Control Act.

Policy Justification

Australia—M142 High Mobility Artillery Rocket Systems (HIMARS)

The Government of Australia has requested to buy up to twenty-two (22) M142 High Mobility Artillery Rocket Systems (HIMARS); sixty (60) M30A1 Guided Multiple Launch Rocket System (GMLRS) Alternative Warhead (AW) Pods with Insensitive Munitions Propulsion System (IMPS); forty (40) M31A1 GMLRS Unitary (GMLRS-U) High Explosive (HE) Pods with IMPS; sixty-six (66) M30A2 Extended Range (ER)-GMLRS AW Pods; and twenty-four (24) M31A2 ER GMLRS Unitary (HE) Pods. Also included are Reduced Range Practice Rocket (RRPR) Pods; intercom systems to support the HIMARS Launcher; M1084A2 HIMARS Re-Supply Vehicles (RSV); trailers; 9300-SL60TN Forklift, Side Loader; radio/communication mounts; machine gun mounts; wheel guards; ruggedized laptops; training; training equipment; publications for HIMARS and its munitions, and spares; services; other support equipment; and other related elements of program and logistic support. The estimated total program cost is \$975 million.

This proposed sale will support the foreign policy and national security objectives of the United States. Australia is one of our most important allies in the Western Pacific. The strategic location of this political and economic power contributes significantly to ensuring peace and economic stability in the region. It is vital to the U.S. national interest to assist our ally in developing and maintaining a strong and ready self-defense capability.

The proposed sale will improve Australia's capability to meet current

and future threats and will enhance interoperability with U.S. forces and other allied forces. Australia will use the capability to strengthen its homeland defense and provide greater security for its critical infrastructure. Australia will have no difficulty absorbing this equipment into its armed forces.

The proposed sale of this equipment and support will not alter the basic military balance in the region.

The principal contractors will be Lockheed Martin, Grand Prairie, TX; L3Harris Corporation, Melbourne, FL; Leonardo DRS, Arlington, VA; and Oshkosh Corporation, Stafford, VA. There are no known offset agreements in connection with this potential sale.

Implementation of this proposed sale will not require the assignment of U.S. Government or contractor representatives to Australia.

There will be no adverse impact on U.S. defense readiness as a result of this proposed sale.

Transmittal No. 23-59

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act

Annex

Item No. vii

(vii) Sensitivity of Technology:

1. The M142 High Mobility Artillery Rocket System (HIMARS) is a wheeled launcher mounted on a 5-ton Family of Medium Tactical Vehicles truck chassis and is transportable by C-130. HIMARS is the modern Army-fielded version of the Multiple Launch Rocket System (MLRS) M270 launcher and can fire all the MLRS Family of Munitions (FOM), including Guided Multiple Launch Rocket System (GMLRS) variants and the Army Tactical Missile System (ATACMS). Utilizing the MLRS FOM, the HIMARS can engage targets between 15 and 300 kilometers with GPS-aided precision accuracy.

2. The Guided Multiple Launch Rocket System (GMLRS) M31A2 Unitary is the Army's primary munition for units fielding the M142 HIMARS and M270A1 Multiple Launcher Rocket System (MLRS) Launchers. The M31 Unitary is a solid propellant artillery rocket that uses Global Positioning System/Precise Positioning Service (GPS/PPS)-aided inertial guidance to deliver a single high-explosive blast fragmentation warhead accurately and quickly to targets at ranges from 15-70 kilometers. The rockets are fired from a launch pod container that also serves as the storage and transportation container for the rockets. Each rocket pod holds six (6) total rockets.

3. The M30A2 GMLRS Alternative Warhead shares a greater than 90% commonality with the M31A1 Unitary. The primary difference between the GMLRS-U and GMLRS-AW is the replacement of the Unitary's high explosive warhead with a 200-pound fragmentation warhead of pre-formed tungsten penetrators which is optimized for effectiveness against large area and imprecisely located targets. The munitions otherwise share a common motor, GPS/PPS-aided inertial guidance and control system, fusing mechanism, multi-option height of burst capability, and effective range of 15-70km.

4. The Extended Range (ER) GMLRS provides a persistent, responsive, all-weather, rapidly deployed, long-range, surface-to-surface, area- and point-precision strike capability. The XM403 Alternative Warhead (AW) carries a 200-pound fragmentation assembly filled with high explosives which, upon detonation, accelerates two layers of preformed penetrators optimized for effectiveness against large area and imprecisely located targets. The XM404 Unitary variant is a 200-pound class unitary with a steel blast-fragmentation case, designed for low collateral damage against point targets. The ER GMLRS maintains the accuracy and effectiveness demonstrated by the baseline GMLRS out to a maximum range of 150 km while also including a new Height of Burst (HOB) capability.

5. The highest level of classification of defense articles, components, and services included in this potential sale is SECRET.

6. If a technologically advanced adversary were to obtain knowledge of the specific hardware and software elements, the information could be used to develop countermeasures that might reduce weapon system effectiveness or be used in the development of a system with similar or advanced capabilities.

7. A determination has been made that Australia can provide the same degree of protection for the sensitive technology being released as the U.S. Government. This sale is necessary in furtherance of the U.S. foreign policy and national security objectives outlined in the Policy Justification.

8. All defense articles and services listed in this transmittal are authorized for release and export to Australia.

[FR Doc. 2024-25115 Filed 10-28-24; 8:45 am]

BILLING CODE 6001-FR-P

DEPARTMENT OF DEFENSE**Office of the Secretary****[Docket ID: DoD–2024–OS–0111]****Privacy Act of 1974; System of Records****AGENCY:** Department of Defense (DoD).**ACTION:** Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Office of the Secretary is establishing a new system of records titled, “Catch a Serial Offender (CATCH) Program Records,” DoD–0024. This system of records covers DoD’s maintenance of records used to collect and compare adult sexual assault reports for the purpose of identifying alleged serial sexual assault offenders. Additionally, DoD is issuing a notice of proposed rulemaking, which proposes to exempt this system of records from certain provisions of the Privacy Act, elsewhere in this issue of the **Federal Register**.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before November 29, 2024. The Routine Uses listed in this document are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* *Federal Rulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for submitting comments.

* *Mail:* Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 05F16, Alexandria, VA 22350–1700.

Instructions: All submissions received must include the agency name and docket number for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Rahwa Keleta, Privacy and Civil Liberties Directorate, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 05F16, Alexandria, VA 22350–

1700; OSD.DPCLTD@mail.mil; (703) 256–1408.

SUPPLEMENTARY INFORMATION:**I. Background**

Section 543 of the Carl Levin and Howard P. “Buck” McKeon National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2015 (Pub. L. 113–291) required the Secretary of Defense to develop a plan that would allow a restricted reporting adult victim of sexual assault to disclose suspect or incident information for the purpose of identifying serial offenders. In response to this requirement, the Naval Criminal Investigative Service (NCIS) developed a database to catalogue and centralize all victim entries into the CATCH program. The eligibility for the CATCH was later extended beyond just Restricted Reporters. The details in submitted CATCH entries are compared against reported subjects in adult sexual assault investigations and other CATCH Program entries. The sexual assault investigation records used for comparison include investigative reports prepared by DoD law enforcement, or other Federal, State, local, Tribal, or foreign law enforcement or investigative bodies, if such records exist. Entries in the CATCH system will consist of information voluntarily submitted into the CATCH system by eligible victims without identifying such victims, through established CATCH processes. At the present time, the CATCH Program gives adult sexual assault victims who filed (1) Restricted Reports, (2) certain Unrestricted Reports where the name of the suspect is not reported to or uncovered by law enforcement, or (3) no official report with the Sexual Assault Prevention and Response (SAPR) program, an opportunity to submit suspect information (without identifying the victim) into the CATCH system after receiving a user name and password from a Sexual Assault Response Coordinator (SARC) or Family Advocacy Program (FAP) representative. There is no self-service feature for CATCH entries; victims must go through a SARC or FAP representative, so they are apprised of their victim’s rights and the CATCH Program is fully explained. The Military Criminal Investigative Organizations (MCIOs) specially assigned to CATCH Headquarters, not at the victim’s installation, analyze suspect information in victim entries submitted into the CATCH Program. If a match is identified, the investigators will notify SAPR or FAP personnel of the match; the CATCH system protects the identity of the victim by not maintaining

information that identifies the victim. The victim’s contact information is stored in a separate database, the Defense Sexual Assault Incident Database (DSAID) File Locker or FAP case management system, which is only accessible to certain SAPR and FAP personnel, not MCIOs. Moreover, section 550 of Public Law 116–92 (National Defense Authorization Act for Fiscal Year 2020) contained additional protections specifically for Restricted Reporters to safeguard the restricted nature of their reports, notwithstanding a victim disclosure made pursuant to the CATCH program. More information about the CATCH Program may be found at the U.S. Department of Defense Sexual Assault Prevention and Response Organization website at <https://www.sapr.mil/catch>. Additionally, DoD is issuing a notice of proposed rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in this issue of the **Federal Register**. DoD system of records notices (SORNs) have been published in the **Federal Register** and are available from the address in **FOR FURTHER INFORMATION CONTACT** or on the Privacy and Civil Liberties Directorate website at <https://dpcl.d.defense.gov>.

II. Privacy Act

Under the Privacy Act, a “system of records” is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A–108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: October 23, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER:

Catch a Serial Offender (CATCH) Program Records, DoD–0024.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301–1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified

cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER(S):

Director, Naval Criminal Investigative Service (NCIS), 27130 Telegraph Road, Quantico, VA 22134-2253, *CATCH@NCIS.NAVY.MIL*.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

10 U.S.C. 932, Art. 132 Retaliation; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1044e, Special Victim's Counsel For Victims Sex-Related Offenses; 10 U.S.C. 1561, Complaints of Sexual Harassment: Investigation by Commanding Officers; 10 U.S.C. 1565b, Victims Of Sexual Assault: Access To Legal Assistance and Services of Sexual Assault Response Coordinators and Sexual Assault Victim Advocates; section 543 of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113-291) DoD Instruction 5505.18, Investigation of Adult Sexual Assault in the Department of Defense; DoD Directive 6495.01, "Sexual Assault Prevention and Response (SAPR) Program; section 550 of Public Law 116-92 (National Defense Authorization Act for Fiscal Year 2020); and E.O. 9397 (Social Security number), as amended.

PURPOSE(S) OF THE SYSTEM:

The system will collect adult sexual assault victims' CATCH entries about alleged perpetrators, without identifying victims, for the purpose of comparison against other CATCH entries and against law enforcement investigative records of adult sexual assaults to identify serial sexual assault offenders. Pursuant to section 550 of Public Law 116-92 (National Defense Authorization Act for Fiscal Year 2020), a victim's disclosure made pursuant to the CATCH program will not operate to terminate a restricted report's status as restricted. Unless a victim expressly decides to participate in an investigation after being notified of a match, the information in a victim's entry in the CATCH system will not be used to initiate an investigation, regardless of the type of victim report (Restricted Reporters, certain Unrestricted Reporters, and victims who filed no report of sexual assault.)

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals named as alleged sexual assault perpetrators by victims eligible to provide information for the CATCH program ("eligible victims"). Such alleged perpetrators include current, former, and retired Active Duty and

Reserve military personnel, DoD civilian personnel, contractors, and members of the public accused of sexual assault by an eligible victim.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system include:

A. Personal Information about individuals named as alleged perpetrators in sexual assault incidents by eligible victims, such as: name and aliases, Social Security number (SSN), date of birth, physical, mailing, and email addresses, phone numbers, place of birth, race/ethnicity, biometric data including photographs, vehicle information, marital status, gender/gender identification, other biographical data, and other information about alleged perpetrators provided by eligible victims.

B. Employment Information such as: position/title, rank/grade, duty station, branch of service, work address, and email address.

C. Case numbers of other investigations associated with alleged perpetrators for purposes of reference.

D. Information about alleged perpetrators obtained by MCIOs from other sources (such as DoD databases; other Federal, State, local, Tribal, or foreign law enforcement databases; or open-source databases) for purposes of validating or confirming information about alleged perpetrators provided by eligible victims or further identifying such alleged perpetrators.

RECORD SOURCE CATEGORIES:

Records and information stored in this system of records are obtained from: the victim, DoD systems of records/databases maintaining personnel information, investigative reports, public records and other publicly available sources, commercial data aggregators, subjects of investigation, witnesses, and law enforcement entities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a Routine Use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, Tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

* Note 1. Given the sensitive nature of records in this system, appropriate discretion and care must be exercised in the extent of disclosure of information under this routine use.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

* Note 2. Given the sensitive nature of records in this system, appropriate discretion and care must be exercised in the extent of disclosure of information under this routine use.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency

or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State, or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act of 1987, as amended.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

K. When an originating record is maintained by the U.S. Department of Defense, records may be disclosed, as authorized, to the U.S. Department of Homeland Security, including the U.S. Coast Guard, for purposes of investigation, verification, or notification by the CATCH investigative program when a reported sexual assault incident allegedly involves a current or former Service member of, or civilian employed by or affiliated with the U.S. Coast Guard.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records about alleged perpetrators may be retrieved by a unique victim reference number (VRN) maintained in the CATCH system apart from any other identifying victim information or by Defense Sexual Assault Incident Database (DSAID) control number maintained in the CATCH system apart from any other identifying victim information. The CATCH entries do not identify the victim and CATCH system information may not be aggregated to identify a victim. Victim identity and victim contact information is found in DSAID, a separate system maintained and operated by the DoD Sexual Assault Prevention and Response Office.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

CATCH Program records are maintained in this system for a period of 10 years and destroyed.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES:

Individuals seeking access to their records may follow the procedures in 32 CFR part 310. Individuals may address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, and email address of the individual. In addition, the requester must provide

either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

Requesters should be aware that DoD has claimed an exemption from first-party access pursuant to (j)(2) of the Privacy Act, 5 U.S.C. 552a(j)(2) and that Congress has provided for an exemption from disclosure under the Freedom of Information Act pursuant to section 550 of Public Law 116-92 (National Defense Authorization Act for Fiscal Year 2020).

CONTESTING RECORD PROCEDURES:

Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES:

Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), and (I), (5), and (8); (f), and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2), as applicable. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), and (c), and published in 32 CFR part 310. In addition, when exempt records received from other systems of records become part of this system, the DoD also claims the same exemptions for those records that are claimed for the prior system(s) of records from which they are a part and claims any additional exemptions set forth here.

HISTORY:

None.

[FR Doc. 2024-25034 Filed 10-28-24; 8:45 am]

BILLING CODE 6001-FR-P

DEPARTMENT OF DEFENSE**Office of the Secretary**

[Transmittal No. 23-48]

Arms Sales Notification**AGENCY:** Defense Security Cooperation Agency, Department of Defense (DoD).**ACTION:** Arms sales notice.**SUMMARY:** The DoD is publishing the unclassified text of an arms sales notification.**FOR FURTHER INFORMATION CONTACT:**Pamela Young at (703) 953-6092, pamela.a.young14.civ@mail.mil, or dsca.ncr.rsrcmgmt.list.cns-mbx@mail.mil.**SUPPLEMENTARY INFORMATION:** This 36(b)(1) arms sales notification is published to fulfill the requirements of

section 155 of Public Law 104-164 dated July 21, 1996. The following is a copy of a letter to the Speaker of the House of Representatives with attached Transmittal 23-48, Policy Justification, and Sensitivity of Technology.

Dated: October 24, 2024.

Aaron T. Siegel,*Alternate OSD Federal Register Liaison Officer, Department of Defense.***BILLING CODE 6001-FR-P****DEFENSE SECURITY COOPERATION AGENCY**2800 DEFENSE PENTAGON
WASHINGTON, DC 20301-2800

August 21, 2023

The Honorable Kevin McCarthy
Speaker of the House
U.S. House of Representatives
H-209, The Capitol
Washington, DC 20515

Dear Mr. Speaker:

Pursuant to the reporting requirements of Section 36(b)(1) of the Arms Export Control Act, as amended, we are forwarding herewith Transmittal No. 23-48, concerning the Army's proposed Letter(s) of Offer and Acceptance to the Government of Poland for defense articles and services estimated to cost \$12.0 billion. We will issue a news release to notify the public of this proposed sale upon delivery of this letter to your office.

Sincerely,

A handwritten signature in black ink, appearing to read "J. Hursch".

James A. Hursch
Director

Enclosures:

1. Transmittal
2. Policy Justification
3. Sensitivity of Technology

BILLING CODE 6001-FR-P

Transmittal No. 23-48

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act, as amended

(i) *Prospective Purchaser*: Government of Poland

(ii) *Total Estimated Value*:

Major Defense Equipment * ..	\$ 7.5 billion
Other	\$ 4.5 billion

TOTAL	\$12.0 billion

Funding Source: National Funds

(iii) *Description and Quantity or Quantities of Articles or Services under Consideration for Purchase*:

Major Defense Equipment (MDE):

Ninety-six (96) AH-64E Apache Attack Helicopters

Two hundred ten (210) T700-GE 701D Engines (192 installed, 18 spares)

Ninety-seven (97) AN/ASQ-170

Modernized Target Acquisition and

Designation Sight/AN/AAR-11

Modernized Pilot Night Vision

Sensors (M-TADS/PNVS) (96

installed, 1 spare)

Thirty-seven (37) AN/APG-78 Fire Control Radars (FCR) Mast Mounted Assembly (MMA) (36 installed, 1 spare)

Thirty-seven (37) Longbow Fire Control Radar (FCR) Radar Electronic Units (REU), (36 installed, 1 spare)

Ninety-six (96) AN/APR-48B

Modernized Radar Frequency

Interferometers (MRFI)

One hundred two (102) AN/AAR-57 Common Missile Warning Systems (CMWS) (96 installed, 6 spares)

Two hundred four (204) AN/ARC-231A, with RT-1987 Receivers Transmitters, Very High Frequency/Ultra High Frequency (VHF/UHF) Radios (192 installed, 12 spares)

One thousand eight hundred forty-four

(1,844) AGM-114R2 Hellfire Missiles

Ninety-six (96) M36E8 Hellfire Captive Air Training Missiles (CATM)

Four hundred sixty (460) AGM-179A Joint Air-to-Ground Missiles (JAGM)

Five hundred eight (508) Stinger 92K Block I Missiles

Seven thousand six hundred fifty (7,650) WGU-59/B Advanced Precision Kill Weapon System II (APKWS-II) Guidance Sections (GS)

Non-MDE:

Also included are Radar Signal Detecting Sets; Laser Detecting Sets; Identification Friend or Foe (IFF) transponders; Improved Data Modems; Small Tactical Terminals; Improved Countermeasure Dispensing Systems (ICMD); Automatic Direction Finders; Doppler Radar Velocity Sensors; Radar Altimeter Common Cores (RACC); Tactical Air Navigation Set (TACAN);

Global Positioning System (GPS) receivers; Simple Key Loader; Advanced Weapon System Automatic Machine Guns; rocket launchers; missile launchers; rockets; ammunition; Manned-Unmanned Teaming (MUMT) Unmanned Aerial System (UAS) Receiver; MUMT Air-Air-Ground kits; training devices; communication systems; helmets; simulators; generators; aircrew survivability equipment; transportation and organization equipment; spare and repair parts; support equipment; tools and test equipment; technical data and publications; personnel training and training equipment; U.S. Government and contractor technical assistance; technical and logistics support services; and other related elements of program and logistical support.

(iv) *Military Department*: Army (PL-B-UEH)

(v) *Prior Related Cases, if any*: None

(vi) *Sales Commission, Fee, etc., Paid, Offered, or Agreed to be Paid*: None

(vii) *Sensitivity of Technology Contained in the Defense Article or Defense Services Proposed to be Sold*: See Attached Annex

(viii) *Date Report Delivered to Congress*: August 21, 2023

* As defined in Section 47(6) of the Arms Export Control Act.

POLICY JUSTIFICATION

Poland—AH-64E Apache Helicopters

The Government of Poland has requested to buy ninety-six (96) AH-64E Apache Attack Helicopters; two hundred ten (210) T700-GE 701D engines (192 installed, 18 spares); ninety-seven (97) AN/ASQ-170 Modernized Target Acquisition and Designation Sight/AN/AAR-11 Modernized Pilot Night Vision Sensors (M-TADS/PNVS) (96 installed, 1 spare); thirty-seven (37) AN/APG-78 Fire Control Radars (FCR) Mast Mounted Assembly (MMA) (36 installed, 1 spare); thirty-seven (37) Longbow Fire Control Radar (FCR) Radar Electronic Units (REU), (36 installed, 1 spare); ninety-six (96) AN/APR-48B Modernized Radar Frequency Interferometers (MRFI); one hundred two (102) AN/AAR-57 Common Missile Warning Systems (CMWS) (96 installed, 6 spares); two hundred four (204) AN/ARC-231A, with RT-1987 Receiver Transmitters, Very High Frequency/Ultra High Frequency (VHF/UHF) radios (192 installed, 12 spares); one thousand eight hundred forty-four (1,844) AGM-114R2 Hellfire Missiles; ninety-six (96) M36E8 Hellfire Captive Air Training Missiles (CATM); four hundred sixty (460) AGM-179A Joint Air-to-Ground

Missiles (JAGM); five hundred eight (508) Stinger 92K Block I Missiles; and seven thousand six hundred fifty (7,650) WGU-59/B Advanced Precision Kill Weapon System II (APKWS-II) Guidance Sections (GS). Also included are Radar Signal Detecting Sets; Laser Detecting Sets; Identification Friend or Foe (IFF) transponders; Improved Data Modems; Small Tactical Terminals; Improved Countermeasure Dispensing Systems (ICMD); Automatic Direction Finders; Doppler Radar Velocity Sensors; Radar Altimeter Common Cores (RACC); Tactical Air Navigation Set (TACAN); Global Positioning System (GPS) receivers; Simple Key Loader; Advanced Weapon System Automatic Machine Guns; rocket launchers; missile launchers; rockets; ammunition; Manned-Unmanned Teaming (MUMT) Unmanned Aerial System (UAS) Receiver; MUMT Air-Air-Ground kits; training devices; communication systems; helmets; simulators; generators; aircrew survivability equipment; transportation and organization equipment; spare and repair parts; support equipment; tools and test equipment; technical data and publications; personnel training and training equipment; U.S. Government and contractor technical assistance; technical and logistics support services; and other related elements of program and logistical support. The estimated total cost is \$12.0 billion.

This proposed sale will support the foreign policy goals and national security objectives of the United States by improving the security of a North Atlantic Treaty Organization (NATO) Ally that is a force for political stability and economic progress in Europe.

The proposed sale will improve Poland's capability to meet current and future threats by providing a credible force that is capable of deterring adversaries and participating in NATO operations. Poland will have no difficulty absorbing this equipment into its armed forces.

The proposed sale of this equipment and support will not alter the basic military balance in the region.

The principal contractors will be Boeing, Mesa, AZ, and Lockheed Martin, Orlando, FL. The purchaser has requested offsets. Any offset agreement will be defined in negotiations between the purchaser and the contractor(s).

Implementation of this proposed sale will require temporary duty travel of five to eight U.S. Government and contractor representatives to Poland for a duration of up to five years to support equipment fielding and training.

There will be no adverse impact on U.S. defense readiness as a result of this proposed sale.

Transmittal No. 23–48

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act

Annex

Item No. vii

(vii) *Sensitivity of Technology:*

1. The AH–64E Apache Attack Helicopter is the Army's advanced attack helicopter, equipped for performing close air support, anti-armor, and armed reconnaissance missions. The aircraft contains the following communications and target identification equipment, navigation equipment, aircraft survivability equipment, displays, and sensors:

a. The AN/ARC–231A (RT 1987) Very High Frequency/Ultra High Frequency (VHF/UHF) radio is a multi-mode software-defined radio providing line of sight VHF/UHF secure and non-secure voice and data communications in the 30.000–941.000 MHz frequency range and Satellite Communications (SATCOM) beyond line of sight secure and non-secure voice and data, including Demand Assigned Multiple ACCESS (DAMA) communications in the 240–320 MHz frequency range on manned and unmanned aviation platforms. ARC–231A (RT 1987) includes improved Type-1 cryptographic algorithm and processing capabilities, Civil Land Mobile Radio, Single Channel Ground and Airborne Radios System (SINCGARS) capabilities, HAVE QUICK (HQ), Second Generation Anti-Jam Tactical UHF Radio for NATO (SATURN) waveform, 8.33 kHz channel spacing for Global Air-Traffic Management (GATM) compliance, and capability for Mobile User Objective System (MUOS) waveform through possible future hardware and software updates.

b. The AN/APX–123A Identification Friend-or-Foe (IFF) digital transponder set provides pertinent platform information in response to an IFF interrogator. The digital transponder provides cooperative Mark XII IFF capability using full diversity selection, as well as Mode Select (Mode S) capability. In addition, the transponder is capable of interfacing with the aircraft's Traffic Collision and Avoidance System (TCAS). The transponder receives pulsed radio frequency interrogation signals in any of six modes (1, 2, 3/A, S, and 5), decodes the signals, and transmits a pulsed reply. The Mark XII IFF operation includes Selective Identification Feature

(SIF) Modes 1, 2, 3/A and C, as well as secure cryptographic Mode 5 operational capability.

c. Link 16 Datalink is a military tactical data link network. Link 16 provides aircrews with enhanced situational awareness and the ability to exchange target information to Command and Control (C2) assets via Tactical Digital Information Link-Joint (TADIL-J). Link 16 can provide a range of combat information in near-real time to U.S. and allied combat aircraft and C2 centers. The AH–64E uses the Harris Small Tactical Terminal (STT) KOR–24A to provide Airborne and Maritime/Fixed Station (AMF) Small Airborne Link 16 Terminal (SALT) capability. The STT is the latest generation of small, two-channel, Link 16 and VHF/UHF radio terminals. While in flight, the STT provides simultaneous communication, voice or data, on two key waveforms.

d. The AN/APR–39 Radar Warning Receiver Signal Detecting Set is a system that provides warning of a radar-directed air defense threat and allows for the employment of appropriate countermeasures. This is the 1553 data bus compatible configuration.

e. The AN/AVR–2B Laser Warning Set is a passive laser warning system that receives, processes, and displays threat information on the aircraft's multi-functional display when the system detects lasers illuminating the aircraft.

f. The AAR–57 Common Missile Warning System (CMWS) detects energy emitted by threat missiles in-flight, evaluates potential false alarm emitters in the environment, declares validity of threats, and selects appropriate countermeasures for defeat. The CMWS consists of an Electronic Control Unit (ECU), Electro-Optic Missile Sensors (EOMSs), and Sequencer and Improved Countermeasures Dispenser (ICMD).

g. The AH–64E uses two EAGLE+MMR Embedded Global Positioning System (GPS)/Inertial Navigation Systems (INS) (EGI) with Multi-Mode Receiver. The EAGLE+MMR is a self-contained, all-attitude navigation system with an embedded GPS receiver controlled via MIL–STD–1553B controller and provides output navigation and GPS timing data to support ADS–B out and other platform systems. The EAGLE's EGI unit houses a 24 channel GPS receiver capable of operating in either Standard Positioning Service (SPS) C/A-code (non-encrypted) or Precise Positioning Service (PPS) Y-code (encrypted).

h. The AN/ASQ–170 Modernized Target Acquisition and Designation Sight/AN/AAQ–11 Pilot Night Vision

Sensor (MTADS/PNVS) provides day, night, and limited adverse weather target information, as well as night navigation capabilities. The PNVS provides thermal imaging that permits nap-of-the-earth flight to, from, and within the battle area, while MTADS provides the copilot gunner with search, detection, recognition, and designation capabilities by means of Direct View Optics (DVO), television, and Forward Looking Infrared (FLIR) sighting systems that may be used singularly or in combinations.

i. The AN/APR–48B Modernized Radar Frequency Interferometer (M–RFI) is an updated version of the passive radar detection and direction-finding system. It utilizes a detachable User Data Module (UDM) on the M–RFI processor, which contains the Radar Frequency (RF) threat library.

j. The AN/APG–78 Longbow Fire Control Radar (FCR) with Radar Electronics Unit (REU) is an active, low-probability-of-intercept, millimeter wave radar. The active radar is combined with a passive Radar Frequency Interferometer (RFI) mounted on top of the helicopter mast. The FCR Ground Targeting Mode detects, locates, classifies, and prioritizes stationary or moving armored vehicles, tanks, and mobile air defense systems, as well as hovering helicopters and helicopters and fixed-wing aircraft in normal flight. If desired, the radar data can be used to refer targets to the regular electro-optical Modernized Target Acquisition and Designation Sight (MTADS).

k. The Manned-Unmanned Teaming X (MUMT–X) data link system provides cross-platform communication and teaming between Apache, unmanned aerial systems (UAS), and other interoperable aircraft and ground platforms. It provides the ability to display real-time UAS sensor information and MTADS full motion video feeds across MUMT-equipped platforms and ground stations.

l. The M299 Missile Launcher, commonly known as the Longbow Hellfire Launcher (LBHL), is a four-rail launcher designed to carry the complete family of AGM–114 Hellfire Missiles.

m. The AGM–114R Hellfire is a semi-active laser guided missile with a multi-purpose warhead that can engage and defeat both high and heavily armored targets, personnel, bunkers, caves, and urban structures.

n. The JAGM–179A is an Air-to-Ground Missile (AGM) consisting of the Hellfire Romeo (AGM–114R) back-end (*i.e.*, propulsion, warhead, and control sections) mated to a newly designed dual-mode guidance section (GS). The dual-mode GS is a combination of

Millimeter Wave (MMW) and Semi-Active Laser (SAL) sensors co-axially aligned on a steerable gimbal. The combination of MMW and SAL sensors provide improved Precision Point (PP) and Fire-and-Forget (FF) capabilities in a single munition. This combination allows for targeting of fast moving and stationary targets in countermeasure and intensive battlefield environments, and in low cloud ceiling and adverse weather. Firing modes include Lock-On Before Launch (LOBL) and Lock-On After Launch (LOAL). Engagement modes include Point Designation (PD)—SAL only, Target Designation (PD)—SAL initiated with MMW engagement completion, Active Fire & Forget/Laser Queuing (AFF-LQ)—MMW initiated with SAL override capability, and Active Fire & Forget (AFF)—MMW only. Hosting platforms include select rotary-wing and fixed-wing aircraft, wheeled or tracked vehicles, ground-based pedestal launchers, and patrol boats. Targets include tactical armor, boats, bunkers, buildings, caves, personnel in the open, rotary-wing and slow fixed-wing aircraft, UAS, and fast-moving non-tactical vehicles. The MMW is capable of hitting low radar cross section targets.

o. The Hellfire M36E9 Captive Air Training Missile (CATM) is a flight-training missile that consists of a functional guidance section coupled to an inert missile bus. It functions like a tactical missile during captive carry on the aircraft, absent launch capability, making it suitable for training the

aircrew in simulated Hellfire Missile target acquisition and lock.

p. The M261 2.75 Inch Rocket Launcher is a nineteen tube, three zone rocket launcher utilized on heavy attack aircraft. It fires the Hydra 70 2.75-inch rocket, an unguided, fin-stabilized air-to-ground rocket that can utilize a variety of warhead and fuze combinations to achieve a range of effects.

q. The AGR-20A Advanced Precision Kill Weapons System (APWKS) is a conversion of the 2.75-inch Hydra 70 rocket which adds a laser guidance kit to enable precision targeting.

2. The highest level of classification of defense articles, components, and services included in this potential sale is SECRET.

3. If a technologically advanced adversary were to obtain knowledge of the specific hardware and software elements, the information could be used to develop countermeasures that might reduce weapon system effectiveness or be used in the development of a system with similar or advanced capabilities.

4. A determination has been made that Poland can provide substantially the same degree of protection for the sensitive technology being released as the U.S. Government. This sale is necessary in furtherance of the U.S. foreign policy and national security objectives outlined in the Policy Justification.

5. All defense articles and services listed in this transmittal have been

authorized for release and export to Poland.

[FR Doc. 2024-25114 Filed 10-28-24; 8:45 am]

BILLING CODE 6001-FR-P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Transmittal No. 23-60]

Arms Sales Notification

AGENCY: Defense Security Cooperation Agency, Department of Defense (DoD).

ACTION: Arms sales notice.

SUMMARY: The DoD is publishing the unclassified text of an arms sales notification.

FOR FURTHER INFORMATION CONTACT:

Pamela Young at (703) 953-6092, pamela.a.young14.civ@mail.mil, or dsca.ncr.rsrcmgmt.list.cns-mbx@mail.mil.

SUPPLEMENTARY INFORMATION: This 36(b)(1) arms sales notification is published to fulfill the requirements of section 155 of Public Law 104-164 dated July 21, 1996. The following is a copy of a letter to the Speaker of the House of Representatives with attached Transmittal 23-60, Policy Justification, and Sensitivity of Technology.

Dated: October 24, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

BILLING CODE 6001-FR-P



DEFENSE SECURITY COOPERATION AGENCY
 2800 DEFENSE PENTAGON
 WASHINGTON, DC 20301-2800

August 28, 2023

The Honorable Kevin McCarthy
 Speaker of the House
 U.S. House of Representatives
 H-209, The Capitol
 Washington, DC 20515

Dear Mr. Speaker:

Pursuant to the reporting requirements of Section 36(b)(1) of the Arms Export Control Act, as amended, we are forwarding herewith Transmittal No. 23-60, concerning the Air Force's proposed Letter(s) of Offer and Acceptance to the Government of Japan for defense articles and services estimated to cost \$104 million. We will issue a news release to notify the public of this proposed sale upon delivery of this letter to your office.

Sincerely,

James A. Hursch
 Director

Enclosures:

1. Transmittal
2. Policy Justification
3. Sensitivity of Technology

BILLING CODE 6001-FR-C

Transmittal No. 23-60

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act, as amended

(i) *Prospective Purchaser:* Government of Japan

(ii) *Total Estimated Value:*

Major Defense Equipment * ..	\$ 93.5 mil- lion
Other	\$ 10.5 mil- lion

TOTAL \$104.0 mil-
lion

(iii) *Description and Quantity or Quantities of Articles or Services under Consideration for Purchase:*

Major Defense Equipment (MDE):
 Fifty (50) AGM-158B/B-2 Joint Air-to-Surface Standoff Missiles with Extended Range (JASSM-ER)
Non-MDE:

Also included are JASSM Anti-jam Global Positioning System Receivers (JAGR), training missiles, and missile containers; munitions support and support equipment; spare parts,

consumables, accessories, and repair/return support; integration and test support and equipment; personnel training and equipment; classified and unclassified software delivery and support; classified and unclassified publications and technical documentation; transportation support; U.S. Government and contractor engineering, technical, and logistics support services; studies and surveys; and other related elements of logistics and program support.

(iv) *Military Department:* Air Force (JA-D-YBH)

(v) *Prior Related Cases, if any:* JA–D–QES

(vi) *Sales Commission, Fee, etc., Paid, Offered, or Agreed to be Paid:* None known at this time

(vii) *Sensitivity of Technology Contained in the Defense Article or Defense Services Proposed to be Sold:* See Attached Annex

(viii) *Date Report Delivered to Congress:* August 28, 2023

* As defined in Section 47(6) of the Arms Export Control Act.

POLICY JUSTIFICATION

Japan—Joint Air-to-Surface Standoff Missiles with Extended Range (JASSM–ER)

The Government of Japan has requested to buy fifty (50) AGM–158B/B–2 Joint Air-to-Surface Standoff Missiles with Extended Range (JASSM–ER). Also included are JASSM Anti-jam Global Positioning System Receivers (JAGR), training missiles, and missile containers; munitions support and support equipment; spare parts, consumables, accessories, and repair/return support; integration and test support and equipment; personnel training and equipment; classified and unclassified software delivery and support; classified and unclassified publications and technical documentation; transportation support; U.S. Government and contractor engineering, technical, and logistics support services; studies and surveys; and other related elements of logistics and program support. The estimated total cost is \$104 million.

This proposed sale will support the foreign policy goals and national security objectives of the United States by improving the security of a major ally that is a force for political stability and economic progress in the Indo-Pacific region.

The proposed sale will improve Japan's capability to meet current and future threats by providing stand-off capability via advanced, long-range strike systems for employment on Japan Air Self-Defense Force (JASDF) fighter aircraft including but not limited to the F–15J. Japan will have no difficulty absorbing these articles and services into its armed forces.

The proposed sale of this equipment and support will not alter the basic military balance in the region.

The principal contractor will be Lockheed Martin, Orlando, FL. There are no known offset agreements proposed in connection with this potential sale.

Implementation of this proposed sale will not require the assignment of any additional U.S. Government or contractor representatives to Japan.

There will be no adverse impact on U.S. defense readiness as a result of this proposed sale.

Transmittal No. 23–60

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act

Annex

Item No. vii

(vii) *Sensitivity of Technology:*

1. The AGM–158B/B–2 Joint Air-to-Surface Standoff Missile with Extended Range (JASSM–ER) All Up Round (AUR) is a low-observable, highly survivable, subsonic cruise missile designed to penetrate next-generation air defense systems enroute to target. The JASSM–ER is designed to kill hard, medium-hardened, soft, and area-type targets. A turbo-fan engine and reconfigured fuel tanks provide added capacity. The extended range over the baseline was obtained by going from a turbo jet to a turbo-fan engine and by reconfiguring the fuel tanks for added capacity.

a. The JASSM Anti-Jam Global Positioning System (GPS) Receiver (JAGR) is an imbedded GPS receiver that resides within the AUR of the JASSM–ER missile and is programed during the AUR-build process to be country-specific. It provides GPS/Inertial Navigation System (INS)-protected GPS null steering antenna systems that can minimize or eliminate undesirable interference, jamming signals, or noise during midcourse guidance.

b. The AGM–158B–2 system capabilities include all the capabilities of the AGM–158B. The AGM–158B–2 configuration will have different internal components to address multiple obsolescence issues as well as subcomponent updates to position for M-Code and other potential upgrades.

2. The highest level of classification of defense articles, components, and services included in this potential sale is SECRET.

3. If a technologically advanced adversary were to obtain knowledge of the specific hardware and software elements, the information could be used to develop countermeasures that might reduce weapon system effectiveness or be used in the development of a system with similar or advanced capabilities.

4. A determination has been made that Japan can provide substantially the same degree of protection for the sensitive technology being released as the U.S. Government. This sale is necessary in furtherance of the U.S. foreign policy and national security objectives outlined in the Policy Justification.

5. All defense articles and services listed in this transmittal have been authorized for release and export to Japan.

[FR Doc. 2024–25116 Filed 10–28–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Transmittal No. 23–25]

Arms Sales Notification

AGENCY: Defense Security Cooperation Agency, Department of Defense (DoD).

ACTION: Arms sales notice.

SUMMARY: The DoD is publishing the unclassified text of an arms sales notification.

FOR FURTHER INFORMATION CONTACT: Pamela Young at (703) 953–6092, pamela.a.young14.civ@mail.mil, or dsca.ncr.rsrcmgmt.list.cns-mbx@mail.mil.

SUPPLEMENTARY INFORMATION: This 36(b)(1) arms sales notification is published to fulfill the requirements of section 155 of Public Law 104–164 dated July 21, 1996. The following is a copy of a letter to the Speaker of the House of Representatives with attached Transmittal 23–25, Policy Justification, and Sensitivity of Technology.

Dated: October 24, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

BILLING CODE 6001–FR–P



DEFENSE SECURITY COOPERATION AGENCY
 2800 DEFENSE PENTAGON
 WASHINGTON, DC 20301-2800

August 23, 2023

The Honorable Kevin McCarthy
 Speaker of the House
 U.S. House of Representatives
 H-209, The Capitol
 Washington, DC 20515

Dear Mr. Speaker:

Pursuant to the reporting requirements of Section 36(b)(1) of the Arms Export Control Act, as amended, we are forwarding herewith Transmittal No. 23-25, concerning the Air Force's proposed Letter(s) of Offer and Acceptance to the Taipei Economic and Cultural Representative Office in the United States (TECRO) for defense articles and services estimated to cost \$500 million. We will issue a news release to notify the public of this proposed sale upon delivery of this letter to your office.

Sincerely,

James A. Hursch
 Director

Enclosures:

1. Transmittal
2. Policy Justification
3. Sensitivity of Technology

BILLING CODE 6001-FR-C

Transmittal No. 23-25

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act, as amended

(i) *Prospective Purchaser:* Taipei Economic and Cultural Representative Office in the United States (TECRO)

(ii) *Total Estimated Value:*

Major Defense Equipment * ..	\$ 0 million
Other	\$ 500 million
TOTAL	\$500 million

(iii) *Description and Quantity or Quantities of Articles or Services under Consideration for Purchase:*

Major Defense Equipment (MDE):
 None
Non-MDE:

Included are Infrared Search and Track (IRST) systems; integration and test support and equipment; aircraft and munitions support and support equipment; software delivery and support; spare parts, consumables and accessories, and repair and return support; publications and technical documentation; personnel training and training equipment; studies and

surveys; U.S. Government and contractor engineering, technical, and logistics support services; and other related elements of logistical and program support.

(iv) *Military Department: Air Force (TW-D-QBF)*

(v) *Prior Related Cases, if any: TW-D-SAD*

(vi) *Sales Commission, Fee, etc., Paid, Offered, or Agreed to be Paid: None known at this time*

(vii) *Sensitivity of Technology Contained in the Defense Article or Defense Services Proposed to be Sold: See Attached Annex*

(viii) *Date Report Delivered to Congress: August 23, 2023*

* As defined in Section 47(6) of the Arms Export Control Act.

POLICY JUSTIFICATION

Taipei Economic and Cultural Representative Office in the United States—F-16 IRST Systems

The Taipei Economic and Cultural Representative Office in the United States (TECRO) has requested to buy F-16 Infrared Search and Track (IRST) systems; integration and test support and equipment; aircraft and munitions support and support equipment; software delivery and support; spare parts, consumables and accessories, and repair and return support; publications and technical documentation; personnel training and training equipment; studies and surveys; U.S. Government and contractor engineering, technical, and logistics support services; and other related elements of logistical and program support. There is no Major Defense Equipment (MDE). The estimated total cost is \$500 million.

This proposed sale is consistent with U.S. law and policy as expressed in Public Law 96-8.

This proposed sale serves U.S. national, economic, and security interests by supporting the recipient's continuing efforts to modernize its armed forces and to maintain a credible defensive capability. The proposed sale will help improve the security of the recipient and assist in maintaining political stability, military balance, and economic progress in the region.

The proposed sale will improve the recipient's capability to meet current and future threats by contributing to the recipient's abilities to defend its airspace, provide regional security, and increase interoperability with the United States through its F-16 program. The recipient will have no difficulty absorbing this equipment into its armed forces.

The proposed sale of this equipment and support will not alter the basic military balance in the region.

The principal contractors will be Lockheed Martin Corporation, St. Louis, MO. There are no known offset agreements proposed in connection with this potential sale. The purchaser typically requests offsets. Any offset agreement would be defined in negotiations between the purchaser and the contractor(s).

Implementation of this proposed sale will not require the assignment of any additional U.S. Government or contractor representatives.

There will be no adverse impact on U.S. defense readiness as a result of this proposed sale.

Transmittal No. 23-25

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act

Annex

Item No. vii

(vii) *Sensitivity of Technology:*

1. The Infrared Search and Track System (IRST) is a high resolution, passive, infrared sensor system that searches for, detects, and tracks threats with infrared signatures at long ranges within its field of regard. It functions without emitting any radiation of its own and enables aircrews to detect adversaries before those adversaries see or sense them.

2. The highest level of classification of defense articles, components, and services included in this potential sale is SECRET.

3. If a technologically advanced adversary were to obtain knowledge of the specific hardware and software elements, the information could be used to develop countermeasures that might reduce weapon system effectiveness or be used in the development of a system with similar or advanced capabilities.

4. A determination has been made that the recipient can provide substantially the same degree of protection for the sensitive technology being released as the U.S. Government. This sale is necessary in furtherance of the U.S. foreign policy and national security objectives outlined in the Policy Justification.

5. All defense articles and services listed in this transmittal have been authorized for release and export to the recipient.

[FR Doc. 2024-25113 Filed 10-28-24; 8:45 am]

BILLING CODE 6001-FR-P

DEPARTMENT OF EDUCATION

[Docket No.: ED-2024-SCC-0132]

Agency Information Collection Activities; Comment Request; National Evaluation of the Pathways to Partnerships Program (84.421E)

AGENCY: Office of Special Education and Rehabilitative Services (OSERS), Department of Education (ED).

ACTION: Notice.

SUMMARY: In accordance with the Paperwork Reduction Act (PRA) of 1995, the Department is proposing a new information collection request (ICR).

DATES: Interested persons are invited to submit comments on or before December 30, 2024.

ADDRESSES: To access and review all the documents related to the information collection listed in this notice, please use <http://www.regulations.gov> by searching the Docket ID number ED-2024-SCC-0132. Comments submitted in response to this notice should be submitted electronically through the Federal eRulemaking Portal at <http://www.regulations.gov> by selecting the Docket ID number or via postal mail, commercial delivery, or hand delivery. If the www.regulations.gov site is not available to the public for any reason, the Department will temporarily accept comments at ICDocketMgr@ed.gov. Please include the docket ID number and the title of the information collection request when requesting documents or submitting comments. Please note that comments submitted after the comment period will not be accepted. Written requests for information or comments submitted by postal mail or delivery should be addressed to the Manager of the Strategic Collections and Clearance Governance and Strategy Division, U.S. Department of Education, 400 Maryland Ave SW, LBJ, Room 4C210, Washington, DC 20202-1200.

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Diandrea Bailey, (202) 987-0126.

SUPPLEMENTARY INFORMATION: The Department, in accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3506(c)(2)(A)), provides the general public and Federal agencies with an opportunity to comment on proposed, revised, and continuing collections of information. This helps the Department assess the impact of its information collection requirements and minimize the public's reporting burden. It also helps the public understand the

Department's information collection requirements and provide the requested data in the desired format. The Department is soliciting comments on the proposed information collection request (ICR) that is described below. The Department is especially interested in public comment addressing the following issues: (1) is this collection necessary to the proper functions of the Department; (2) will this information be processed and used in a timely manner; (3) is the estimate of burden accurate; (4) how might the Department enhance the quality, utility, and clarity of the information to be collected; and (5) how might the Department minimize the burden of this collection on the respondents, including through the use of information technology. Please note that written comments received in response to this notice will be considered public records.

Title of Collection: National Evaluation of the Pathways to Partnerships Program (84.421E).

OMB Control Number: 1820-NEW.

Type of Review: New ICR.

Respondents/Affected Public: Individuals or Households.

Total Estimated Number of Annual Responses: 17,137.

Total Estimated Number of Annual Burden Hours: 4,760.

Abstract: The U.S. Department of Education's Rehabilitation Services Administration (RSA) requests clearance for new data collection activities to support the evaluation of the 84.421E Federal fiscal year (FFY) 2023 Disability Innovation Fund (DIF), Pathways to Partnerships Innovative Model Demonstration Project. The purpose of the DIF, as provided by the Consolidated Appropriations Act, 2022 (Pub. L. 117-103), is to support innovative activities aimed at increasing competitive integrated employment as defined in section 7 of the Rehabilitation Act of 1973 (Rehabilitation Act) (29 U.S.C. 705(5)) for children, youth, and other individuals with disabilities. The program aims to create systematic and seamless approaches to offering transition services to children with disabilities, ages 10-13 and youth with disabilities ages 14 to 24 through collaborations among State vocational rehabilitation (VR) agencies, State education agencies (SEAs), local education agencies (LEAs), Federally funded Centers for Independent Living (CILs), and other organizations offering services to this population. RSA is investing a total of \$198,975,322 in grant funding to the 20 States through the FFY 2023 DIF.

This request covers primary data collection activities for the National Evaluation of the Pathways to Partnerships Program. These activities include the following:

- Surveys and interviews with program participants or their parent or guardian
- Surveys with State VR, SEA, and CIL directors
- Surveys and interviews with project staff
- Collecting project administrative data (staff rosters, cost worksheets, and web analytics) from project directors

In September 2023, RSA awarded five-year cooperative agreements for the 84.421E FFY 2023 DIF model demonstration projects. The awards provide 20 State VR agencies or SEAs with funding to implement Pathways to Partnerships model demonstration projects. The Pathways to Partnerships models vary across the 20 projects, but the projects' purpose is to create and implement systematic approaches to delivering transition services to children and youth with disabilities. The approaches must entail establishing close partnerships across key agencies to deliver these services in ways likely to improve the education and employment outcomes of children and youth with disabilities.

Dated: October 23, 2024.

Juliana Pearson,

PRA Coordinator, Strategic Collections and Clearance, Governance and Strategy Division, Office of Chief Data Officer, Office of Planning, Evaluation and Policy Development.

[FR Doc. 2024-25047 Filed 10-28-24; 8:45 am]

BILLING CODE 4000-01-P

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

Agency Information Collection Activities: Extension Without Change of an Existing Collection; Comment Request

AGENCY: Equal Employment Opportunity Commission.

ACTION: Notice of information collection; extension without change.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, the Equal Employment Opportunity Commission (EEOC or Commission) announces that it intends to submit to the Office of Management and Budget (OMB) a request for a three-year extension without change of the information collection described below.

DATES: Written comments on this notice must be submitted on or before December 30, 2024.

ADDRESSES: You may submit comments by any of the following methods; please use only one method:

Federal eRulemaking Portal: <https://www.regulations.gov>. Follow the instructions on the website for submitting comments.

Mail: Comments may be submitted by mail to Raymond Windmiller, Executive Officer, Executive Secretariat, Equal Employment Opportunity Commission, 131 M Street NE, Washington, DC 20507.

Fax: Comments totaling six or fewer pages may be sent by fax machine to (202) 663-4114. Receipt of fax transmittals will not be acknowledged, except that the sender may request confirmation of receipt by calling the Executive Secretariat staff at (202) 921-2815 (voice), (800) 669-6820 (TTY), or (844) 234-5122 (ASL Video Phone).

Instructions: All comments received will be posted without change to <https://www.regulations.gov>, including any personal information you provide. However, the EEOC reserves the right to refrain from posting libelous or otherwise inappropriate comments, including those that contain obscene, indecent, or profane language; that contain threats or defamatory statements; that contain hate speech directed at race, color, sex, national origin, age, religion, disability, or genetic information; or that promote or endorse services or products.

To read the public comments received by the EEOC, go to <https://www.regulations.gov> and search for this item. There may be a few days' delay between submission of a comment and public posting on this docket. The received comments also will be available for review on a computer in the Commission's Headquarters library, 131 M Street NE, Suite 4NW08R, Washington, DC 20507, between the hours of 9:00 a.m. and 4:30 p.m. on days the Commission is open for business. You must make an appointment with library staff to review the comments in the Commission's library by contacting 202-921-3119.

FOR FURTHER INFORMATION CONTACT:

Kathleen Oram, Assistant Legal Counsel, at (202) 921-2665 or Kathleen.Oram@eeoc.gov. Requests for this notice in an alternative format should be made to the Office of Communications and Legislative Affairs at (202) 921-3191 (voice), (800) 669-6820 (TTY), or (844) 234-5122 (ASL Video Phone).

SUPPLEMENTARY INFORMATION:

Introduction

The Equal Employment Opportunity Commission gives notice of its intent to submit the recordkeeping requirements contained in the Uniform Guidelines on Employee Selection Procedures (UGESP or Uniform Guidelines) ¹ to the Office of Management and Budget for a three-year extension without change under the Paperwork Reduction Act of 1995 (PRA).

Request for Comments

Pursuant to the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35, and OMB regulation 5 CFR 1320.8(d)(1), the EEOC invites public comments that will enable the agency to:

(1) Evaluate whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden of the collection of information, including the validity of the methodology and assumptions used;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, to be collected; e.g., permitting electronic submission of responses.

Overview of Current Information Collection

Collection Title: Recordkeeping Requirements of the Uniform Guidelines on Employee Selection Procedures, 29 CFR part 1607, 41 CFR part 60–3, 28 CFR part 50, 5 CFR part 300.

OMB Number: 3046–0017.

Type of Respondent: Businesses or other institutions; Federal Government; State or local governments and farms.

North American Industry Classification System (NAICS) Code: Multiple.

Standard Industrial Classification Code (SIC): Multiple.

Description of Affected Public: Any employer, Government contractor, labor organization, or employment agency covered by the Federal equal employment opportunity laws.

Respondents: 887,869.

Responses: 887,869.

Recordkeeping Hours: 15,422,941 per year.

Number of Forms: None.

Form Number: None.

Frequency of Report: None.

Abstract: The Uniform Guidelines provide fundamental guidance for all

Title VII-covered employers about the use of employment selection procedures. The records addressed by UGESP are used by respondents to ensure that they are complying with Title VII and Executive Order 11246; by the Federal agencies that enforce Title VII and Executive Order 11246 to investigate, conciliate, and litigate charges of employment discrimination; and by complainants to establish violations of Federal equal employment opportunity laws. While there are no data available to quantify these benefits, the collection of accurate applicant flow data enhances each employer's ability to address deficiencies in recruitment and selection processes, including detecting barriers to equal employment opportunity.

Burden Statement: There are no reporting requirements associated with UGESP. The burden being estimated is the cost of collecting and storing a job applicant's gender, race, and ethnicity data.

The only paperwork burden derives from this recordkeeping. Only employers covered under Title VII and Executive Order 11246 are subject to UGESP. However, for the purposes of burden calculation, data for all employers are counted.² The number of employers with 15 or more employees is estimated at 887,869 which combines estimates from private employment,³ the public sector,⁴ colleges and universities,⁵ apprenticeship programs,⁶ and referral unions.⁷ Employers with 15

² In calculating burden, data from multiple sources are used. Some of these sources do not allow us to identify only those employers who are covered by Title VII (employers with 15 or more employees).

³ Source of original data: U.S. Census Bureau, 2021 Statistics of U.S. Businesses (SUSB) (Dec. 2023). (<https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html>). Local Downloadable CSV data. Select U.S. & states, 6-digit NAICS. The original number of employers was adjusted to only include those with 15 or more employees.

⁴ Source of original data: 2022 Census of Governments: Employment. Individual Government Data File (<https://www.census.gov/data/datasets/2022/econ/apges/2022.html>). Local Downloadable Data zip file "Individual Unit Files". The original number of government entities was adjusted to only include those with 15 or more employees.

⁵ Source: U.S. Department of Education, National Center for Education Statistics, IPEDS, Fall 2022, Institutional Characteristics component (provisional data). See Table 1, "Number and percentage distribution of Title IV institutions, by control of institution, level of institution, and region: United States and other U.S. jurisdictions, academic year 2022–23" (<https://nces.ed.gov/ipeds/search/viewtable?tableId=35945&returnUrl=%2Fsearch>).

⁶ Source: U.S. Department of Labor, Registered Apprenticeship National Results Fiscal Year 2021, Number of active apprenticeship programs in 2021 (<https://www.dol.gov/agencies/eta/apprenticeship/about/statistics/2021>).

⁷ The EEOC has undertaken measures to enhance the agency's existing EEO–3 data frame (i.e., roster)

or more employees represent approximately 13.5% of all employers in the U.S. and employ about 86.2% of all employees in the U.S.⁸

This burden assessment is based on an estimate of the number of job applications submitted to all employers in one year, including paper-based and electronic applications. The total number of job applications submitted every year to covered employers is estimated to be 1,850,752,956 based on an average of approximately 26 applications⁹ for every hire and a Bureau of Labor Statistics data estimate of 71,046,000 annual hires.¹⁰ This figure also includes 136,806 applicants for union membership reported on the EEO–3 form for 2022.

The employer burden associated with collecting and storing applicant demographic data is based on the following assumptions: applicants would need to be asked to provide three pieces of information—sex, race/ethnicity, and an identification number (a total of approximately 13 keystrokes); the employer may need to transfer information received to a database either manually or electronically; and the employer would need to store the 13 characters of information for each applicant. Recordkeeping costs and burden are assumed to be the time cost associated with entering 13 keystrokes.

Assuming that the required recordkeeping takes 30 seconds per record, and assuming a total of 1,850,752,956 paper and electronic applications per year (as calculated above), the resulting UGESP burden hours would be 15,422,941. Based on a wage rate of \$22.94¹¹ per hour for the

of potentially eligible filers that was most recently used during the 2022 EEO–3 data collection. The number of referral unions was estimated by comparing the EEOC's 2022 EEO–3 frame to a list of active unions from the U.S. Department of Labor's Office of Labor Management Standards (OLMS) Online Public Disclosure Room (OPDR) database (<https://olmsapps.dol.gov/olpdr/>).

⁸ Source of original data: U.S. Census Bureau, 2021 Statistics of U.S. Businesses (SUSB) (Dec. 2023). (<https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html>). Local Downloadable CSV data. Select U.S. & states, 6-digit NAICS. The original number of employers was adjusted to only include those with 15 or more employees.

⁹ The average number of applicants per job opening in 2023, according to the ICIMS 2024 January Workforce Report (<https://icims.drift.click/January-2024-Workforce-Report>).

¹⁰ Bureau of Labor Statistics Job Openings and Labor Turnover Survey, 2023 annual level data (seasonally adjusted), (<http://www.bls.gov/jlt/data.htm>) is the source of the original data. The BLS figure includes new hires in both the public and the private sectors across all employer sizes.

¹¹ Burden hour cost estimates are based on the median hourly wage rate of \$22.94 for Human Resources Assistants, except payroll and timekeeping obtained from the Bureau of Labor

¹ 29 CFR, part 1607, 41 CFR part 60–3, 28 CFR part 50, 5 CFR part 300.

individuals entering the data, the collection and storage of applicant demographic data would come to approximately \$353,802,267 per year. The foregoing assumptions likely are over-inclusive because many employers have electronic job application processes that should be able to capture applicant flow data automatically.

While the burden hours and costs for the UGESP recordkeeping requirement seem large, the average burden per employer is relatively small. UGESP applies to an estimated 887,869 employers, or about 13.5% of employers in the U.S., and these employers employ about 86.2% of employees in the U.S.¹² Therefore, the estimated cost per covered employer is about \$398. Additionally, 36.4% of employees work for firms with at least 5,000 employees,¹³ for which the burden of data entry is transferred to the applicants via use of electronic application systems. Finally, UGESP allows for simplified recordkeeping for employers with more than 15 but less than 100 employees.¹⁴

For the Commission.

Dated: October 23, 2024.

Charlotte A. Burrows,
Chair.

[FR Doc. 2024–25087 Filed 10–28–24; 8:45 am]

BILLING CODE 6570–01–P

Statistics, May 2023 (see U.S. p of Labor, Bureau of Labor Statistics, Occupational Employment and Wage Statistics, <https://www.bls.gov/oes/current/oes434161.htm>).

¹² Source of original data: U.S. Census Bureau, 2021 Statistics of U.S. Businesses (SUSB) (Dec. 2023). (<https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html>). Local Downloadable CSV data. Select U.S. & states, 6-digit NAICS. The original number of employers was adjusted to only include those with 15 or more employees.

¹³ Source of original data: 2021 Economic Census. (<https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html>). Local Downloadable CSV data. Select U.S. & states, 6-digit NAICS. The original number of employers was adjusted to only include those with 15 or more employees.

¹⁴ See 29 CFR 1607.15A(1): *Simplified recordkeeping for users with less than 100 employees*. In order to minimize recordkeeping burdens on employers who employ one hundred (100) or fewer employees, and other users not required to file EEO–1, *et seq.*, reports, such users may satisfy the requirements of this section 15 if they maintain and have available records showing, for each year: (a) The number of persons hired, promoted, and terminated for each job, by sex, and where appropriate by race and national origin; (b) The number of applicants for hire and promotion by sex and where appropriate by race and national origin; and (c) The selection procedures utilized (either standardized or not standardized).

FEDERAL COMMUNICATIONS COMMISSION

[OMB 3060–0179; FR ID 257346]

Information Collection Being Reviewed by the Federal Communications Commission

AGENCY: Federal Communications Commission.

ACTION: Notice and request for comments.

SUMMARY: As part of its continuing effort to reduce paperwork burdens, and as required by the Paperwork Reduction Act of 1995 (PRA), the Federal Communications Commission (FCC or Commission) invites the general public and other Federal agencies to take this opportunity to comment on the following information collections. Comments are requested concerning: whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; the accuracy of the Commission's burden estimate; ways to enhance the quality, utility, and clarity of the information collected; ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology; and ways to further reduce the information collection burden on small business concerns with fewer than 25 employees.

The FCC may not conduct or sponsor a collection of information unless it displays a currently valid Office of Management and Budget (OMB) control number. No person shall be subject to any penalty for failing to comply with a collection of information subject to the PRA that does not display a valid OMB control number.

DATES: Written PRA comments should be submitted on or before December 30, 2024. If you anticipate that you will be submitting comments but find it difficult to do so within the period of time allowed by this notice, you should advise the contact listed below as soon as possible.

ADDRESSES: Direct all PRA comments to Cathy Williams, FCC, via email to PRA@fcc.gov and to Cathy.Williams@fcc.gov.

FOR FURTHER INFORMATION CONTACT: For additional information about the information collection, contact Cathy Williams at (202) 418–2918.

SUPPLEMENTARY INFORMATION:

OMB Control Number: 3060–0179.

Title: Section 73.1590, Equipment Performance Measurements.

Form Number: N/A.

Type of Review: Extension of a currently approved collection.

Respondents: Business or other for-profit entities; not-for-profit institutions.

Number of Respondents and Responses: 13,049 respondents and 13,049 responses.

Estimated Time per Response: 0.5–18 hours.

Frequency of Response: Recordkeeping requirement.

Total Annual Burden: 12,335 hours.

Total Annual Cost: No cost.

Obligation to Respond: Required to obtain or retain benefits. The statutory authority for this collection is contained in Section 154(i) of the Communications Act of 1934, as amended.

Needs and Uses: The information collection requirements contained in 47 CFR 73.1590(d) require licensees of AM, FM and TV stations to make audio and video equipment performance measurements for each main transmitter. These measurements and a description of the equipment and procedures used in making the measurements must be kept on file at the transmitter or remote control point for two years. In addition, this information must be made available to the FCC upon request.

Federal Communications Commission.

Marlene Dortch,

Secretary, Office of the Secretary.

[FR Doc. 2024–25102 Filed 10–28–24; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

[OMB 3060–0715, OMB 3060–0742; FR ID 257912]

Information Collections Being Submitted for Review and Approval to Office of Management and Budget

AGENCY: Federal Communications Commission.

ACTION: Notice and request for comments.

SUMMARY: As part of its continuing effort to reduce paperwork burdens, as required by the Paperwork Reduction Act (PRA) of 1995, the Federal Communications Commission (FCC or the Commission) invites the general public and other Federal Agencies to take this opportunity to comment on the following information collection. Pursuant to the Small Business Paperwork Relief Act of 2002, the FCC seeks specific comment on how it might “further reduce the information collection burden for small business

concerns with fewer than 25 employees.”

The Commission may not conduct or sponsor a collection of information unless it displays a currently valid Office of Management and Budget (OMB) control number. No person shall be subject to any penalty for failing to comply with a collection of information subject to the PRA that does not display a valid OMB control number.

DATES: Written comments and recommendations for the proposed information collection should be submitted on or before November 29, 2024.

ADDRESSES: Comments should be sent to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting “Currently under 30-day Review—Open for Public Comments” or by using the search function. Your comment must be submitted into www.reginfo.gov per the above instructions for it to be considered. In addition to submitting in www.reginfo.gov also send a copy of your comment on the proposed information collection to Nicole Ongele, FCC, via email to PRA@fcc.gov and to Nicole.Ongele@fcc.gov. Include in the comments the OMB control number as shown in the **SUPPLEMENTARY INFORMATION** below.

FOR FURTHER INFORMATION CONTACT: For additional information or copies of the information collection, contact Nicole Ongele at (202) 418–2991. To view a copy of this information collection request (ICR) submitted to OMB: (1) go to the web page <http://www.reginfo.gov/public/do/PRAMain>, (2) look for the section of the web page called “Currently Under Review,” (3) click on the downward-pointing arrow in the “Select Agency” box below the “Currently Under Review” heading, (4) select “Federal Communications Commission” from the list of agencies presented in the “Select Agency” box, (5) click the “Submit” button to the right of the “Select Agency” box, (6) when the list of FCC ICRs currently under review appears, look for the Title of this ICR and then click on the ICR Reference Number. A copy of the FCC submission to OMB will be displayed.

SUPPLEMENTARY INFORMATION: As part of its continuing effort to reduce paperwork burdens, as required by the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. 3501–3520), the FCC invited the general public and other Federal Agencies to take this opportunity to comment on the following information collection. Comments are requested concerning: (a) Whether the proposed collection of information is necessary

for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission’s burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; and (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology. Pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4), the FCC seeks specific comment on how it might “further reduce the information collection burden for small business concerns with fewer than 25 employees.”

OMB Control Number: 3060–0715.

Title: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information.

Form Number: N/A.

Type of Review: Revision of a currently approved collection.

Respondents: Business or other for-profit entities, and state, local, or tribal government.

Number of Respondents and Responses: 2,935 respondents; 91,735,200 responses.

Estimated Time per Response: 0.1–120 hours.

Frequency of Response: On occasion, annual, and one-time reporting requirements; recordkeeping; and third party disclosure requirements.

Obligation to Respond: Mandatory. Statutory authority for these collections are contained in Sections 201 and 222 of the Communications Act of 1934, as amended, 47 U.S.C. 201, 222.

Total Annual Burden: 269,534 hours.

Total Annual Cost: No Cost.

Needs and Uses: Section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222, establishes the duty of telecommunications carriers to protect the confidentiality of its customers’ proprietary information. This proprietary information includes personally identifiable information derived from a customer’s relationship with a provider of telecommunications services. This information collection implements the statutory obligations of Section 222. These regulations impose safeguards to protect Customer Proprietary Network Information (CPNI) and other customer proprietary information against unauthorized access and disclosure.

On November 16, 2023, the FCC released the *SIM Swap and Port-Out Fraud Order* (88 FR 85794 (December 8, 2023)), which adopted a baseline

framework to combat SIM swap fraud by amending section 64.2010 of the CPNI rules to add paragraph (h) on Subscriber Identity Module (SIM) changes and adds new information collection requirements in paragraphs (h)(3), (h)(5), (h)(6), and (h)(8) of that rule. A SIM swap involves the fraudulent transfer (or “swap”) of an account from a device associated with one SIM to a device associated with a different SIM, allowing a bad actor to control the victim’s mobile account and access the victim’s CPNI. The new rules establish a uniform framework that gives wireless providers flexibility to implement customer authentication and security methods to address SIM swap fraud. The *SIM Swap and Port-Out Fraud Order* modifies the existing CPNI collection requirements to require wireless providers to: (1) immediately notify customers of any requests for a SIM change associated with the customer’s account before the SIM change is completed; (2) provide customers with advance notice of any account protection measures offered; (3) maintain a clear process for customers to report SIM fraud and promptly provide customers with documentation of fraud involving their accounts; and (4) track and maintain for three years a record of SIM change requests and authentication measures used.

On December 21, 2023, the Commission released the *Data Breach Report and Order* (89 FR 9968 (February 12, 2024)), which modifies the scope of customer data and reportable breaches covered by the Commission’s rules, and also modifies the Commission’s data breach notification rules to require covered service providers to electronically notify the FCC of a reportable data breach through a link to a central reporting facility, contemporaneously with the existing obligation to notify the United States Secret Service Bureau (Secret Service) and the Federal Bureau of Investigation (FBI), and adopts equivalent requirements for Telecommunications Relay Services (TRS) providers. Covered service providers include providers of telecommunications, interconnected Voice over Internet Protocol (VoIP), and TRS. All covered providers are required to maintain a record, electronically or in some other manner, of any breaches discovered, and notifications made. Covered providers are also required to submit, via the central reporting facility, an annual reporting of certain small breaches.

OMB Control Number: 3060–0742.

Title: Sections 52.21 through 52.37, Telephone Number Portability, 47 CFR

part 52, subpart (C), and CC Docket No. 95–116.

Form Number: N/A.

Type of Review: Revision of a currently approved collection.

Respondents: Business or other for profit entities.

Number of Respondents and

Responses: 1,626 respondents; 13,672,050 responses.

Estimated Time per Response: 0.0666 hours–60 hours.

Frequency of Response: On occasion and one-time reporting requirements, recordkeeping requirement, and third party disclosure requirement.

Obligation to Respond: Required to obtain or retain benefits. Statutory authority for this information collection is contained in 47 U.S.C. 151, 152, 154(i), 201–205, 215, 251(b)(2), 251(e)(2) and 332 of the Communications Act of 1934, as amended.

Total Annual Burden: 792,235 hours.

Total Annual Cost: No cost.

Needs and Uses: Section 251(b)(2) of the Communications Act of 1934, as amended, requires LECs to “provide, to the extent technically feasible, number portability in accordance with requirements prescribed by the Commission.” Through the LNP process, consumers have the ability to retain their phone number when switching telecommunications service providers, enabling them to choose a provider that best suits their needs and enhancing competition. In the Porting Interval Order and Further Notice, the Commission mandated a one business day porting interval for simple wireline-to-wireline and intermodal port requests. The information collected in the standard local service request data fields is necessary to complete simple wireline-to-wireline and intermodal ports within the one business day porting interval mandated by the Commission and will be used to comply with Section 251 of the Telecommunications Act of 1996.

On November 16, 2023, the FCC released a *Report and Order and Further Notice of Proposed Rulemaking* (88 FR 85794 (Dec. 8, 2023)) (*SIM Swap and Port-Out Fraud Order*), which adds new information collection requirements. The *SIM Swap and Port-Out Fraud Order* adopted baseline measures to increase protections for customers against fraudulent port-outs by adding new section 52.37 in Part 52, and adds new information collection requirements in paragraphs (c), (e), and (g), of that rule. Port-out fraud occurs where a bad actor impersonates a customer of a wireless provider and convinces the provider to port the real customer’s telephone number to a new

wireless provider and a device that the bad actor controls, allowing a bad actor to control the victim’s mobile account and receive text messages and phone calls intended for the victim. The new rules establish a uniform framework that gives wireless providers flexibility to implement customer authentication and security methods to address port-out fraud. Wireless providers are required to comply with the new or modified rules except where the Safe Connections Act requires alternate procedures to be used. The *SIM Swap and Port-Out Fraud Order* modifies the existing Local Number Portability collection requirements to require wireless providers to: (1) immediately notify customers of any requests for a port-out request associated with the customer’s account before effectuating the request; (2) provide customers with advance notice of any account protection measures offered; and (3) maintain a clear process for customers to report fraudulent number ports, and promptly provide customers with documentation of fraudulent ports involving their accounts.

Federal Communications Commission.

Marlene Dortch,

Secretary, Office of the Secretary.

[FR Doc. 2024–25103 Filed 10–28–24; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL MEDIATION AND CONCILIATION SERVICE

Privacy Act of 1974; System of Records

AGENCY: Federal Mediation and Conciliation Service.

ACTION: Notice of a modified system of records.

SUMMARY: Federal Mediation and Conciliation Service (FMCS) Center for Conflict Resolution Education (CCRE) and Field Operations use this system to process conference attendee and participant registration. FMCS hosts, co-hosts, sponsors, or co-sponsors conferences designed to meet the real-world challenges of labor management relations, conflict resolution, mediation, and arbitration. FMCS uses additional vendors to register attendees and participants and to promote conferences. FMCS uses GovDelivery Communications Cloud to promote events. The notice amendment includes administrative updates to refine details published under summary, addresses, supplementary information, purpose of the system, policies and practices for storage of records, administrative

safeguards, record access procedures, and the history section. These sections are amended to refine previously published information about the system of records. The dates, further information contact, system name, security classification, system location, system manager, authority for maintenance of the system, categories of individuals covered by the system, categories of records in the system, record source categories, routine uses, policies and practices for retrieval of records, policies and procedures for retention and disposal of records, contesting records procedures, notification procedures, and exemptions promulgated sections remain unchanged. This amended SORN deletes and supersedes the SORN published in the **Federal Register** on July 22, 2022.

DATES: This system of records will be effective without further notice on November 29, 2024 unless otherwise revised pursuant to comments received. Comments must be received on or before November 29, 2024.

ADDRESSES: You may send comments, identified by FMCS–00012, by any of the following methods:

- *Mail:* FMCS, 250 E Street SW, Washington, DC 20427.
- *Email:* register@fmcs.gov. Include FMCS–00012 on the subject line of the message.

FOR FURTHER INFORMATION CONTACT:

Kimberly Warren, Digital Media Strategist, at kwarren@fmcs.gov or call 202–606–5364. NLMC questions, email address is nlmcinfo@fmcs.gov.

SUPPLEMENTARY INFORMATION: The notice amendment includes administrative updates to refine details published under summary, addresses, supplementary information, purpose of the system, policies and practices for storage of records, administrative safeguards, record access procedures, and the history section. These sections are amended to refine previously published information about the system of records. The dates, further information contact, system name, security classification, system location, system manager, authority for maintenance of the system, categories of individuals covered by the system, categories of records in the system, record source categories, routine uses, policies and practices for retrieval of records, policies and procedures for retention and disposal of records, contesting records procedures, notification procedures, and exemptions promulgated sections remain unchanged.

To further promote the use of mediation, conflict resolution, and labor relations management in accordance with FMCS's mission, FMCS sponsors and co-sponsors conferences. These conferences educate and train members of the public and private sectors. GovDelivery is a web-based email subscription management application, provided by Granicus, that allows members of the public to subscribe to get information from the FMCS via email. Subscribers can choose from numerous subscriptions offered by FMCS, including, but not limited to, press releases, training opportunities, and event-related notifications. Attendees and participants may subscribe via a secure web page, to receive FMCS emails through a signup page on *fmcs.gov*.

SYSTEM NAME AND NUMBER:

FMCS Conference System—FMCS—00012.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

FMCS, 250 E Street SW, Washington, DC 20427.

SYSTEM MANAGER(S):

Greg Raelson, Director of Congressional and Public Affairs, email *graelson@fmcs.gov*, call 202-606-8081 or send mail to FMCS, 250 E Street SW, Washington, DC 20427, Attn: Greg Raelson. For GovDelivery, call 800-314-0147 or contact support at <https://support.granicus.com/s/contactsupport>.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

29 U.S.C. 172; 29 U.S.C. 173 (e); and 29 CFR 1403.

PURPOSE(S) OF THE SYSTEM:

The purpose of the system is for collecting, processing, and maintaining participant's or attendee's basic contact information for FMCS conferences. The basic information is required to determine the participant's or attendee's region or geographical location and to have adequate preparation for the conference. This information is also used to assess the best allocation of FMCS resources. The system gives a detailed structure of the conference including the conference program, keynote sessions, list of invited speakers with their background information, timetables for the conference meetings, venues of the conference, conference sponsors, and conference fees. The system is made up of interrelated components to perform to task, for example a computer system and IT system (multiple computers joined by a

network). The system also includes GovDelivery which handles digital subscription management and deliver opt-in email and other messaging to FMCS audiences. Audiences include, but are not limited to, citizens who are interested in receiving news and updates from the FMCS, seek to register for FMCS events and conferences, and who opt to receive targeted communications or specific topics related to conflict management.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals in this system include: the public (as attendees or participants), conference speakers, and Federal employees who register on the FMCS website for participation in selected training workshops, webinars, training sessions, and conference sessions hosted by FMCS.

CATEGORIES OF RECORDS IN THE SYSTEM:

The categories of records maintained in the system include:

- (1) List of conference programs, including event location, time, date, conference events and agendas;
- (2) Information pertaining to registration including names, registration fees, conference description, and professional affiliation;
- (3) Attendee's information or participant information including first name, last name, email address, title, office, employer/organization, address, room #/mail code, city, state, zip/postal code, country, and telephone and fax number; and
- (4) Information concerning the basis for and supporting documentation regarding the conference.

RECORD SOURCE CATEGORIES:

The information pertaining to this system is primarily collected via website from individuals requesting to register for an event sponsored by FMCS. The sources of information include attendees, speakers, exhibitors, officials, education professionals, FMCS employees, and guests.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside the FMCS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

- (a) To disclose pertinent information to the appropriate Federal, State, or

local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule regulation or order where the record, either alone or in conjunction with other information creates an indication of a violation or potential violation of civil or criminal laws or regulations.

(b) To disclose information to the National Archives and Records Administration (NARA) for use in its records management inspections; to the Government Accountability Office (GAO) for oversight purposes; to the Department of Justice (DOJ) to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or to the Office of Management and Budget (OMB) to obtain that office's advice regarding obligations under the Privacy Act.

(c) To disclose information to the National Archives and Records Administration (NARA) or the General Services Administration in records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

(d) To a former employee of the Agency for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Agency regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Agency requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(e) To disclose information to contractors, grantees, experts, consultants, detailees, and other non-Government employees performing or working on a contract, service, or other assignment for the Federal Government when necessary to accompany an agency function related to this system of records.

(f) To officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accordance with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

(g) To disclose information to a Member of Congress or a congressional office in response to an inquiry made on behalf of, and at the request of, an individual who is the subject of the record.

(h) In an appropriate proceeding before a court, grand jury, or

administrative or adjudicative body or official, when FMCS or other Agency representing FMCS determines the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(i) To the Department of Justice, including Offices of the U.S. Attorneys; another Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body; another party in litigation before a court, adjudicative, or administrative body; or to a court, adjudicative, or administrative body. Such disclosure is permitted only when it is relevant and necessary to the litigation or proceeding, and one of the following is a party to the litigation or has an interest in such litigation:

- (1) FMCS, or any component thereof;
- (2) Any employee or former employee of FMCS in their official capacity;
- (3) Any employee or former employee of FMCS in their capacity where the Department of Justice or FMCS has agreed to represent the employee;
- (4) The United States, a Federal agency, or another party in litigation before a court, adjudicative, or administrative body, upon the FMCS General Counsel's approval, pursuant to 5 CFR part 295 or otherwise.

(j) To any federal agency, organization, or person for the purposes of performing audit or oversight operations related to the operation of this system of records as authorized by law, but only information necessary and relevant to such audit or oversight function.

(k) To disclose information to appropriate agencies, entities, and persons when: (1) FMCS suspects or has confirmed that there has been a breach of the system of records; (2) FMCS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, FMCS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with FMCS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(l) To disclose information to another Federal agency or Federal entity, when FMCS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2)

preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

(m) To disclose to professional affiliations, licensing entities, and employers to verify attendance and course completion.

(n) To disclose, in a limited capacity, to vendor(s) to provide requested accommodations associated with conference attendance or participation.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

These records are maintained in electronic form only accessible to authorized personnel. Electronic records are stored on the agency's internal servers with restricted access to only authorized personnel and designated officials as determined by agency officials. GovDelivery is a hosted subscription system, and all records are maintained by the hosting company.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

The records are retrieved by the name or other programming identifier assigned to an individual in the electronic database system. Records may also be retrieved by the title of the conference and entity associated with the attendee's or participant's registration.

POLICIES AND PRACTICES FOR RETENTION OF DISPOSAL OF RECORDS:

All records are retained and disposed of in accordance with General Records Schedule 6.4, issued by the National Archives and Records Administration, and FMCS. Records are destroyed when three years old or when they are no longer needed for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Regarding the Conference system, records are maintained in a Microsoft Azure Storage Blob with a Windows File System shared folder with permissions set to only allow those with designated access by membership through a Windows Azure group membership. Group access and modification is controlled by IT which uses a privileged administrator account. Array is physically located in a locked computer room with limited badge access. GovDelivery is a remote hosted subscription system accessed by username/password maintained by the host company and created by the user of the systems. FMCS administrators maintain accounts/access and content

for the hosted spaces. GovDelivery is a FedRAMP authorized vendor and use government accepted procedures for keeping data safe.

RECORD ACCESS PROCEDURES:

Attendees and participants may access the GovDelivery system via links placed on client web pages or in system-generated emails. GovDelivery subscribers have access to their own personal data in the system. Individuals must provide the following information for their records to be located and identified: (1) Full name, (2) Address, and (3) A reasonably identifying description of the record content requested. Requests can be submitted via fmcs.gov/foia/, via email to privacy@fmcs.gov, or via mail to FMCS, Privacy Office, 250 E Street SW, Washington, DC 20427. See 29 CFR 1410.3, Individual access requests.

CONTESTING RECORDS PROCEDURES:

See 29 CFR 1410.6, Requests for correction or amendment of records, on how to contest the content of any records. Privacy Act requests to amend or correct records may be submitted to the Privacy Office at privacy@fmcs.gov or Privacy Officer at FMCS, Privacy Office, 250 E Street SW, Washington, DC 20427. Also, see <https://www.fmcs.gov/privacy-policy/>.

NOTIFICATION PROCEDURES:

See 29 CFR 1410.3(a), Individual access requests.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

This amended SORN deletes and supersedes the SORN published in the **Federal Register** on July 22, 2022, at 87 FR 43853.

Dated: October 24, 2024.

Anna Davis,
General Counsel.

[FR Doc. 2024-25071 Filed 10-28-24; 8:45 am]

BILLING CODE 6732-01-P

FEDERAL RESERVE SYSTEM

Agency Information Collection Activities: Announcement of Board Approval Under Delegated Authority and Submission to OMB

AGENCY: Board of Governors of the Federal Reserve System.

SUMMARY: The Board of Governors of the Federal Reserve System (Board) is adopting a proposal to extend for three years, without revision, the Reporting, Recordkeeping, and Disclosure

Requirements Associated with the Consumer Financial Protection Bureau's (CFPB) Home Mortgage Disclosure Act (HMDA) Loan/Application Register Required by Regulation C (FR HMDA LAR; OMB No. 7100-0247).

FOR FURTHER INFORMATION CONTACT:

Federal Reserve Board Clearance Officer—Nuha Elmaghrabi—Office of the Chief Data Officer, Board of Governors of the Federal Reserve System, nuha.elmaghrabi@frb.gov, (202) 452-3884.

Office of Management and Budget (OMB) Desk Officer for the Federal Reserve Board, Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Room 10235, 725 17th Street NW, Washington, DC 20503, or by fax to (202) 395-6974.

SUPPLEMENTARY INFORMATION: On June 15, 1984, OMB delegated to the Board authority under the Paperwork Reduction Act (PRA) to approve and assign OMB control numbers to collections of information conducted or sponsored by the Board. Board-approved collections of information are incorporated into the official OMB inventory of currently approved collections of information. The OMB inventory, as well as copies of the PRA Submission, supporting statements (which contain more detailed information about the information collections and burden estimates than this notice), and approved collection of information instrument(s) are available at <https://www.reginfo.gov/public/do/PRAMain>. These documents are also available on the Federal Reserve Board's public website at <https://www.federalreserve.gov/apps/reportingforms/home/review> or may be requested from the agency clearance officer, whose name appears above. On the page displayed at the link above, you can find the supporting information by referencing the collection identifier, FR HMDA LAR.

Final Approval Under OMB Delegated Authority of the Extension for Three Years, Without Revision, of the Following Information Collection

Collection title: Reporting, Recordkeeping, and Disclosure Requirements Associated with the CFPB's Home Mortgage Disclosure Act Loan/Application Register Required by Regulation C.

Collection identifier: FR HMDA LAR.
OMB control number: 7100-0247.

General description of collection: The HMDA was enacted in 1975 and is implemented by Regulation C. Generally, the HMDA requires certain

depository and non-depository institutions that make certain mortgage loans to collect, report, and disclose data about originations and purchases of mortgage loans, as well as loan applications that do not result in originations (for example, applications that are denied or withdrawn).

The FR HMDA LAR is the Board's information collection associated with the CFPB's Regulation C. The FR HMDA LAR is used to (1) help determine whether financial institutions are serving the housing needs of their communities, (2) assist public officials in distributing public-sector investments so as to attract private investment to areas where it is needed, and (3) assist in identifying possible discriminatory lending patterns and enforcing anti-discrimination statutes.

Frequency: Quarterly and annually.

Respondents: Except those that are supervised by the CFPB: state member banks, their subsidiaries, subsidiaries of bank holding companies, subsidiaries of savings and loan holding companies, U.S. branches and agencies of foreign banks (other than federal branches, federal agencies, and insured state branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601-604a; 611-631).

Total estimated number of respondents: 654.

Total estimated annual burden hours: 960,235.

Current actions: On June 7, 2024, the Board published a notice in the **Federal Register** (89 FR 48636) requesting public comment for 60 days on the extension, without revision, of the FR HMDA LAR. The comment period for this notice expired on August 6, 2024. The Board did not receive any comments.

Board of Governors of the Federal Reserve System, October 23, 2024.

Benjamin W. McDonough,

Deputy Secretary and Ombuds of the Board.

[FR Doc. 2024-25040 Filed 10-28-24; 8:45 am]

BILLING CODE 6210-01-P

FEDERAL RESERVE SYSTEM

Change in Bank Control Notices; Acquisitions of Shares of a Bank or Bank Holding Company

The notificants listed below have applied under the Change in Bank Control Act (Act) (12 U.S.C. 1817(j)) and § 225.41 of the Board's Regulation Y (12 CFR 225.41) to acquire shares of a bank or bank holding company. The factors

that are considered in acting on the applications are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The public portions of the applications listed below, as well as other related filings required by the Board, if any, are available for immediate inspection at the Federal Reserve Bank(s) indicated below and at the offices of the Board of Governors. This information may also be obtained on an expedited basis, upon request, by contacting the appropriate Federal Reserve Bank and from the Board's Freedom of Information Office at <https://www.federalreserve.gov/foia/request.htm>. Interested persons may express their views in writing on the standards enumerated in paragraph 7 of the Act.

Comments received are subject to public disclosure. In general, comments received will be made available without change and will not be modified to remove personal or business information including confidential, contact, or other identifying information. Comments should not include any information such as confidential information that would not be appropriate for public disclosure.

Comments regarding each of these applications must be received at the Reserve Bank indicated or the offices of the Board of Governors, Ann E. Misback, Secretary of the Board, 20th Street and Constitution Avenue NW, Washington, DC 20551-0001, not later than November 13, 2024.

A. Federal Reserve Bank of Atlanta (Erien O. Terry, Assistant Vice President), 1000 Peachtree Street NE, Atlanta, Georgia 30309. Comments can also be sent electronically to Applications.Comments@atl.frb.org:

1. *John Daniel Way; RF Way Family Trust, John Daniel Way, as trustee; Trust for the Benefit of James Daniel Way, John Daniel Way, as trustee; John Samuel Way, all of Hawkinsville, Georgia; Mary Ann Way, Alexandria, Virginia; Robert F. Way; Robert F. Way Family Trust, Robert F. Way, as trustee, both of Perry, Georgia; Dottie Way Woodroof, W. Cole Woodroof, Mary Margaret Sandy, William Cole Woodroof, Jr., all of Cordele, Georgia; as a group acting in concert, to retain voting shares of Planters First Bancorp, Inc., Hawkinsville, Georgia, and indirectly retain voting shares of Planters First Bank, Cordele, Georgia.*

B. Federal Reserve Bank of Minneapolis (Mark Rauzi, Vice President), 90 Hennepin Avenue, Minneapolis, Minnesota 55480-0291. Comments can also be sent electronically to MA@mpls.frb.org:

1. *Katelyn Kae Olson, Adrian, Minnesota*; to become co-trustee of First State Bank Southwest KSOP Plan and Trust, and thereby acquire control of First Rushmore Bancorporation, Inc., both of Worthington, Minnesota, and thereby indirectly acquire control of First State Bank Southwest, Pipestone, Minnesota.

Board of Governors of the Federal Reserve System.

Michele Taylor Fennell,

Associate Secretary of the Board.

[FR Doc. 2024–25118 Filed 10–28–24; 8:45 am]

BILLING CODE 6210–01–P

FEDERAL RESERVE SYSTEM

Proposed Agency Information Collection Activities; Comment Request

AGENCY: Board of Governors of the Federal Reserve System.

ACTION: Notice, request for comment.

SUMMARY: The Board of Governors of the Federal Reserve System (Board) invites comment on a proposal to extend for three years, without revision, the Recordkeeping Provisions Associated with the Guidance on Sound Incentive Compensation Policies (FR 4027; OMB No. 7100–0327).

DATES: Comments must be submitted on or before December 30, 2024.

ADDRESSES: You may submit comments, identified by FR 4027, by any of the following methods:

- *Agency Website:* <https://www.federalreserve.gov/>. Follow the instructions for submitting comments at <https://www.federalreserve.gov/apps/foia/proposedregs.aspx>.

- *Email:* regs.comments@federalreserve.gov. Include the OMB number or FR number in the subject line of the message.

- *FAX:* (202) 452–3819 or (202) 452–3102.

- *Mail:* Federal Reserve Board of Governors, Attn: Ann E. Misback, Secretary of the Board, Mailstop M–4775, 2001 C St. NW, Washington, DC 20551.

All public comments are available from the Board's website at <https://www.federalreserve.gov/apps/foia/proposedregs.aspx> as submitted, unless modified for technical reasons or to remove personally identifiable information at the commenter's request. Accordingly, comments will not be edited to remove any confidential business information, identifying information, or contact information. Public comments may also be viewed electronically or in paper in Room M–

4365A, 2001 C St. NW, Washington, DC 20551, between 9:00 a.m. and 5:00 p.m. on weekdays, except for Federal holidays. For security reasons, the Board requires that visitors make an appointment to inspect comments. You may do so by calling (202) 452–3684. Upon arrival, visitors will be required to present valid government-issued photo identification and to submit to security screening in order to inspect and photocopy comments.

Additionally, commenters may send a copy of their comments to the Office of Management and Budget (OMB) Desk Officer for the Federal Reserve Board, Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Room 10235, 725 17th Street NW, Washington, DC 20503, or by fax to (202) 395–6974.

FOR FURTHER INFORMATION CONTACT:

Federal Reserve Board Clearance Officer—Nuha Elmaghribi—Office of the Chief Data Officer, Board of Governors of the Federal Reserve System, nuha.elmaghribi@frb.gov, (202) 452–3884.

SUPPLEMENTARY INFORMATION: On June 15, 1984, OMB delegated to the Board authority under the Paperwork Reduction Act (PRA) to approve and assign OMB control numbers to collections of information conducted or sponsored by the Board. In exercising this delegated authority, the Board is directed to take every reasonable step to solicit comment. In determining whether to approve a collection of information, the Board will consider all comments received from the public and other agencies.

During the comment period for this proposal, a copy of the proposed PRA OMB submission, including the draft reporting form and instructions, supporting statement (which contains more detail about the information collection and burden estimates than this notice), and other documentation, will be made available on the Board's public website at <https://www.federalreserve.gov/apps/reportingforms/home/review> or may be requested from the agency clearance officer, whose name appears above. On the page displayed at the link above, you can find the supporting information by referencing the collection identifier, FR 4027. Final versions of these documents will be made available at <https://www.reginfo.gov/public/do/PRAMain>, if approved.

Request for Comment on Information Collection Proposal

The Board invites public comment on the following information collection, which is being reviewed under authority delegated by the OMB under the PRA. Comments are invited on the following:

- a. Whether the proposed collection of information is necessary for the proper performance of the Board's functions, including whether the information has practical utility;

- b. The accuracy of the Board's estimate of the burden of the proposed information collection, including the validity of the methodology and assumptions used;

- c. Ways to enhance the quality, utility, and clarity of the information to be collected;

- d. Ways to minimize the burden of information collection on respondents, including through the use of automated collection techniques or other forms of information technology; and

- e. Estimates of capital or startup costs and costs of operation, maintenance, and purchase of services to provide information.

At the end of the comment period, the comments and recommendations received will be analyzed to determine the extent to which the Board should modify the proposal.

Proposal Under OMB Delegated Authority To Extend for Three Years, Without Revision the Following Information Collection

Collection title: Recordkeeping Provisions Associated with the Guidance on Sound Incentive Compensation Policies.

Collection identifier: FR 4027.

OMB control number: 7100–0327.

General description of collection: The interagency Guidance on Sound Incentive Compensation Policies (the Guidance) is intended to assist banking organizations in designing and implementing incentive compensation arrangements that do not encourage imprudent risk-taking and that are consistent with the safety and soundness of the organization. The Guidance contains voluntary recordkeeping activities. With respect to organizations regulated by the Board, the voluntary Guidance applies to U.S. bank holding companies, savings and loan holding companies, state member banks, Edge and agreement corporations, and the U.S. operations of foreign banks with a branch, agency, or commercial lending company subsidiary in the United States (collectively, banking organizations).

Frequency: As needed.

Respondents: Banking organizations, as defined above.

Total estimated number of respondents: 5,122.

Total estimated annual burden hours: 205,440.

Board of Governors of the Federal Reserve System, October 23, 2024.

Benjamin W. McDonough,

Deputy Secretary and Ombuds of the Board.

[FR Doc. 2024-25041 Filed 10-28-24; 8:45 am]

BILLING CODE 6210-01-P

FEDERAL RESERVE SYSTEM

Agency Information Collection

Activities: Announcement of Board Approval Under Delegated Authority and Submission to OMB

AGENCY: Board of Governors of the Federal Reserve System.

SUMMARY: The Board of Governors of the Federal Reserve System (Board) is adopting a proposal to extend for three years, without revision, the Recordkeeping and Disclosure Requirements Associated with CFPB's Regulation Z (FR Z; OMB No. 7100-0199).

FOR FURTHER INFORMATION CONTACT:

Federal Reserve Board Clearance Officer—Nuha Elmaghrabi—Office of the Chief Data Officer, Board of Governors of the Federal Reserve System, nuha.elmaghrabi@frb.gov, (202) 452-3884.

Office of Management and Budget (OMB) Desk Officer for the Federal Reserve Board, Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Room 10235, 725 17th Street NW, Washington, DC 20503, or by fax to (202) 395-6974.

SUPPLEMENTARY INFORMATION: On June 15, 1984, OMB delegated to the Board authority under the Paperwork Reduction Act (PRA) to approve and assign OMB control numbers to collections of information conducted or sponsored by the Board. Board-approved collections of information are incorporated into the official OMB inventory of currently approved collections of information. The OMB inventory, as well as copies of the PRA Submission, supporting statements (which contain more detailed information about the information collections and burden estimates than this notice), and approved collection of information instrument(s) are available at <https://www.reginfo.gov/public/do/PRAMain>. These documents are also available on the Federal Reserve Board's

public website at <https://www.federalreserve.gov/apps/reportingforms/home/review> or may be requested from the agency clearance officer, whose name appears above. On the page displayed at the link above, you can find the supporting information by referencing the collection identifier, FR Z.

Final Approval under OMB Delegated Authority of the Extension for Three Years, Without Revision, of the Following Information Collection

Collection title: Recordkeeping and Disclosure Requirements Associated with CFPB's Regulation Z.

Collection identifier: FR Z.

OMB control number: 7100-0199.

General description of collection: The Truth in Lending Act (TILA) and Regulation Z require creditors to provide consumers with disclosures about the costs, terms, and related information regarding a wide range of credit products for personal, family, or household purposes. Depending on the credit product, required disclosures include information that must be provided at the time of the consumer's application for credit, at consummation (for closed-end credit) or account-opening (for open-end credit), and throughout the term of the loan. The TILA and Regulation Z also contain rules concerning recordkeeping and credit advertising.

The FR Z is the Board's information collection associated with the Consumer Financial Protection Bureau's (CFPB's) Regulation Z. FR Z is used to promote the informed use of credit by consumers for personal, family, or household purposes by requiring these disclosures about the terms and costs of these products, as well as ensuring that consumers are provided with timely information on the nature and costs of the residential real estate settlement process.

Frequency: Event-generated.

Respondents: State member banks with assets of \$10 billion or less that are not affiliated with an insured depository institution with assets over \$10 billion (irrespective of the consolidated assets of any holding company); non-depository affiliates of such state member banks; and non-depository affiliates of bank holding companies that are not affiliated with an insured depository institution with assets over \$10 billion.

Total estimated number of respondents: 3,695.

Total estimated annual burden hours: 387,079.

Current actions: On June 7, 2024, the Board published a notice in the **Federal**

Register (89 FR 48645) requesting public comment for 60 days on the extension, without revision, of the FR Z. The comment period for this notice expired on August 6, 2024. The Board did not receive any comments.

Board of Governors of the Federal Reserve System, October 23, 2024.

Benjamin W. McDonough,

Deputy Secretary and Ombuds of the Board.

[FR Doc. 2024-25039 Filed 10-28-24; 8:45 am]

BILLING CODE 6210-01-P

FEDERAL RESERVE SYSTEM

Formations of, Acquisitions by, and Mergers of Bank Holding Companies

The companies listed in this notice have applied to the Board for approval, pursuant to the Bank Holding Company Act of 1956 (12 U.S.C. 1841 *et seq.*) (BHC Act), Regulation Y (12 CFR part 225), and all other applicable statutes and regulations to become a bank holding company and/or to acquire the assets or the ownership of, control of, or the power to vote shares of a bank or bank holding company and all of the banks and nonbanking companies owned by the bank holding company, including the companies listed below.

The public portions of the applications listed below, as well as other related filings required by the Board, if any, are available for immediate inspection at the Federal Reserve Bank(s) indicated below and at the offices of the Board of Governors. This information may also be obtained on an expedited basis, upon request, by contacting the appropriate Federal Reserve Bank and from the Board's Freedom of Information Office at <https://www.federalreserve.gov/foia/request.htm>. Interested persons may express their views in writing on the standards enumerated in the BHC Act (12 U.S.C. 1842(c)).

Comments received are subject to public disclosure. In general, comments received will be made available without change and will not be modified to remove personal or business information including confidential, contact, or other identifying information. Comments should not include any information such as confidential information that would not be appropriate for public disclosure.

Comments regarding each of these applications must be received at the Reserve Bank indicated or the offices of the Board of Governors, Ann E. Misback, Secretary of the Board, 20th Street and Constitution Avenue NW, Washington, DC 20551-0001, not later than November 29, 2024.

A. Federal Reserve Bank of Dallas (Karen Smith, Director, Mergers & Acquisitions) 2200 North Pearl Street, Dallas, Texas 75201–2272. Comments can also be sent electronically to Comments.applications@dal.frb.org:

1. *First Liberty National Bancshares, Inc., Liberty, Texas*; to acquire Pearland State Bank, Pearland, Texas, and First National Bank of Alvin, Alvin, Texas.

Board of Governors of the Federal Reserve System.

Michele Taylor Fennell,

Associate Secretary of the Board.

[FR Doc. 2024–25119 Filed 10–28–24; 8:45 am]

BILLING CODE P

FEDERAL RESERVE SYSTEM

Proposed Agency Information Collection Activities; Comment Request

AGENCY: Board of Governors of the Federal Reserve System.

ACTION: Notice, request for comment.

SUMMARY: The Board of Governors of the Federal Reserve System (Board) invites comment on a proposal to extend for three years, without revision, the Recordkeeping Requirements of Regulation H and Regulation K Associated with the Procedures for Monitoring Bank Secrecy Act Compliance (FR K; OMB No. 7100–0310).

DATES: Comments must be submitted on or before December 30, 2024.

ADDRESSES: You may submit comments, identified by FR K, by any of the following methods:

- **Agency Website:** <https://www.federalreserve.gov/>. Follow the instructions for submitting comments at <https://www.federalreserve.gov/apps/foia/proposedregs.aspx>.
- **Email:** regs.comments@federalreserve.gov. Include the OMB number or FR number in the subject line of the message.
- **FAX:** (202) 452–3819 or (202) 452–3102.

- **Mail:** Federal Reserve Board of Governors, Attn: Ann E. Misback, Secretary of the Board, Mailstop M–4775, 2001 C St. NW, Washington, DC 20551.

All public comments are available from the Board's website at <https://www.federalreserve.gov/apps/foia/proposedregs.aspx> as submitted, unless modified for technical reasons or to remove personally identifiable information at the commenter's request. Accordingly, comments will not be edited to remove any confidential

business information, identifying information, or contact information. Public comments may also be viewed electronically or in paper in Room M–4365A, 2001 C St NW, Washington, DC 20551, between 9:00 a.m. and 5:00 p.m. on weekdays, except for Federal holidays. For security reasons, the Board requires that visitors make an appointment to inspect comments. You may do so by calling (202) 452–3684. Upon arrival, visitors will be required to present valid government-issued photo identification and to submit to security screening in order to inspect and photocopy comments.

Additionally, commenters may send a copy of their comments to the Office of Management and Budget (OMB) Desk Officer for the Federal Reserve Board, Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Room 10235, 725 17th Street NW, Washington, DC 20503, or by fax to (202) 395–6974.

FOR FURTHER INFORMATION CONTACT: Federal Reserve Board Clearance Officer—Nuha Elmaghrabi—Office of the Chief Data Officer, Board of Governors of the Federal Reserve System, nuha.elmaghrabi@frb.gov, (202) 452–3884.

SUPPLEMENTARY INFORMATION: On June 15, 1984, OMB delegated to the Board authority under the Paperwork Reduction Act (PRA) to approve and assign OMB control numbers to collections of information conducted or sponsored by the Board. In exercising this delegated authority, the Board is directed to take every reasonable step to solicit comment. In determining whether to approve a collection of information, the Board will consider all comments received from the public and other agencies.

During the comment period for this proposal, a copy of the proposed PRA OMB submission, including the draft reporting form and instructions, supporting statement (which contains more detail about the information collection and burden estimates than this notice), and other documentation, will be made available on the Board's public website at <https://www.federalreserve.gov/apps/reportingforms/home/review> or may be requested from the agency clearance officer, whose name appears above. On the page displayed at the link above, you can find the supporting information by referencing the collection identifier, FR K. Final versions of these documents will be made available at <https://www.reginfo.gov/public/do/PRAMain>, if approved.

Request for Comment on Information Collection Proposal

The Board invites public comment on the following information collection, which is being reviewed under authority delegated by the OMB under the PRA. Comments are invited on the following:

- a. Whether the proposed collection of information is necessary for the proper performance of the Board's functions, including whether the information has practical utility;
- b. The accuracy of the Board's estimate of the burden of the proposed information collection, including the validity of the methodology and assumptions used;
- c. Ways to enhance the quality, utility, and clarity of the information to be collected;
- d. Ways to minimize the burden of information collection on respondents, including through the use of automated collection techniques or other forms of information technology; and
- e. Estimates of capital or startup costs and costs of operation, maintenance, and purchase of services to provide information.

At the end of the comment period, the comments and recommendations received will be analyzed to determine the extent to which the Board should modify the proposal.

Proposal Under OMB Delegated Authority To Extend for Three Years, Without Revision, the Following Information Collection

Collection title: Recordkeeping Requirements of Regulation H and Regulation K Associated with the Procedures for Monitoring Bank Secrecy Act Compliance.

Collection identifier: FR K.

OMB control number: 7100–0310.

General description of collection: Section 208.63 of the Board's Regulation H—Membership of State Banking Institutions in the Federal Reserve System (12 CFR part 208) requires state member banks to establish and maintain in writing procedures reasonably designed to ensure and monitor compliance with the provisions of the Bank Secrecy Act (BSA) and its implementing regulations. Sections 211.5(m)(1) and 211.24(j)(1) of the Board's Regulation K—International Banking Operations (12 CFR part 211) impose those same requirements on Edge and agreement corporations and, except for a federal branch or a federal agency or a state branch that is insured by the Federal Deposit Insurance Corporation (FDIC), the U.S. branches, agencies, and representative offices of

foreign banks operating in the United States.

Frequency: One-time and on occasion.

Respondents: State member banks; Edge and agreement corporations; and U.S. branches, agencies, and representative offices of foreign banks operating in the United States, except for a federal branch or a federal agency or a state branch that is insured by the FDIC.

Total estimated number of respondents: 878.

Total estimated annual burden hours: 3,544.

Board of Governors of the Federal Reserve System, October 23, 2024.

Benjamin W. McDonough,

Deputy Secretary and Ombuds of the Board.

[FR Doc. 2024–25043 Filed 10–28–24; 8:45 am]

BILLING CODE 6210–01–P

FEDERAL RESERVE SYSTEM

Agency Information Collection Activities: Announcement of Board Approval Under Delegated Authority and Submission to OMB

AGENCY: Board of Governors of the Federal Reserve System.

SUMMARY: The Board of Governors of the Federal Reserve System (Board) is adopting a proposal to extend for three years, without revision, the Recordkeeping and Disclosure Requirements Associated with Consumer Financial Protection Bureau's (CFPB's) Regulation B (FR B; OMB No. 7100–0201).

FOR FURTHER INFORMATION CONTACT:

Federal Reserve Board Clearance Officer—Nuha Elmaghrabi—Office of the Chief Data Officer, Board of Governors of the Federal Reserve System, nuha.elmaghrabi@frb.gov, (202) 452–3884.

Office of Management and Budget (OMB) Desk Officer for the Federal Reserve Board, Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Room 10235, 725 17th Street NW, Washington, DC 20503, or by fax to (202) 395–6974.

SUPPLEMENTARY INFORMATION: On June 15, 1984, OMB delegated to the Board authority under the Paperwork Reduction Act (PRA) to approve and assign OMB control numbers to collections of information conducted or sponsored by the Board. Board-approved collections of information are incorporated into the official OMB inventory of currently approved collections of information. The OMB inventory, as well as copies of the PRA

Submission, supporting statements (which contain more detailed information about the information collections and burden estimates than this notice), and approved collection of information instrument(s) are available at <https://www.reginfo.gov/public/do/PRAMain>. These documents are also available on the Federal Reserve Board's public website at <https://www.federalreserve.gov/apps/reportingforms/home/review> or may be requested from the agency clearance officer, whose name appears above. On the page displayed at the link above, you can find the supporting information by referencing the collection identifier, FR B.

Final Approval Under OMB Delegated Authority of the Extension for Three Years, Without Revision, of the Following Information Collection

Collection title: Recordkeeping and Disclosure Requirements Associated with CFPB's Regulation B.

Collection identifier: FR B.

OMB control number: 7100–0201.

General description of collection: The Equal Credit Opportunity Act (ECOA) was enacted in 1974 and is implemented by the CFPB's Regulation B. The ECOA prohibits discrimination in any aspect of a credit transaction because of race, color, religion, national origin, sex, marital status, age, receipt of public assistance, or the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act. To aid in implementation of this prohibition, the statute and Regulation B subject creditors to various mandatory disclosure requirements, notification provisions informing applicants of action taken on credit applications, provision of appraisal reports in connection with mortgages, credit history reporting, monitoring rules, and recordkeeping requirements. The FR B is the Board's information collection associated with the CFPB's Regulation B for institutions the Board supervises.

Frequency: Event generated and annually.

Respondents: Except those that are supervised by the CFPB: state member banks, their subsidiaries, subsidiaries of bank holding companies, subsidiaries of savings and loan holding companies, U.S. branches and agencies of foreign banks (other than federal branches, federal agencies, and insured state branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601–604a; 611–631).

Total estimated number of respondents: 841.

Total estimated annual burden hours: 81,346.

Current actions: On July 1, 2024, the Board published a notice in the **Federal Register** (89 FR 54463) requesting public comment for 60 days on the extension, without revision, of the FR B. The comment period for this notice expired on August 30, 2024. The Board did not receive any comments.

Board of Governors of the Federal Reserve System, October 23, 2024.

Benjamin W. McDonough,

Deputy Secretary and Ombuds of the Board.

[FR Doc. 2024–25044 Filed 10–28–24; 8:45 am]

BILLING CODE 6210–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Submission for Office of Management and Budget Review; Child and Family Services Reviews (OMB #0970–0214)

AGENCY: Children's Bureau, Administration for Children and Families, U.S. Department of Health and Human Services.

ACTION: Request for Public Comments.

SUMMARY: The Administration for Children and Families (ACF) is requesting a 3-year extension of the activities associated with the Child and Family Services Reviews information collection (Office of Management and Budget (OMB) #0970–0214, expiration January 31, 2025). There are no changes requested to the collection.

DATES: *Comments due within 30 days of publication.* OMB must make a decision about the collection of information between 30 and 60 days after publication of this document in the **Federal Register**. Therefore, a comment is best assured of having its full effect if OMB receives it within 30 days of publication.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting “Currently under 30-day Review—Open for Public Comments” or by using the search function. You can also obtain copies of the proposed collection of information by emailing infocollection@acf.hhs.gov. Identify all emailed

requests by the title of the information collection.

SUPPLEMENTARY INFORMATION:

Description: The following activities are associated with the *Child and Family Services and Reviews* (CFSR) collection: CFSR Statewide Assessment; CFSR On-site Review; and the CFSR Program Improvement Plan. The collection of information for review of state child and family services programs (45 CFR 1355.33(b), 1355.33(c) and 1355.35(a)) is to determine whether such programs are in substantial conformity with state plan requirements under titles IV–B and IV–E of the Social Security Act (the Act) and is authorized

by section 1123(a) [42 U.S.C. 1320a–2a] of the Act. The CFSR looks at the outcomes related to safety, permanency and well-being of children served by the child welfare system and at seven systemic factors that support the outcomes. The information collection is needed to monitor state plan requirements under titles IV–B and IV–E of the Act and is required by federal statute. The resultant information will allow ACF to determine if states are in compliance with state plan requirements and are achieving desired outcomes for children and families. If necessary, ACF will require states to revise applicable statutes, rules,

policies, and procedures, and provide proper training to staff, through the development and implementation of program improvement plans. The CFSR reviews not only address conformity with state plan requirements but also assist states in enhancing the capacities to serve children and families. In computing the number of burden hours for this information collection, ACF based the annual burden estimates on ACF's and states' experiences in conducting reviews and developing program improvement plans.

Respondents: State Title IV–E Agencies.

Annual Burden Estimates

Instrument	Total number of respondents	Total number of responses per respondent	Average burden hours per response	Total burden hours	Annual burden hours
Statewide Assessment (45 CFR 1355.33(b))	39	1	120	4,680	1,560
On-site Review Instrument Stakeholder Interview Guide (45 CFR 1355.33(c))	39	1	1,186	46,254	15,418
Program Improvement Plan (45 CFR 1355.35(a))	39	1	300	11,700	3,900

Estimated Total Annual Burden Hours: 20,878.

Authority: 42 U.S.C. 1320a–2a.

Mary C. Jones,

ACF/OPRE Certifying Officer.

[FR Doc. 2024–25033 Filed 10–28–24; 8:45 am]

BILLING CODE 4184–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Center for Scientific Review; Notice of Closed Meetings

Pursuant to section 1009 of the Federal Advisory Committee Act, as amended, notice is hereby given of the following meetings.

The meetings will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: Center for Scientific Review Special; Emphasis Panel Small Business: Neuroprosthetics, Biosensors and Clinical Devices.

Date: November 21, 2024.

Time: 10 a.m. to 4 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Angela Monique Boutte, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Dr., Bethesda, MD 20892, (301) 594–0063, email: boutteam@csr.nih.gov.

Name of Committee: Center for Scientific Review Special Emphasis Panel; RFA–NR–24–006: Understanding the Intersection of Social Inequities to Optimize Health and Reduce Health Disparities: The Axes Initiative.

Date: November 21, 2024.

Time: 11 a.m. to 4:30 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Suzanne Ryan, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 3139, MSC 7770, Bethesda, MD 20892, (301) 435–1712, email: ryansj@csr.nih.gov.

Name of Committee: Center for Scientific Review Special Emphasis Panel; Myalgic Encephalomyelitis-Chronic Fatigue Syndrome.

Date: November 21, 2024.

Time: 11 a.m. to 4 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Roger Janz, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Bethesda, MD 20892, (301) 402–8515, email: janzr2@csr.nih.gov.

Name of Committee: Center for Scientific Review Special Emphasis Panel; Member Conflict: Special Emphasis Panel on Topics in Endocrinology and Metabolism.

Date: November 21, 2024.

Time: 11 a.m. to 4 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Victoria Martinez Virador, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Bethesda, MD 20892, (301) 594–4703, email: victoria.virador@nih.gov.

Name of Committee: Center for Scientific Review Special Emphasis Panel; RFA–OD–24–012: Predoctoral Training in Advanced Data Analytics for Behavioral and Social Sciences Research (BSSR)—Institutional Research Training Program [T32].

Date: November 21, 2024.

Time: 12 p.m. to 6 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Victoriya Volkova, Ph.D., DVM, Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Bethesda, MD 20817, (301) 594–7781, email: volkovav2@csr.nih.gov.

Name of Committee: Center for Scientific Review Special Emphasis Panel; Member Conflict: Sensorimotor, Olfaction, and Interception.

Date: November 21, 2024.

Time: 12 p.m. to 6 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Kirk Thompson, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 5184, MSC 7844, Bethesda, MD 20892, 301-435-1242, email: kgt@mail.nih.gov.

Name of Committee: Center for Scientific Review Special Emphasis Panel; Member Conflict: Skeletal Muscle and Rehabilitation Sciences.

Date: November 22, 2024.

Time: 9 a.m. to 6 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Chee Lim, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 4128, Bethesda, MD 20892, (301) 435-1850, email: limc4@csr.nih.gov.

(Catalogue of Federal Domestic Assistance Program Nos. 93.306, Comparative Medicine; 93.333, Clinical Research, 93.306, 93.333, 93.337, 93.393-93.396, 93.837-93.844, 93.846-93.878, 93.892, 93.893, National Institutes of Health, HHS)

Dated: October 24, 2024.

Bruce A. George,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2024-25099 Filed 10-28-24; 8:45 am]

BILLING CODE 4140-01-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2024-0028]

Request for Comment on Product Security Bad Practices Guidance

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: Notice of availability; extension of comment period.

SUMMARY: On October 16, 2024, the Cybersecurity Division (CSD) within the Cybersecurity and Infrastructure Security Agency (CISA) published a request for comment in the **Federal Register** on the voluntary, draft Product Security Bad Practices guidance, which requests feedback on the draft guidance. CISA is extending the comment period

for the draft guidance for an additional fourteen days through December 16, 2024.

DATES: The comment period for the proposed voluntary guidance published on October 16, 2024, at 89 FR 83508 is extended. Comments and related materials must be submitted on or before December 16, 2024.

ADDRESSES: You may submit comments, identified by docket number CISA-2024-0028, by following the instructions below for submitting comments via the Federal eRulemaking Portal at <https://www.regulations.gov>.

Instructions: All comments received must include the agency name and docket number Docket Number CISA-2024-0028. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided. CISA reserves the right to publicly republish relevant and unedited comments in their entirety that are submitted to the docket. Do not include personal information such as account numbers, social security numbers, or the names of other individuals. Do not submit confidential business information or otherwise sensitive or protected information.

Docket: For access to the docket to read the draft Product Security Bad Practices Guidance or comments received, go to <https://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: Kirk Lawrence, 202-617-0036, SecureByDesign@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION: On October 16, 2024, CISA published a request for comment on voluntary, draft Product Security Bad Practices guidance (89 FR 83508). In the draft guidance, we provided an overview of product security practices that are deemed exceptionally risky, particularly for organizations supporting critical infrastructure or national critical functions (NCFs), and it provides recommendations for software manufacturers to voluntarily mitigate these risks. The guidance contained in the document is non-binding, and while CISA encourages organizations to avoid these bad practices, the document imposes no requirement on them to do so. The draft guidance is scoped to software manufacturers who develop software products and services, including on-premises software, cloud services, and software as a service (SaaS), used in support of critical infrastructure or NCFs. The request for comment provided for a 45-day comment period, set to close on

December 2, 2024. CISA received requests to extend the deadline given the Thanksgiving holiday. Therefore, the comment period is now open through December 16, 2024.

This notice is issued under the authority of 6 U.S.C. 652 and 659.

Jeffrey E. Greene,

Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2024-25078 Filed 10-28-24; 8:45 am]

BILLING CODE 9111-LF-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2024-0029]

Request for Comment on Security Requirements for Restricted Transactions Under Executive Order 14117

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), DHS.

ACTION: Notice and request for comment.

SUMMARY: CISA seeks public input on the development of security requirements for restricted transactions as directed by Executive Order (E.O.) 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." E.O. 14117 addresses national-security and foreign-policy threats that arise when countries of concern and covered persons can access bulk U.S. sensitive personal data or government-related data. The proposed CISA security requirements for restricted transactions would apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ).

DATES: Written comments are requested on or before November 29, 2024.

ADDRESSES: You may send comments, identified by docket number CISA-2024-0029, through the Federal eRulemaking Portal available at <http://www.regulations.gov>.

Instructions: All comments received will be posted to <https://www.regulations.gov>, including any personal information provided. For detailed instructions on sending comments and for information on the types of comments that are of particular interest to CISA, see the "Public Participation" and "Request for Public Input" heading of the **SUPPLEMENTARY INFORMATION** section of this document. Please note that this notice and request

for comment is not a rulemaking and that the Federal eRulemaking Portal is being utilized only as a mechanism for receiving comments.

FOR FURTHER INFORMATION CONTACT: Alicia Smith, Senior Policy Counsel, Cybersecurity and Infrastructure Security Agency, EOSecurityReqs@cisa.dhs.gov, 202–316–1560.

SUPPLEMENTARY INFORMATION:

I. Public Participation

All interested stakeholders are invited to comment on this notice and the security requirements described herein by submitting written data, comments, views, or arguments using the method identified in the **ADDRESSES** section. Interested stakeholders may view a copy of the proposed security requirements on CISA's website by visiting <https://www.cisa.gov> and searching for "Proposed Security Requirements for Restricted Transactions." A copy of the proposed security requirements is also included in the docket for this notice and request for comment, docket number CISA–2024–0029. All members of the public are invited to comment including, but not limited to, specialists in the field, academic experts, industry stakeholders, and public interest groups.

Instructions: All submissions must include the agency name and Docket ID for this notice. Comments may be submitted electronically via the Federal eRulemaking Portal.

To submit comments electronically:

1. Go to www.regulations.gov and enter CISA–2024–0029 in the search field,
2. Click the "Comment Now!" icon, complete the required fields, and
3. Enter or attach your comments.

All submissions, including attachments and other supporting materials, will become part of the public record and may be subject to public disclosure. CISA reserves the right to publish relevant comments publicly, unedited and in their entirety. Personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Do not submit confidential business information or otherwise sensitive or protected information. All comments received will be posted to <http://www.regulations.gov>. Commenters are encouraged to identify the number of the specific topic or topics that they are addressing.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov> and search for the Docket ID.

II. Background

A. History and Legal Authority

On February 28, 2024, the President issued E.O. 14117 entitled "Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern" (the "Order"), pursuant to his authority under the Constitution and laws of the United States, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), and section 301 of Title 3, United States Code. In the Order, the President expanded the scope of the national emergency declared in E.O. 13873 of May 15, 2019 "Securing the Information and Communications Technology and Services Supply Chain," and further addressed the national emergency with additional measures in E.O. 14034 of June 9, 2021, "Protecting Americans' Sensitive Data from Foreign Adversaries." Specifically, Section 2(a) of E.O. 14117 directs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, to issue, subject to public notice and comment, regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest ("transaction"), where the transaction: (i) involves bulk sensitive personal data or United States Government-related data, as defined by final rules implementing the Order; (ii) is a member of a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk sensitive personal data or United States Government-related data in a manner that contributes to the national emergency described in the Order; and (iii) meets other criteria specified by the Order.¹

Among other things, the E.O., at Section 2(c) instructs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the relevant agencies, to issue regulations identifying specific categories of transactions ("restricted transactions") that meet the criteria

described in (ii) above for which the Attorney General determines that security requirements, to be established by the Secretary of Homeland Security through the Director of CISA in accordance with Section 2(d) of the Order, adequately mitigate the risks of access by countries of concern or covered persons² to bulk sensitive personal data or United States Government-related data. In turn, Section 2(d) directs the Secretary of Homeland Security, acting through the Director of CISA, to propose, seek public comment on, and publish those security requirements, and Section 2(e) delegates to the Secretary of Homeland Security the President's powers under IEPPA as necessary to carry out Section 2(d).

On March 5, 2024, DOJ published an advance notice of proposed rulemaking (ANPRM) explaining a proposed framework that DOJ is considering for its forthcoming rules that would regulate certain data transactions involving bulk U.S. sensitive personal data and government-related data, as DOJ proposed to define these terms in the ANPRM. 89 FR 15780. The ANPRM states that DOJ is considering identifying three classes of restricted data transactions to address critical risk areas to the extent they involve countries of concern or covered persons and bulk U.S. sensitive personal data: vendor agreements; employment agreements; and investment agreements. 89 FR 15783. If implemented as described, such categories of transactions would be restricted, and otherwise prohibited unless they meet the security requirements developed by DHS in coordination with DOJ. *See* 89 FR 15788. The ANPRM includes an outline of what the security requirements might entail. 89 FR 15795. Through the ANPRM, DOJ also proposes a framework for enforcement of its regulations. *See* 89 FR 15797–15798.

DOJ is issuing a notice of proposed rulemaking (NPRM), Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, [DOJ Docket No. NSD–104, RIN 1124–AA01], in the proposed rule section of this issue of the **Federal Register** for public comment. Through this notice, CISA announces the proposed security requirements applicable to the classes of restricted transactions defined in DOJ's

¹ The other criteria do not directly impact the development of the security requirements but are related to DOJ's implementation of the E.O.'s directive via their regulations. *See* E.O. 14117, sec. 2(a)(iii)–(v), 89 FR 15421, 15423 (Mar. 1, 2024).

² Section 2(c)(iii) of the Order requires the Attorney General to identify, with the concurrence of the Secretaries of State and Commerce, countries of concern and, as appropriate, classes of covered persons for the purposes of the Order.

NPRM and requests public comment on the content of the security requirements.

B. Purpose and Structure of Proposed Security Requirements

The primary goal of the proposed security requirements is to address national-security and foreign-policy threats that arise when countries of concern³ and covered persons access bulk U.S. sensitive personal data or U.S. government-related data that may be implicated by the categories of restricted transactions. As explained in E.O. 14117, unrestricted transfers of Americans' bulk sensitive personal data and U.S. government-related data to countries of concern present a range of threats to national security and foreign policy. See 89 FR 15421. Access to bulk sensitive personal data and government-related data can allow countries of concern to engage in malicious cyber-enabled activities and malign foreign influence. See 89 FR 15422. With access to such data, countries of concern can track and build profiles on U.S. individuals, including members of the military and Federal employees and contractors, for illicit purposes such as blackmail and espionage. *Id.* Countries of concern can also use access to this data to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities to intimidate them; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties. *Id.* In making this assessment, DOJ noted that the Office of the Director of National Intelligence (ODNI) has assessed that adversaries view data, including personally identifiable information on U.S. citizens, "as a strategic resource" to increase the effectiveness of their espionage, influence, kinetic, and cyber-attack operations and provide a strategic advantage over the United States. See *id.* (citing Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* at 26 (Feb. 6, 2023), <https://perma.cc/4B2Y-7NVD>). DOJ assessed that advanced technologies, including big-data analytics, artificial intelligence, and high-performance computing, increase the ability of countries of concern to analyze and manipulate large tranches of data to more effectively target, influence, and coerce people in the

United States. See 89 FR 15781 and E.O. 14117.

The proposed security requirements are designed to mitigate the risk of sharing bulk U.S. sensitive personal data or U.S. government-related data with countries of concern or covered persons through restricted transactions.⁴ They do this by imposing conditions specifically on the *covered data* that may be shared as part of a restricted transaction, on the *covered systems* more broadly (both terms CISA is proposing to define within the security requirements), and on the organization as a whole. While the proposed requirements on covered systems and on an organization's governance of those systems apply more broadly than to the data at issue and the restricted transaction itself, CISA assesses that implementation of these requirements is necessary to validate that the organization has the technical capability and sufficient governance structure to appropriately select, successfully implement, and continue to apply the proposed covered data-level security requirements in a way that addresses the risks identified by DOJ for the restricted transactions. For example, to ensure and validate that a covered system denies covered persons access to covered data, it is necessary to maintain audit logs of accesses as well as organizational processes to utilize those logs. Similarly, it is necessary for an organization to develop identity management processes and systems to establish an understanding of which persons may have access to different data sets.

In addition to proposed requirements on covered systems, applying security requirements on the covered data itself that may be accessed in a restricted transaction is also necessary to address the risks. The specific requirements that are most technologically and logistically appropriate for different types of

restricted transactions may vary. For example, some transactions may be amenable to approaches that minimize data or process it in such a way that does not reveal covered data to covered persons. In other cases, techniques such as access control and encryption may be more appropriate to deny any access by covered persons to covered data. The proposed security requirements contemplate multiple options to minimize the risk to covered data, though all the options build upon the foundation of the proposed requirements imposed on covered systems and the organization as a whole. While CISA is proposing that U.S. persons⁵ engaging in restricted transactions must implement all the organizational and covered-system level requirements, CISA proposes that such persons will have some flexibility to determine which combination of data-level requirements are sufficient to fully and effectively prevent access to covered data by covered persons and/or countries of concern, based on the nature of the transaction and the data at issue.

The proposed security requirements are divided into two sections: organizational and covered system-level requirements (Section I) and covered data-level requirements (Section II). The listed requirements were selected with the intent of directly mitigating the risk of access to covered data, with additional requirements included to ensure effective governance of that access, as well as approaches for establishing an auditable basis for compliance purposes. Requirements that directly mitigate the risk of access include I.B.1–2, I.B.4–6, and all data-level requirements (II.A.1–3, II.B.1–3, II.C, and II.D). Requirements included as a mechanism for ensuring proper implementation and governance of those access controls include I.A.1–7. Additional requirements incorporated as a mechanism for ensuring auditable compliance of the aforementioned access controls include I.B.3 and I.C. These proposed requirements reflect a minimum set of practices that CISA believes are required for effective data

³ Terms used in CISA's proposed security requirements that are defined in the DOJ rulemaking have the same meaning in the proposed security requirements as provided in the DOJ rulemaking.

⁴ CISA notes that the proposed security requirements are, as required by the E.O., designed to "address the unacceptable risk posed by restricted transactions, as identified by the Attorney General." E.O. 14117 Sec. 2(d). They are not intended to reflect a comprehensive cybersecurity program. For example, several areas addressed in CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), available at <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>, are not reflected in the proposed data security requirements, even though the CPGs themselves are a common set of protections that CISA recommends all critical infrastructure entities voluntarily implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. As the operational lead for federal cybersecurity and national coordinator for critical infrastructure security and resilience, CISA recommends that all U.S. persons implement cybersecurity best practices in light of the risk and potential consequence of cyber events.

⁵ As noted above, for the purposes of the proposed security requirements, to the extent CISA uses a term that is proposed to be defined in the DOJ rulemaking, CISA proposes to use that definition. Therefore, CISA is using the term U.S. persons as proposed to be defined by the DOJ [A]NPRM. That definition reads "any United States citizen, national, or lawful permanent resident; or any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; or any *entity* organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any *person* in the United States." 89 FR 15788 and proposed 28 CFR 202.257.

protection, as informed by CISA's operational experience. Through this notice, CISA seeks additional input based on the experience industry stakeholders. These requirements have been designed to be representative of broadly accepted industry best practices and are intended to address the needs of national security without imposing an unachievable burden on industry.

As directed by E.O. 14117, the proposed security requirements are based on National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF), and the NIST Privacy Framework (PF). 89 FR 15424. See NIST, Cybersecurity Framework ver. 2.0, available at <https://www.nist.gov/cyberframework>, and NIST, Privacy Framework ver. 1.0, available at <https://www.nist.gov/privacy-framework>. CISA has also leveraged existing performance goals, guidance, practices, and controls, including the CISA Cross-Sector Cybersecurity Performance Goals (CPGs), which are themselves based on the NIST CSF and PF. CISA, Cross-Sector Cybersecurity Performance Goals, available at <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>. By leveraging existing performance goals, guidance, practices, and controls, CISA hopes to mitigate the burden of understanding and implementing the security requirements where necessary. In the proposed security requirements, CISA included parentheticals noting the specific NIST CSF and PF provisions upon which the proposed security requirements are based. CISA is seeking additional public comment on these references.

The DOJ NPRM proposes to require, consistent with E.O. 14117, that United States persons engaging in restricted transactions must comply with the final security requirements by incorporating the standards by reference.

Finally, the proposed security requirements include a definitions section. To the extent the proposed requirements use a term already proposed to be defined in the DOJ rulemaking, CISA's use of that term in the proposed security requirement would carry the same meaning. For the purpose of these proposed security requirements, CISA proposes to include definitions for six terms used exclusively in the proposed security requirements:

- **Asset.** CISA proposes to define the term to mean data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes. This proposed definition is derived from the CSF NIST CSF version 1.1, which defined asset as “[t]he data, personnel, devices, systems, and

facilities that enable the organization to achieve business purposes.”

- **Covered data.** CISA proposes to define the term to mean the two categories of data identified by the E.O. and that DOJ is proposing to regulate—bulk U.S. sensitive personal data or government-related data.

- **Information system.** CISA proposes to define this term consistent with the definition in the Paperwork Reduction Act (PRA), 44 U.S.C. 3502.⁶ The term would mean a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- **Covered system.** CISA proposes to define this term as a specific type of information system that is used to conduct a number of activities related to covered data as part of a restricted transaction. These activities are drawn from a combination of the activities in the proposed definition of *information system* in the proposed security requirements and the activities in the DOJ ANPRM's proposed definition of *access*. See 89 FR 15788; proposed 28 CFR 202.201. The term would mean an information system used to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, view, receive, collect, process, maintain, use, share, disseminate, or dispose of covered data as part of a restricted transaction, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified.

- **Network.** CISA proposes to define this term, which CISA developed consistent with the definition of the term in NIST Special Publication 800–171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. The term would mean a system of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

⁶ 6 U.S.C. 650(14) (which applies to all of Title XXII of the Homeland Security Act of 2002, which, in turn, contains most of CISA's authorities) defines Information System as having the meaning given the term in the Paperwork Reduction Act, 44 U.S.C. 3502, and specifically includes “industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.” 6 U.S.C. 650(14). However, given CISA's assumption that this type of operational technology is unlikely to be implicated by DOJ's proposed regulations, CISA is not proposing to include the operational technology-related prong here. CISA welcomes comments on this assumption.

III. Request for Public Input

A. Importance of Public Feedback

CISA is committed to seeking and incorporating public input into its approach to the development and content of the security requirements required by E.O. 14117. The proposed security requirements are available for review on CISA's website by visiting <https://www.cisa.gov> and searching for “Proposed Security Requirements for Restricted Transactions.” A copy of the proposed security requirements is also included in the docket for this notice and request for comment, docket number CISA–2024–0029. Below is a list of questions regarding the proposed security requirements for which CISA believes feedback could be particularly useful. CISA seeks a balanced approach to development of the security requirements, which would mitigate the risks of access to Americans' bulk sensitive personal data or government-related data by countries of concern while accounting for the impact that adopting these measures may have on those entities that would implement them. CISA encourages public comment on these topics and any other topics that commenters believe may be useful to CISA in the development of the forthcoming security requirements. The type of feedback that is most useful to the agency will identify specific approaches that CISA may want to consider and provide information supporting why the approach would foster a cost-effective and balanced approach. As discussed in more detail below, commenters may want to consider submitting views on organizational- and system-level requirements and/or data-level requirements. Feedback that contains specific information, data, or recommendations is more useful to CISA than generic feedback that omits these components. For comments that contain any numerical estimates, CISA encourages the commenter to provide any assumptions made in calculating the numerical estimates.

B. List of Questions for Commenters

Below is a non-exhaustive list of questions that are meant to assist members of the public in formulating their comments in response to this notice. The list of questions is not intended to restrict the issues that commenters may address. For more information on the proposed regulatory structure in which the security requirements will apply, please review DOJ's NPRM, Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related

Data by Countries of Concern or Covered Persons, [DOJ Docket No. NSD–104, RIN 1124–AA01], published in today's proposed rule section of the **Federal Register** for public comment.

1. Are the proposed security requirements sufficiently robust to mitigate the risks of access to Americans' bulk sensitive personal data or government-related data by countries of concern?

2. Are the proposed organizational- and system-level requirements sufficient to provide U.S. persons engaging in restricted transactions confidence that logical and physical access to covered data is sufficiently managed to deny access to covered persons or countries of concern?

3. Do the security requirements provide sufficient flexibility, clarity, and specificity for the types of restricted transactions typically engaged in by U.S. entities, including to avoid overly burdening commercial activity not involving covered data while providing sufficient level of detail to aid in compliance verification?

4. Are there other data-level requirements (beyond those listed in Section II of the proposed security requirements) that CISA should consider that would enable U.S. entities to engage in commercial transactions without revealing covered data to covered persons or countries of concern?

5. The current approach allows for flexibility to determine which data-level requirements are sufficient to fully and effectively prevent access to covered data by covered persons and/or countries of concern. Are there data-level requirements that CISA should consider requiring in all cases?

6. What additional interpretive guidance would be helpful to U.S. entities in determining which data-level requirements should be applied based on the nature of the transaction and the data at issue?

7. What substantive requirements should CISA consider in Section II.C. to further define appropriate privacy-enhancing technologies that may be used within restricted transactions?

8. Should the standards for data aggregation in Section II.A differ from the proposed definition of bulk in the DOJ regulations? If so, are there requirements CISA should impose for U.S. persons engaged in restricted transactions to ensure that covered data is not re-constructable through aggregation while permitting more granular thresholds?

9. Are there additional substantive standards that should be added to the data-level requirements in Section II to

better ensure their implementation can achieve the policy goal of not permitting access to covered data by covered persons or countries of concern?

10. To what extent could the measures described currently be reversed, broken, or circumvented by a technologically sophisticated actor? Are there additional conditions that would better or more appropriately mitigate this risk? If so, please describe them in detail.

11. To what extent could the measures described be rendered reversible, breakable, or able to be circumvented by anticipated future technology advances? What type of future technology advances would pose the greatest risk to these types of protective measures?

12. Would it be useful to the entities likely to undertake restricted transactions if CISA mapped these requirements to ISO–27001 or example controls from NIST Special Publication 800–171 (e.g., to facilitate compliance audits)?

Jennie M. Easterly,

Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2024–24709 Filed 10–22–24; 4:15 pm]

BILLING CODE 9111–11F–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

**[FWS–HQ–MB–2024–N056;
FXMB1231099BPP0–256–FF09M22000;
OMB Control Number 1018–0067]**

Agency Information Collection Activities; Submission to the Office of Management and Budget; Approval Procedures for Nontoxic Shot and Shot Coatings

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of information collection; request for comment.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, we, the U.S. Fish and Wildlife Service (Service), are proposing to renew an information collection without change.

DATES: Interested persons are invited to submit comments on or before November 29, 2024.

ADDRESSES: Written comments and recommendations for the proposed information collection should be submitted within 30 days of publication of this notice at <https://www.reginfo.gov/public/do/PRAMain>. Find this particular information

collection by selecting “Currently under Review—Open for Public Comments” or by using the search function. Please provide a copy of your comments to the Service Information Collection Clearance Officer, U.S. Fish and Wildlife Service, MS: PRB (JAO/3W), 5275 Leesburg Pike, Falls Church, VA 22041–3803 (mail); or by email to Info_Coll@fws.gov. Please reference “1018–0067” in the subject line of your comments.

FOR FURTHER INFORMATION CONTACT:

Madonna L. Baucum, Service Information Collection Clearance Officer, by email at Info_Coll@fws.gov, or by telephone at (703) 358–2503. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

SUPPLEMENTARY INFORMATION:

In accordance with the Paperwork Reduction Act (PRA; 44 U.S.C. 3501 *et seq.*) and its implementing regulations at 5 CFR 1320, all information collections require approval under the PRA. We may not conduct or sponsor and you are not required to respond to a collection of information unless it displays a currently valid OMB control number.

As part of our continuing effort to reduce paperwork and respondent burdens, we invite the public and other Federal agencies to comment on new, proposed, revised, and continuing collections of information. This helps us assess the impact of our information collection requirements and minimize the public's reporting burden. It also helps the public understand our information collection requirements and provide the requested data in the desired format.

On August 7, 2024, we published in the **Federal Register** (89 FR 64476) a notice of our intent to request that OMB renew this information collection. In that notice, we solicited comments for 60 days, ending on October 7, 2024. In a continued effort to increase public awareness of, and participation in, our public commenting processes associated with information collection requests, the Service also published the **Federal Register** notice on [Regulations.gov](https://www.regulations.gov) (Docket No. FWS–HQ–MB–2024–0093) to provide the public with an additional method to submit comments (in addition to the typical U.S. mail submission method). We received an

anonymous comment in response to that notice which did not address the information collection requirements; therefore, no response is required.

We are especially interested in public comment addressing the following:

(1) Whether or not the collection of information is necessary for the proper performance of the functions of the agency, including whether or not the information will have practical utility;

(2) The accuracy of our estimate of the burden for this collection of information, including the validity of the methodology and assumptions used;

(3) Ways to enhance the quality, utility, and clarity of the information to be collected; and

(4) How might the agency minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of response.

Comments that you submit in response to this notice are a matter of public record. We will include or summarize each comment in our request to OMB to approve this ICR. Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment—including your personal identifying information—may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Abstract: The Migratory Bird Treaty Act (MBTA; 16 U.S.C. 703 *et seq.*) prohibits the unauthorized take of migratory birds and authorizes the Secretary of the Interior to regulate take of migratory birds in the United States. Under this authority, we control the hunting of migratory game birds through regulations in 50 CFR part 20. On January 1, 1991, we banned lead shot for hunting waterfowl and coots in the United States.

This is a non-form collection. Regulations at 50 CFR 20.134 outline the application and approval process for new types of nontoxic shot. When considering approval of a candidate material as nontoxic, we must ensure that it is not hazardous in the environment and that secondary exposure (ingestion of spent shot or its components) is not a hazard to migratory birds. To make that decision, we require each applicant to provide information about the solubility and

toxicity of the candidate material. Additionally, for law enforcement purposes, a noninvasive field detection device must be available to distinguish candidate shot from lead shot. This information constitutes the bulk of an application for approval of nontoxic shot. The Director uses the data in the application to decide whether to approve a material as nontoxic.

Title of Collection: Approval Procedures for Nontoxic Shot and Shot Coatings (50 CFR 20.134).

OMB Control Number: 1018–0067.

Form Number: None.

Type of Review: Extension of a currently approved collection.

Respondents/Affected Public: Businesses that produce and/or market approved nontoxic shot types or nontoxic shot coatings.

Total Estimated Number of Annual Respondents: 1.

Total Estimated Number of Annual Responses: 1.

Estimated Completion Time per Response: 3,200 hours.

Total Estimated Number of Annual Burden Hours: 3,200 hours.

Respondent's Obligation: Required to obtain or retain a benefit.

Frequency of Collection: On occasion.

Total Estimated Annual Nonhour Burden Cost: \$26,630 (\$1,630 application processing fee and \$25,000 for solubility testing).

An agency may not conduct or sponsor and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number.

The authority for this action is the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*).

Madonna Baucum,

Information Collection Clearance Officer, U.S. Fish and Wildlife Service.

[FR Doc. 2024–25112 Filed 10–28–24; 8:45 am]

BILLING CODE 4333–15–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

[FWS–R5–ES–2024–0039;
FXES11140500000–245–FF05E00000]

Proposed Multi-Bat Species General Conservation Plan for Routine Development Projects in New York, Pennsylvania, and West Virginia; Draft Environmental Assessment

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of availability; request for comments.

SUMMARY: We, the U.S. Fish and Wildlife Service (Service), announce the

availability for public comment of a proposed general conservation plan (GCP), as well as an associated draft environmental assessment, for routine development projects in New York, Pennsylvania, and West Virginia that impact the federally listed Indiana bat (*Myotis sodalis*) and/or northern long-eared bat (*Myotis septentrionalis*), and/or the proposed to be listed tricolored bat (*Perimyotis subflavus*). We invite comments from the public and local, State, Tribal, and Federal agencies.

DATES: We will accept comments received or postmarked on or before November 29, 2024. Comments submitted online at <https://www.regulations.gov> (see **ADDRESSES**) must be received by 11:59 p.m. eastern time on November 29, 2024.

ADDRESSES:

Obtaining documents: The documents this notice announces, as well as any comments and other materials that we receive, will be available for public inspection online in Docket No. FWS–R5–ES–2024–0039 at <https://www.regulations.gov>.

Submitting comments: If you wish to submit comments on any of the documents, you may do so in writing by one of the following methods:

- **Online:** <https://www.regulations.gov>. Follow the instructions for submitting comments on Docket No. FWS–R5–ES–2024–0039.

- **U.S. Mail:** Public Comments Processing; Attn: Docket No. FWS–R5–ES–2024–0039; U.S. Fish and Wildlife Service Headquarters, MS: PRB/3W; 5275 Leesburg Pike, Falls Church, VA 22041–3803.

We will post all comments on <https://www.regulations.gov>. This generally means that we will post any personal information you provide us (see Public Availability of Comments under **SUPPLEMENTARY INFORMATION** for more information).

FOR FURTHER INFORMATION CONTACT: Eric Tattersall, by telephone at 413–253–8630. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

SUPPLEMENTARY INFORMATION: We, the U.S. Fish and Wildlife Service (Service), announce the availability of a proposed general conservation plan (GCP), as well as an associated draft environmental assessment (EA), for routine development projects in New York,

Pennsylvania, and West Virginia that may impact Indiana bat (*Myotis sodalis*), northern long-eared bat (*Myotis septentrionalis*), and/or tricolored bat (*Perimyotis subflavus*). We invite comments from the public and local, State, Tribal, and Federal agencies.

We developed and now make available the GCP to provide a streamlined mechanism to assist future individual applicants engaged in certain otherwise lawful routine development projects to meet statutory and regulatory requirements of a habitat conservation plan for issuance of an incidental take permit under section 10(a)(1)(B) of the Endangered Species Act of 1973, as amended (ESA; 16 U.S.C. 1531 *et seq.*), while promoting conservation of the Indiana bat (*Myotis sodalis*), the northern long-eared bat (*Myotis septentrionalis*), and the tricolored bat (*Perimyotis subflavus*). The GCP includes measures to minimize and mitigate impacts to the covered species. Permits issued under the GCP would authorize incidental take of the covered species for up to 15 years after the GCP becomes effective. We developed the GCP in accordance with section 10(a)(2)(A) of the ESA (16 U.S.C. 1531 *et seq.*).

We prepared the draft EA in accordance with the National Environmental Policy Act of 1969 (NEPA; 42 U.S.C. 4321 *et seq.*) to evaluate the potential effects to the natural and human environment resulting from issuing permits under the GCP.

Background

Section 9 of the ESA and its implementing regulations prohibit the “take” of animal species listed as endangered or threatened. Take is defined under the ESA as to “harass, harm, pursue, hunt, shoot, wound, kill, trap, capture, or collect, or to attempt to engage in any such conduct” (16 U.S.C. 1532). However, under section 10(a)(1)(B) of the ESA, we may issue permits to authorize take of listed species that is incidental to, and not the purpose of, carrying out an otherwise lawful activity (*i.e.*, “incidental taking” (50 CFR 17.3)). Regulations governing permits for the incidental taking of endangered and threatened species, respectively, are found in the Code of Federal Regulations at 50 CFR 17.22 and 50 CFR 17.32.

Proposed Action

The proposed action is approval of the GCP that has been prepared by the Service in accordance with section 10(a)(2)(A) of the ESA to provide a more efficient and standardized mechanism for proponents engaged in certain otherwise lawful routine development projects on non-Federal lands. The proposed GCP describes the routine development activities for which the plan establishes associated conservation measures an applicant would agree to undertake first to avoid and then to minimize and mitigate for the impacts of the incidental take of the listed (and proposed) bat species to the maximum extent practicable, and to ensure that incidental take will not appreciably

reduce the likelihood of the survival and recovery of these species in the wild. The GCP would allow private individuals, local and State agencies, and other non-Federal entities to meet the statutory and regulatory requirements of the ESA by applying for a permit and complying with the requirements of the GCP, including all applicable avoidance, minimization, and mitigation actions. We propose that applications for projects falling within the GCP and which adopt all applicable plan requirements would meet the permit issuance criteria as required by section 10(a)(2)(B) of the ESA, thereby enabling the establishment of a programmatic permitting and conservation process to address a defined suite of project types impacting defined listed species within a defined planning area. The GCP would be available for adoption and use by eligible applicants for a period of 10 years. Individual permits issued through the streamlined GCP process may be authorized for a term of up to 5 years. Therefore, permittees would have up to 5 years to complete their projects, even if the permit is issued in the final year (*i.e.*, year 10) of the GCP. If a project proponent is unable to complete their covered activities during the duration of their permit, they can request a permit renewal (for up to 5 additional years) from the Service.

Covered Species

The proposed GCP would cover the bat species in table 1.

TABLE 1—BAT SPECIES COVERED IN THE PROPOSED GENERAL CONSERVATION PLAN

Common name	Scientific name	Federal listing status
Indiana bat	<i>Myotis sodalis</i>	Endangered.
Northern long-eared bat	<i>Myotis septentrionalis</i>	Endangered.
Tricolored bat	<i>Perimyotis subflavus</i>	Proposed endangered.

National Environmental Policy Act Compliance

The draft EA provides the required NEPA documentation for the proposed Federal action (approval of a conservation plan and subsequent issuance of permits pursuant to section 10(a)(1)(B) of the ESA), providing information on the environmental baseline and a discussion of impacts to the human and natural environment that may occur as a result of implementation of the GCP. Importantly, the scope of the EA is limited to evaluation of the proposed GCP as a mechanism to standardize permit issuance for covered activities;

this EA neither evaluates nor results in approval of the routine development activities. Land use approval(s) for individual projects would continue to be the responsibility of the local or State agency(ies) that have appropriate jurisdiction(s) over individual projects. A section 10(a)(1)(B) incidental take permit issued by the Service does not authorize the covered activities themselves; rather, it authorizes only the take of covered species resulting from those activities. We are also considering a no-action alternative to the proposed action in the EA. Under this no-action alternative, the Service would not approve the proposed GCP as a standardized mechanism for

compliance with section 10 of the ESA. Project proponents planning to conduct otherwise lawful routine development activities involving potential impacts to Indiana bat, northern long-eared bat, and/or tricolored bat would continue to develop project-specific HCPs in order to apply for and obtain permits authorizing those species to be taken.

Public Availability of Comments

All comments received, including names and addresses, will become part of the administrative record associated with this action. If you submit a comment via <https://www.regulations.gov>, your entire comment, including any personal

identifying information such as your address, phone number, and email address, will be posted on the website.

If you submit a hardcopy comment that includes personal identifying information, you may request at the top of your document that we withhold this information from public review. However, we cannot guarantee that we will be able to do so. We will post all hardcopy comments on <https://www.regulations.gov>.

Next Steps

The Service will evaluate the comments received to determine whether the GCP meets the requirements of section 10(a) of the ESA (16 U.S.C. 1531 *et seq.*). We will also conduct an intra-Service consultation pursuant to section 7 of the ESA to evaluate the effects of the proposed take. After considering the above findings, we will determine whether the permit issuance criteria of section 10(a)(1)(B) of the ESA have been met. If met, the Service will implement the GCP and issue ITPs to qualified applicants that agree to comply with all avoidance, minimization, and mitigation actions that apply to their proposed projects.

Authority

We provide this notice under section 10(c) of the ESA (16 U.S.C. 1531 *et seq.*) and its implementing regulations (50 CFR 17.22 and 17.32) and NEPA (42 U.S.C. 4321 *et seq.*) and its implementing regulations (40 CFR 1500–1508 and 43 CFR 46).

Sharon Marino,

Assistant Regional Director, Ecological Services, Northeast Region.

[FR Doc. 2024–25089 Filed 10–28–24; 8:45 am]

BILLING CODE 4333–15–P

DEPARTMENT OF THE INTERIOR

Bureau of Land Management

[BLM_NV_FRN_4500183156]

Notice of Availability of the Record of Decision for the Rhyolite Ridge Lithium-Boron Project, Esmeralda County, NV

AGENCY: Bureau of Land Management, Interior.

ACTION: Notice of availability.

SUMMARY: The Bureau of Land Management (BLM) announces the availability of the Record of Decision (ROD) for the Final Environmental Impact Statement (EIS) for the Rhyolite Ridge Lithium-Boron Project (Project) located in Esmeralda County, Nevada. The ROD constitutes the decision of the

BLM to approve the plan of operations for the Project.

DATES: The Acting Deputy Secretary of the Interior signed the ROD on October 24, 2024.

ADDRESSES: The ROD is available online at <https://eplanning.blm.gov/eplanning-ui/project/2012309/510>.

FOR FURTHER INFORMATION CONTACT:

Scott Distel, Project Manager, telephone (775) 635–4000; address 50 Bastian Road, Battle Mountain, NV 89820; email BLM_NV_BMDO_P&EC_NEPA@blm.gov. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services for contacting Mr. Distel. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

SUPPLEMENTARY INFORMATION: The authorized officer for this action has reviewed the environmental analysis in the Final EIS and has selected the North and South Overburden Storage Facility Alternative (Preferred Alternative/ Selected Alternative), along with the applicable Applicant-Committed Environmental Protection Measures (ACEPMs) specified in Sections 2.1.13 and 2.2.2 of the Final EIS. The BLM's selection is based on the environmental analysis in the Final EIS, which was published on September 20, 2024. There were no substantial changes to the Final EIS during the 30-day public availability period following publication. An errata sheet was issued following the Final EIS correcting Final EIS Page 4–41, fifth paragraph, line 8, from “approximately 100 feet” to “approximately 25 feet.”

The ROD approves the plan of operations for the Project (NVNV106205338) submitted to the BLM pursuant to 43 CFR 3809 and 3715, and the analysis in the Final EIS. The BLM has considered the analysis of the effectiveness of the mitigation measures, and has determined that implementation of the ROD, with the identified mitigation measures, will not cause unnecessary or undue degradation of the public lands and is consistent with applicable legal requirements.

In accordance with 40 CFR 1505.2(c), the mitigation measures and ACEPMs represent practicable means to avoid or minimize environmental harm from the BLM's Selected Alternative. The ACEPMs, which were developed to avoid or minimize environmental impacts resulting from the Selected Alternative, are part of the Plan. All ACEPMs were designed to avoid or

minimize environmental impacts to resources affected by the Plan. All mitigation within the BLM's authority will be implemented and enforced.

The ROD is conditioned on compliance with the Biological Opinion issued by the U.S. Fish and Wildlife Service (USFWS) provided in Appendix A of the ROD and all other necessary local, State, and Federal approvals, authorizations, and permits. Other agencies, including but not limited to Esmeralda County and USFWS, are responsible for issuing and enforcing their own decisions and applicable authorizations for the Project.

Approval of the Project constitutes the final decision of the Department of the Interior (DOI) and, in accordance with the regulations at 43 CFR 4.410(a)(3) and *Blue Star, Inc.*, 41 IBLA 333 (1979), is not subject to administrative appeal under DOI regulations at 43 CFR part 4.

(Authority: 40 CFR 1501.9)

Laura Daniel-Davis,

Acting Deputy Secretary of the Interior.

[FR Doc. 2024–25096 Filed 10–28–24; 8:45 am]

BILLING CODE 4331–21–P

DEPARTMENT OF THE INTERIOR

National Park Service

[NPS–WASO–NRNHL–DTS#–38984; PPWOCRADIO, PCU00RP14.R50000]

National Register of Historic Places; Notification of Pending Nominations and Related Actions

AGENCY: National Park Service, Interior.

ACTION: Notice.

SUMMARY: The National Park Service is soliciting electronic comments on the significance of properties nominated before October 19, 2024, for listing or related actions in the National Register of Historic Places.

DATES: Comments should be submitted electronically by November 13, 2024.

ADDRESSES: Comments are encouraged to be submitted electronically to *National Register Submissions@nps.gov* with the subject line “Public Comment on <property or proposed district name, (County) State>.” If you have no access to email, you may send them via U.S. Postal Service and all other carriers to the National Register of Historic Places, National Park Service, 1849 C Street NW, MS 7228, Washington, DC 20240.

FOR FURTHER INFORMATION CONTACT: Sherry A. Frear, Chief, National Register of Historic Places/National Historic Landmarks Program, 1849 C Street NW,

MS 7228, Washington, DC 20240,
sherry_frear@nps.gov, 202-913-3763.

SUPPLEMENTARY INFORMATION: The properties listed in this notice are being considered for listing or related actions in the National Register of Historic Places. Nominations for their consideration were received by the National Park Service before October 24, 2024. Pursuant to 36 CFR 60.13, comments are being accepted concerning the significance of the nominated properties under the National Register criteria for evaluation.

Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment—including your personal identifying information—may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Nominations submitted by State or Tribal Historic Preservation Officers

Key: State, County, Property Name, Multiple Name (if applicable), Address/Boundary, City, Vicinity, Reference Number.

COLORADO

Denver County

The Owl Club of Denver, 2815 Madison Street, Denver, SG100011062

Otero County

Manzanola United Methodist Church (MUMC), 115 Park Street, Manzanola, SG100011069

IOWA

Linn County

Luther A. and Elinore T. Brewer House, 616 10th Ave. SE, Cedar Rapids, SG100011084

Marshall County

Louis F. and Emma M. (Edler) Wohler House-Emma Wohler Maternity Home, 407 3rd Ave. NE, State Center, SG100011083

Polk County

Davidson Bros. Company Warehouse and Manufacturing Building, 108 SW 3rd Street, Des Moines, SG100011064

NEW YORK

Erie County

Sacred Heart Roman Catholic Church and Convent, 198 Emslie Street, Buffalo, SG100011076

Yeomans House, 866 East Main Street, East Aurora, SG100011077

New York County

Dominican Historic District, Roughly W. 155th St., Broadway, Dyckman St., Harlem River Drive, Manhattan, SG100011048

Gaylord White Houses, 209 Second Avenue, New York, SG100011075

Onondaga County

Montgomery Street-Columbus Circle Historic District (Boundary Increase and Decrease), E. Onondaga, E. Fayette, Harrison, S. State, Madison, S. Warren & Montgomery Sts., Syracuse, BC100011082

Ontario County

SENECA CHIEF (shipwreck), Address Restricted, Canandaigua, SG100011074

Richmond County

West Brighton Plaza, Generally, Henderson Ave., Broadway, Castleton Ave., and Alaska Ave., Staten Island, SG100011081

Ulster County

Kingston Barrel Factory, 35 Bruyn Avenue, Kingston, SG100011078

Westchester County

Sailing Vessel GITANA, New Rochelle Lower Harbor, New Rochelle, SG100011073

TENNESSEE

Bedford County

Rosenwald Recreation and Community Center, 516 Tillman St., Shelbyville, SG100011067

TEXAS

Hays County

Dunbar Historic District, Roughly bounded by South Fredericksburg Street, West Martin Luther King Drive, Herndon Street, and Centre Street, San Marcos, SG100011049

Wise County

Bridgeport Commercial Historic District, Halsell Street, roughly between 9th Street and 12th Street, Bridgeport, SG100011085

UTAH

Box Elder County

Spiral Jetty, North Shore of the Great Salt Lake, Corinne vicinity, SG100011066

WYOMING

Natrona County

Izaak Walton League of America, Charles E. Piersall Chapter, Clubhouse-Lodge, 4205 Fort Caspar Road, Mills, SG100011060

Teton County

John Clymer Residence, 7255 N. Rachel Way, Teton Village, SG100011059
Ellen G. Walker Shop, 81 S. King Street, Jackson, SG100011061
Coe Cabin, 85 S. King Street, Jackson, SG100011063

Additional documentation has been received for the following resource(s):

IOWA

Muscatine County

McKee Button Company (Additional Documentation), 1020 Hershey Ave., Muscatine, AD100005784

NEW YORK

Albany County

Center Square-Hudson-Park Historic District (Additional Documentation), Roughly bounded by Park Ave., State, Lark and S. Swan Sts., Albany, AD80002578

Tompkins County

Ithaca Downtown Historic District (Additional Documentation), E. and W. State, N. & S. Cayuga, N. Aurora, N. Tioga Sts., Ithaca, AD05000018

TENNESSEE

Anderson County

Edwards-Fowler House (Additional Documentation), 1062 Old Lake City Hwy, Rocky Top (formerly Lake City) vicinity, AD75001726

Bedford County

Gilliland, James, House (Additional Documentation), 803 Lipscomb St., Shelbyville, AD75001730

Hamblen County

Hamblen County Courthouse (Additional Documentation), 511 W. 2nd North St., Morristown, AD73001770

Hamilton County

Brown House (Additional Documentation), 9521 Ooltewah-Georgetown Rd., Ooltewah vicinity, AD73001781

Lawrence County

Lawrence County Jail (Additional Documentation), 233 Waterloo Street, Lawrenceburg, AD76001784

Loudon County

Bowman House (Additional Documentation), At the end of Tanasi Court, Loudon vicinity, AD70000610

Montgomery County

Sevier Station (Additional Documentation), 326 Walker Street, Clarksville, AD71000827

Rutherford County

Collier-Crichlow House (Additional Documentation), 511 E. Main St., Murfreesboro, AD73001822
Palmer, Gen. Joseph B., House (Additional Documentation), 434 E. Main St., Murfreesboro, AD73001825

Scott County

Old Scott County Jail (Additional Documentation), 214 Litton Covered Bridge Road, Huntsville, AD74001927

Sullivan County

Alison, Finlay, House (Additional Documentation), 1334 N. Pickens Bridge Road, Piney Flats vicinity, AD73001851

Wilson County

Pickett Chapel Methodist Church (Additional Documentation), 209 E. Market Street, Lebanon, AD77001302

Authority: 36 CFR 60.13

Sherry A. Frear,

Chief, National Register of Historic Places/
National Historic Landmarks Program.

[FR Doc. 2024–25045 Filed 10–28–24; 8:45 am]

BILLING CODE P

DEPARTMENT OF THE INTERIOR

Bureau of Safety and Environmental Enforcement

[Docket ID BSEE–2024–0003; EEEE500000
254E1700D2 ET1SF0000.EAQ000; OMB
Control Number 1014–0023]

Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Pollution Prevention and Control

AGENCY: Bureau of Safety and
Environmental Enforcement, Interior.

ACTION: Notice of information collection;
request for comment.

SUMMARY: In accordance with the
Paperwork Reduction Act (PRA) of
1995, the Bureau of Safety and
Environmental Enforcement (BSEE)
proposes to renew an information
collection with revisions.

DATES: Interested persons are invited to
submit comments on or before
November 29, 2024.

ADDRESSES: Written comments and
recommendations for the proposed
information collection should be sent
within 30 days of publication of this
notice to [www.reginfo.gov/public/do/](http://www.reginfo.gov/public/do/PRAMain)
PRAMain. Find this particular
information collection by selecting
“Currently under 30-day Review—Open
for Public Comments” or by using the
search function. Please provide a copy
of your comments to Nikki Mason, BSEE
ICCO, 45600 Woodland Road, Sterling,
VA 20166; or by email to [nikki.mason@](mailto:nikki.mason@bsee.gov)
bsee.gov. Please reference OMB Control
Number 1014–0023 in the subject line of
your comments.

FOR FURTHER INFORMATION CONTACT: To
request additional information about
this ICR, contact Nikki Mason by email
at nikki.mason@bsee.gov or by
telephone at (703) 787–1607.
Individuals in the United States who are
deaf, deafblind, hard of hearing, or have
a speech disability may dial 711 (TTY,
TDD, or TeleBraille) to access
telecommunications relay services.
Individuals outside the United States
should use the relay services offered
within their country to make
international calls to the point-of-
contact in the United States. You may

also view the ICR at [http://](http://www.reginfo.gov/public/do/PRAMain)
www.reginfo.gov/public/do/PRAMain.

SUPPLEMENTARY INFORMATION: In
accordance with the PRA and 5 CFR
1320.8(d)(1), we provide the general
public and other Federal agencies with
an opportunity to comment on new,
proposed, revised, and continuing
collections of information. This helps us
assess the impact of our information
collection requirements and minimize
the public’s reporting burden. It also
helps the public understand our
information collection requirements and
provide the requested data in the
desired format.

A Federal Register notice with a 60-
day public comment period soliciting
comments on this collection of
information was published on July 12,
2024 (89 FR 57165). No comments were
received.

As part of our continuing effort to
reduce paperwork and respondent
burdens, we are again soliciting
comments from the public and other
Federal agencies on the proposed ICR
that is described below. We are
especially interested in public comment
addressing the following:

- (1) Whether or not the collection of
information is necessary for the proper
performance of the functions of the
agency, including whether or not the
information will have practical utility;
- (2) The accuracy of our estimate of the
burden for this collection of
information, including the validity of
the methodology and assumptions used;
- (3) Ways to enhance the quality,
utility, and clarity of the information to
be collected; and
- (4) How might the agency minimize
the burden of the collection of
information on those who are to
respond, including through the use of
appropriate automated, electronic,
mechanical, or other technological
collection techniques or other forms of
information technology, e.g., permitting
electronic submission of response.

Comments that you submit in
response to this notice are a matter of
public record. Before including your
address, phone number, email address,
or other personal identifying
information in your comment, you
should be aware that your entire
comment—including your personal
identifying information—may be made
publicly available at any time. While
you can ask us in your comment to
withhold your personal identifying
information from public review, we
cannot guarantee that we will be able to
do so.

Abstract: This authority and
responsibility are among those

delegated to BSEE. The regulations at 30
CFR 250, subpart C requirements
concern pollution prevention and
control and are the subject of this
collection. This request also covers any
related Notices to Lessees and Operators
(NLTs) that BSEE issues to clarify,
supplement, or provide additional
guidance on some aspects of our
regulations.

The information collected under
Subpart C is used in our efforts to:

- record the location of items lost
overboard to aid in recovery during site
clearance activities on the lease;
- conduct operations according to all
applicable regulations, requirements,
and in a safe and workmanlike manner;
- properly handle for the protection
of OCS workers and the environment
the discharge or disposal of drill
cuttings, sand, and other well solids,
including those containing naturally
occurring radioactive materials (NORM);
and
- inspect facilities daily for the
prevention of pollution and ensure that
any observed problems are corrected.

Title of Collection: 30 CFR part 250,
subpart C, Pollution Prevention and
Control.

OMB Control Number: 1014–0023.

Form Number: None.

Type of Review: Revision of a
currently approved collection.

Respondents/Affected Public:
Potential respondents include Federal
OCS oil, gas, and sulfur lessees and/or
operators and holders of pipeline rights-
of-way.

**Total Estimated Number of Annual
Respondents:** Currently there are
approximately 555 Federal OCS oil, gas,
and sulfur lessees and holders of
pipeline rights-of-way. Not all the
potential respondents will submit
information in any given year, and some
may submit multiple times.

**Total Estimated Number of Annual
Responses:** 3,168.

**Estimated Completion Time per
Response:** Varies from 1 hour to 134
hours, depending on activity.

**Total Estimated Number of Annual
Burden Hours:** 137,835.

Respondent’s Obligation: Responses
are mandatory.

Frequency of Collection: Submissions
are generally on occasion, weekly, and
daily.

**Total Estimated Annual Nonhour
Burden Cost:** None.

An agency may not conduct, or
sponsor and a person is not required to
respond to a collection of information
unless it displays a currently valid OMB
control number.

The authority for this action is the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*).

Kirk Malstrom,

Chief, Regulations and Standards Branch.

[FR Doc. 2024–25074 Filed 10–28–24; 8:45 am]

BILLING CODE 4310–VH–P

INTERNATIONAL TRADE COMMISSION

[Investigation Nos. 701–TA–453 and 731–TA–1136–1137 (Third Review)]

Sodium Nitrite From China and Germany; Scheduling of Expedited Five-Year Reviews

AGENCY: United States International Trade Commission.

ACTION: Notice.

SUMMARY: The Commission hereby gives notice of the scheduling of expedited reviews pursuant to the Tariff Act of 1930 (“the Act”) to determine whether revocation of the antidumping and countervailing duty orders on sodium nitrite from China and the antidumping duty order on sodium nitrite from Germany would be likely to lead to continuation or recurrence of material injury within a reasonably foreseeable time.

DATES: October 4, 2024.

FOR FURTHER INFORMATION CONTACT: Rachel Devenney (202–205–3172), Office of Investigations, U.S. International Trade Commission, 500 E Street SW, Washington, DC 20436. Hearing-impaired persons can obtain information on this matter by contacting the Commission’s TDD terminal on 202–205–1810. Persons with mobility impairments who will need special assistance in gaining access to the Commission should contact the Office of the Secretary at 202–205–2000. General information concerning the Commission may also be obtained by accessing its internet server (<https://www.usitc.gov>). The public record for this proceeding may be viewed on the Commission’s electronic docket (EDIS) at <https://edis.usitc.gov>.

SUPPLEMENTARY INFORMATION:

Background.—On October 4, 2024, the Commission determined that the domestic interested party group response to its notice of institution (89 FR 54536, July 1, 2024) of the subject five-year reviews was adequate and that the respondent interested party group response was inadequate. The Commission did not find any other circumstances that would warrant

conducting full reviews.¹ Accordingly, the Commission determined that it would conduct expedited reviews pursuant to section 751(c)(3) of the Act (19 U.S.C. 1675(c)(3)).²

For further information concerning the conduct of these reviews and rules of general application, consult the Commission’s Rules of Practice and Procedure, part 201, subparts A and B (19 CFR part 201), and part 207, subparts A, D, E, and F (19 CFR part 207).

Staff report.—A staff report containing information concerning the subject matter of the reviews has been placed in the nonpublic record, and will be made available to persons on the Administrative Protective Order service list for these reviews on December 30, 2024. A public version will be issued thereafter, pursuant to § 207.62(d)(4) of the Commission’s rules.

Written submissions.—As provided in § 207.62(d) of the Commission’s rules, interested parties that are parties to the reviews and that have provided individually adequate responses to the notice of institution,³ and any party other than an interested party to the reviews may file written comments with the Secretary on what determinations the Commission should reach in the reviews. Comments are due on or before 5:15 p.m. on January 8, 2025 and may not contain new factual information. Any person that is neither a party to the five-year reviews nor an interested party may submit a brief written statement (which shall not contain any new factual information) pertinent to the reviews by January 8, 2025. However, should the Department of Commerce (“Commerce”) extend the time limit for its completion of the final results of its reviews, the deadline for comments (which may not contain new factual information) on Commerce’s final results is three business days after the issuance of Commerce’s results. If comments contain business proprietary information (BPI), they must conform with the requirements of §§ 201.6, 207.3, and 207.7 of the Commission’s rules. The Commission’s *Handbook on Filing Procedures*, available on the Commission’s website at https://www.usitc.gov/documents/handbook_

¹ A record of the Commissioners’ votes, the Commission’s statement on adequacy, and any individual Commissioner’s statements will be available from the Office of the Secretary and at the Commission’s website.

² Commissioner David S. Johanson voted to conduct full reviews.

³ The Commission has found the response submitted on behalf of Chemtrade Chemicals US LLC to be individually adequate. Comments from other interested parties will not be accepted (*see* 19 CFR 207.62(d)(2)).

on filing procedures.pdf, elaborates upon the Commission’s procedures with respect to filings.

In accordance with §§ 201.16(c) and 207.3 of the rules, each document filed by a party to the reviews must be served on all other parties to the reviews (as identified by either the public or BPI service list), and a certificate of service must be timely filed. The Secretary will not accept a document for filing without a certificate of service.

Determination.—The Commission has determined these reviews are extraordinarily complicated and therefore has determined to exercise its authority to extend the review period by up to 90 days pursuant to 19 U.S.C. 1675(c)(5)(B).

Authority: These reviews are being conducted under authority of title VII of the Act; this notice is published pursuant to § 207.62 of the Commission’s rules.

By order of the Commission.

Issued: October 24, 2024.

Lisa Barton,

Secretary to the Commission.

[FR Doc. 2024–25097 Filed 10–28–24; 8:45 am]

BILLING CODE 7020–02–P

DEPARTMENT OF LABOR

Office of Federal Contract Compliance Programs

Notice of Request Under the Freedom of Information Act for Federal Contractors’ Type 2 Consolidated EEO–1 Report Data

AGENCY: Office of Federal Contract Compliance Programs, Labor.

ACTION: Notice.

SUMMARY: The U.S. Department of Labor’s Office of Federal Contract Compliance Programs (OFCCP) has received two requests under the Freedom of Information Act (FOIA) for 2021 Type 2 Consolidated Employer Information Reports, Standard Form 100 (EEO–1 Report), filed by the federal contractors. These two requests have come from the University of Utah and a non-profit organization named “As You Sow,” respectively. OFCCP has reason to believe that the information requested may be protected from disclosure under FOIA Exemption 4, which protects disclosure of confidential commercial information, but has not yet determined whether the requested information is protected from disclosure under that exemption. OFCCP is requesting that entities that filed Type 2 Consolidated EEO–1 Reports as federal contractors for the

2021 reporting year and object to the disclosure of this information submit those objections to OFCCP within 40 days of the date of this Notice.

DATES: Written objections to the FOIA requests discussed herein are due December 9, 2024.

FOR FURTHER INFORMATION CONTACT: Kelley Smith, Director, Division of Management and Administrative Programs, Office of Federal Contract Compliance Programs, 200 Constitution Avenue NW, Room C-3325, Washington, DC 20210. Telephone: 1-800-397-6251 (voice). If you are deaf, hard of hearing, or have a speech disability, please dial 7-1-1 to access telecommunications relay services.

SUPPLEMENTARY INFORMATION:

Background

A. Background on EEO-1 Reports

Multi-establishment employers must file annually a "Consolidated Report" (formerly known as a Type 2 Report) for all employees at the employer's headquarters as well as all its establishments, categorized by job category, sex, and race or ethnicity.

Since 1966, the Equal Employment Opportunity Commission (EEOC) has required eligible employers to submit workforce demographic data (EEO-1 Component 1) on an annual basis. All private employers that are covered by Title VII of the Civil Rights Act of 1964, as amended (Title VII) and that have 100 or more employees are required to file the workforce demographic data. 42 U.S.C. 2000e-8(c); 29 CFR 1602.7. In addition, OFCCP's regulations require federal contractors¹ and first-tier subcontractors that are covered by Executive Order 11246 and that have 50 or more employees to file the EEO-1 Report. 41 CFR 60-1.7(a).

The EEO-1 Report is administered as a single data collection to meet the statistical needs of both EEOC and OFCCP. OFCCP's regulations describe the EEO-1 Report as being "promulgated jointly . . . [with] the Equal Employment Opportunity Commission." 41 CFR 60-1.7(a)(1). Employers submit their data to the EEOC. See EEOC, Agency Information Collection Activities: Existing Collection, 88 FR 27504 (May 2, 2023). OFCCP then obtains the EEO-1 data of federal contractors from the EEOC.

Section 709(e) of Title VII of the Civil Rights Act of 1964 imposes criminal penalties and makes it unlawful for any officer or employee of EEOC from

making public the employment data derived from any of its data collections prior to the institution of any proceeding under EEOC's authority involving such information. 42 U.S.C. 2000e-8(e). Because OFCCP obtains EEO-1 data for contractors under its own E.O. 11246 authority, some courts have held that the Title VII prohibition against disclosure provision does not apply to OFCCP. See; *Sears, Roebuck & Co. v. General Services Admin.*, 509 F.2d 527, 529 (D.C. Cir. 1974). Accordingly, the EEO-1 data of federal contractors received by OFCCP are subject to the provisions of FOIA, meaning that members of the public may file FOIA requests asking OFCCP to disclose such records in its possession.

B. Legal Authorities Governing FOIA Requests for Potentially Commercial Confidential Information

Executive Order 12600 (E.O. 12600), published on June 23, 1987, established a formal process for notifying persons who submit confidential commercial information to the United States when that information becomes the subject of a FOIA request. 3 CFR 235 (1988), reprinted in 5 U.S.C. 552 note (2012 & supp. V 2017). Exemption 4 to the FOIA protects against the disclosure of "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." 5 U.S.C. 552(b)(4). E.O. 12600 is based on the principle that companies are entitled to notification and an opportunity to object to disclosure of this category of information before an agency makes a possible disclosure determination.

The Department's regulations implementing E.O. 12600 can be found at 29 CFR 70.26. These regulations require the agency to notify submitters of a FOIA request when it has reason to believe that the information requested may be protected from disclosure under Exemption 4 but has not yet made a determination. 29 CFR 70.26(d)(2). Further, the Department's regulations provide that when notification of a voluminous number of submitters is required, notice can be effectuated by posting and publishing it "in a place reasonably calculated to accomplish notification." *Id.* at 70.26(j). Given OFCCP's best estimate that these FOIA requests cover at least 14,000 unique federal contractors, OFCCP is fulfilling its notification obligation through this **Federal Register** notice, a

contemporaneous posting on the OFCCP website (<https://www.dol.gov/agencies/ofccp/submitter-notice-response-portal>), and notification to all federal contractors and federal contractor

representatives that have registered and provided electronic mail contact information through the agency's Contractor Portal and/or have subscribed to OFCCP's GovDelivery electronic mail listserv.

Once notified, the Department's regulations state that submitters will be provided a reasonable time to respond to the notice. *Id.* at 70.26(e). If a submitter has any objection to disclosure, it is "required to submit a detailed written statement as to why the information is a trade secret or commercial or financial information that is privileged or confidential." *Id.* If the agency receives a timely written objection, it will give careful consideration to the objection prior to making a decision whether the requested information should be disclosed or withheld under FOIA Exemption 4. E.O. 12600, Sec. 5. If the agency determines that disclosure is appropriate notwithstanding the submitter's objection, the agency will provide the submitter written notice of the reason for the decision, and a specified disclosure date that is a reasonable time subsequent to the notice. 29 CFR 70.26(f).

Process for Submitting Objections to the FOIA Requests

Consistent with E.O. 12600 and the Department's regulations, OFCCP is hereby notifying federal contractors that submitted a Consolidated EEO-1 Report for the 2021 reporting year (hereinafter Covered Contractors) of both aforementioned FOIA requests.² Covered Contractors have 40 days from the date of this Notice, or December 9, 2024, to submit to OFCCP a written objection to the disclosure of its 2021 Consolidated EEO-1 Report. Written objections must be received by OFCCP no later than this date. To facilitate this process, OFCCP has created a web form through which Covered Contractors may submit written objections, which can be found at <https://www.dol.gov/agencies/ofccp/submitter-notice-response-portal>. OFCCP strongly encourages Covered Contractors that wish to submit written objections to utilize this web form to facilitate processing. If utilizing the web form is not feasible, contractors may also submit written objections via email at OFCCPsubmitterResponse@dol.gov, or by mail to the contact provided in this notice. Regardless of the delivery system used, any objections filed by Covered Contractors must include the

¹ Hereinafter, all references to "contractors" or "federal contractors" includes first-tier subcontractors as well, unless specified otherwise.

² These requests also sought federal contractors' Consolidated Report EEO-1 data for the 2022 reporting year. However, because OFCCP currently only has the EEO-1 data for reporting year 2021 in its possession, this Notice is limited to that dataset.

contractor's name, address, contact information for the contractor (or its representative), and should, at minimum, address the following questions in detail so that OFCCP may evaluate the objection to determine whether the information should be withheld or disclosed pursuant to FOIA Exemption 4:

1. What specific information from the 2021 EEO-1 Report does the contractor consider to be a trade secret or commercial or financial information?
2. What facts support the contractor's belief that this information is commercial or financial in nature?
3. Does the contractor customarily keep the requested information private or closely-held? What steps have been taken by the contractor to protect the confidentiality of the requested data, and to whom has it been disclosed?
4. Does the contractor contend that the government provided an express or implied assurance of confidentiality? If no, were there express or implied indications at the time the information was submitted that the government would publicly disclose the information?
5. How would disclosure of this information harm an interest of the contractor protected by Exemption 4 (such as by causing foreseeable harm to the contractor's economic or business interests)?

In the event that a Covered Contractor fails to respond to the notice within the time specified, it will be considered to have no objection to disclosure of the information. *See* 29 CFR 70.26(e). For Covered Contractors that do submit timely objections, OFCCP will independently evaluate the objection(s) submitted consistent with the agency's regulations described herein and other relevant legal authority. If OFCCP determines to disclose the information over the objection of the Covered Contractor, OFCCP will provide written notice to the Covered Contractor of the reasons the disclosure objections were not sustained, a description of the information that will be disclosed, and a specified disclosure date that is a reasonable time subsequent to the notice. *Id.* at 70.26(f).

Michele Hodge,

Acting Director, Office of Federal Contract Compliance Programs.

[FR Doc. 2024-24381 Filed 10-28-24; 8:45 am]

BILLING CODE 4510-CM-P

DEPARTMENT OF LABOR

Agency Information Collection Activities; Submission for OMB Review; Comment Request; Mine Mapping and Records of Opening, Closing, and Reopening of Mines

ACTION: Notice of availability; request for comments.

SUMMARY: The Department of Labor (DOL) is submitting this Mine Safety and Health Administration (MSHA)-sponsored information collection request (ICR) to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995 (PRA). Public comments on the ICR are invited.

DATES: The OMB will consider all written comments that the agency receives on or before November 29, 2024.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting "Currently under 30-day Review—Open for Public Comments" or by using the search function.

FOR FURTHER INFORMATION CONTACT: Michael Howell by telephone at 202-693-6782, or by email at DOL_PRA_PUBLIC@dol.gov.

SUPPLEMENTARY INFORMATION: This information collection protects miners by assuring that up-to-date, accurate mine maps contain the information needed to clarify the best alternatives for action during an emergency operation. Also, coal mine operators routinely use maps to create safe and effective development plans.

Mine maps are schematic depictions of critical mine infrastructure, such as water, power, transportation, ventilation, and communication systems. Using accurate, up-to-date maps during a disaster, mine emergency personnel can locate refuges for miners and identify sites of explosion potential; they can know where stationary equipment was placed, where ground was secured, and where they can best begin a rescue operation. During a disaster, maps can be crucial to the safety of the emergency personnel who must enter a mine to begin a search for survivors.

Mine maps may describe the current status of an operating mine or provide crucial information about a long-closed mine that is being reopened.

Coal mine operators use map information to develop safe and effective plans and to help determine hazards before beginning work in areas, such as abandoned underground mines or the worked-out and inaccessible areas of an active underground or surface mine. Abandoned mines or inaccessible areas of active mines may have water inundation potentials and explosive levels of methane or lethal gases. If an operator, unaware of the hazards, were to mine into such an area, miners could be killed or seriously injured. For additional substantive information about this ICR, see the related notice published in the **Federal Register** on July 12, 2024 (89 FR 57168).

Comments are invited on: (1) whether the collection of information is necessary for the proper performance of the functions of the Department, including whether the information will have practical utility; (2) the accuracy of the agency's estimates of the burden and cost of the collection of information, including the validity of the methodology and assumptions used; (3) ways to enhance the quality, utility and clarity of the information collection; and (4) ways to minimize the burden of the collection of information on those who are to respond, including the use of automated collection techniques or other forms of information technology.

This information collection is subject to the PRA. A Federal agency generally cannot conduct or sponsor a collection of information, and the public is generally not required to respond to an information collection, unless the OMB approves it and displays a currently valid OMB Control Number. In addition, notwithstanding any other provisions of law, no person shall generally be subject to penalty for failing to comply with a collection of information that does not display a valid OMB Control Number. *See* 5 CFR 1320.5(a) and 1320.6.

Agency: DOL-MSHA.

Title of Collection: Mine Mapping and Records of Opening, Closing, and Reopening of Mines.

OMB Control Number: 1219-0073.

Affected Public: Businesses or other for-profits.

Number of Respondents: 376.

Frequency: On occasion.

Number of Responses: 1,540.

Annual Burden Hours: 8,308 hours.

Total Estimated Annual Other Costs Burden: \$5,134,836.

(Authority: 44 U.S.C. 3507(a)(1)(D))

Michael Howell,

Senior Paperwork Reduction Act Analyst.

[FR Doc. 2024-25028 Filed 10-28-24; 8:45 am]

BILLING CODE 4510-43-P

DEPARTMENT OF LABOR**Bureau of Labor Statistics****Technical Advisory Committee; Notice of Meeting and Agenda; Correction****AGENCY:** Bureau of Labor Statistics.**ACTION:** Notice; correction.

SUMMARY: The Bureau of Labor Statistics published a document in the **Federal Register** on October 18, 2024, announcing the November 7, 2024 Technical Advisory Committee meeting. The document contained an incorrect registration link.

SUPPLEMENTARY INFORMATION:**Correction**

In the **Federal Register** Notice on page 83908 in the third column, correct <https://blstac.beventbrite.com> to read: Individuals planning to attend the meeting should register at <https://blstac.eventbrite.com>.

Dated: October 23, 2024.

Leslie Bennett,*Chief, Division of Management Systems.*

[FR Doc. 2024-25030 Filed 10-28-24; 8:45 am]

BILLING CODE 4510-24-P**NATIONAL AERONAUTICS AND SPACE ADMINISTRATION****[Notice: 24-076]****Astrophysics Advisory Committee****AGENCY:** National Aeronautics and Space Administration.**ACTION:** Notice of meeting.

SUMMARY: In accordance with the Federal Advisory Committee Act, the National Aeronautics and Space Administration (NASA) announces a meeting of the Astrophysics Advisory Committee.

DATES: Thursday, November 7, 2024, 9 a.m.–5 p.m., and Friday, November 8, 2024, 9 a.m.–5 p.m., All times are eastern time.

ADDRESSES: Public attendance will be virtual only. Webex registration information below.

FOR FURTHER INFORMATION CONTACT: Mr. David Morris, Designated Federal Officer, Astrophysics Advisory Committee, NASA Headquarters, Washington, DC 20546, via email at david.c.morris@nasa.gov or at (202) 718-9061.

SUPPLEMENTARY INFORMATION: As noted above, this meeting will be open to the public via Webinar and telephonically. Any interested person must use a touch-

tone phone to participate in this meeting. The Webex connectivity information for each day will be provided to those who register in advance through the registration link below. For audio, when you join the Webex event, you may use your computer or provide your phone number to receive a call back, otherwise, call the U.S. toll conference number listed for each day in the registration information that is sent after registration. Attendees must preregister to receive meeting connection information. Preregister at: <https://nasaevents.webex.com/nasaevents/j.php?MTID=m94141b8705290e7765ef0e2fef80bcb7>.

The agenda for the meeting includes the following topics:

- Astrophysics Division Update
- Updates on Specific Astrophysics Missions
- Discussion of reports from the Program Analysis Groups

The public may submit and upvote comments/questions ahead of the meeting through the website: <https://nasa.cnf.io/sessions/n24m/#!/dashboard>, that will be opened for input on October 28, 2024.

It is imperative that the meeting be held on these dates to accommodate the scheduling priorities of the key participants.

For more information, please visit <https://beta.science.nasa.gov/researchers/nac/science-advisory-committees/apac/>.

Jamie M. Krauk,*Advisory Committee Management Officer, National Aeronautics and Space Administration.*

[FR Doc. 2024-25082 Filed 10-28-24; 8:45 am]

BILLING CODE 7510-13-P**NATIONAL COUNCIL ON DISABILITY****Sunshine Act Meetings**

TIME AND DATE: The Members of the National Council on Disability (NCD) will hold a quarterly business meeting on Thursday, November 7, 2024, 1:00 p.m.–4:00 p.m., Eastern Standard Time (EST).

PLACE: This meeting will occur via Zoom videoconference. Registration is required. Interested parties are encouraged to join the meeting in an attendee status by Zoom Desktop Client, Mobile App, or Telephone to dial-in. Updated information is available on NCD's event page at <https://www.ncd.gov/meeting/2024-11-07-nov-7-2024-council-meeting/>. To register for the Zoom webinar, please use the

following URL: https://events.zoomgov.com/ev/AioHqgW_2CRBZxxCdmUEs-cZKhGXqvAbM0kPOLyZzkpPC-DakrJO-ApymXj7jq6MmWodMQXHvW1qh9WF_26fGDcuEFnW2klvOurK8ef-QYO4YQ.

In the event of audio disruption or failure, attendees can follow the meeting by accessing the Communication Access Realtime Translation (CART) link provided. CART is text-only translation that occurs real time and is not an exact transcript.

STATUS: This meeting is open to the public in its entirety.

MATTERS TO BE CONSIDERED: Following welcome remarks and introductions, the Executive Committee will provide their report, including financial and governance reports; followed by the Chair's report; policy updates; a presentation on NCD's accessible ground transportation and people with mobility disabilities project, followed by Council member Q&A; a break; Council member community report outs; a disability data presentation, followed by Council member Q&A; public comment on voting experiences; concluding with adjournment.

Agenda: The times provided below are approximations for when each agenda item is anticipated to be discussed (all times Eastern Daylight Time):

Thursday, November 7, 2024

- 1:00–1:05 p.m. Welcome and Call to Order
- 1:05–1:20 p.m. Executive Committee Report Outs. Financial Report, Governance Report
- 1:20–1:25 p.m. Chair's Report
- 1:25–1:40 p.m. Policy Updates
- 1:40–2:15 p.m. Accessible Ground Transportation and People with Mobility Disabilities Project Presentation, Q&A from Council Members
- 2:15–2:30 p.m. BREAK
- 2:30–3:00 p.m. Council Member Report Outs on Community Outreach/ Input
- 3:00–3:30 p.m. Disability Data Update, Q&A from Council Members
- 3:30–3:31 p.m. Verbal recap of any chat comments received
- 3:30–4:00 p.m. Public Comment
- 4:00 p.m. Adjourn

Public Comment: Your participation during the public comment period provides an opportunity for us to hear from you—individuals, businesses, providers, educators, parents and advocates. For the November 7 Council meeting, NCD will have a public comment session to receive perspectives

on voting experiences in the Nov. 5, 2024 General Election. Commenters are encouraged to respond to the following prompts regarding their voting experience during the November 5, 2024 General Election:

1. Did you experience any accessibility issues when you voted? What were they?

2. If you did experience any accessibility issues when you voted, were the poll workers knowledgeable on how to assist so you could exercise your right to vote independently?

Additional information on specifics of the topic and guidelines are available on NCD's public comment page at <https://www.ncd.gov/public-comment/>.

Because of the virtual format, the Council will receive public comment by email or by video or audio over Zoom. To provide public comment during an NCD Council Meeting, NCD now requires advanced registration by either signing up to present while registering for the meeting or sending an email to PublicComment@ncd.gov with the subject line "Public Comment" and your name, organization, state, and topic of comment included in the body of your email. Deadline for registration is Nov. 5, 8:00 p.m. EST.

While public comment can be submitted on any topic over email, comments during the meeting are explicitly for voting experiences in the Nov. 5 General Election.

If any time remains following the conclusion of the comments of those registered, NCD may call upon those who desire to make comments but did not register.

CONTACT PERSON FOR MORE INFORMATION: Nicholas Sabula, Public Affairs Specialist, NCD, 1331 F Street NW, Suite 850, Washington, DC 20004; 202-272-2004 (V), or nsabula@ncd.gov.

Accommodations: An ASL interpreter will be on-camera during the entire meeting, and CART has been arranged for this meeting and will be embedded into the Zoom platform as well as available via streamtext link. The web link to access CART (in English) is: <https://www.streamtext.net/player?event=NCD>.

If you require additional accommodations, please indicate on the registration form or notify Stacey Brown by sending an email to sbrown@ncd.gov as soon as possible, no later than 24 hours before the meeting.

Language Access: If you need language access services, please indicate on the registration form or notify Nicholas Sabula by sending an email to nsabula@ncd.gov as soon as possible, no later than by November 1.

Due to last-minute confirmations or cancellations, NCD may substitute items without advance public notice.

Dated: October 23, 2024.

Anne C. Sommers McIntosh,

Executive Director.

[FR Doc. 2024-25064 Filed 10-25-24; 11:15 am]

BILLING CODE 8421-02-P

NATIONAL LABOR RELATIONS BOARD

Notice of Appointments of Individuals To Serve as Members of Performance Review Boards

AGENCY: National Labor Relations Board.

ACTION: Notice; appointment to serve as members of performance review boards.

SUMMARY: The National Labor Relations Board is issuing this notice that the individuals whose names and position titles appear below have been appointed to serve as members of performance review boards in the National Labor Relations Board for the rating year beginning October 1, 2023 and ending September 30, 2024.

FOR FURTHER INFORMATION CONTACT:

Roxanne L. Rothschild, Executive Secretary, National Labor Relations Board, 1015 Half Street SE, Washington, DC 20570, (202) 273-1940 (this is not a toll-free number), 1-866-315-6572 (TTY/TDD).

SUPPLEMENTARY INFORMATION:

Name and Title

Joan A. Sullivan—Associate General Counsel, Division of Operations Management
Peter Sung Ohr—Deputy General Counsel, Office of the General Counsel
Nancy Kessler Platt—Associate General Counsel, Division of Legal Counsel
Andrew Krafts—Executive Assistant to the Chairman (Chief of Staff), The Board
Grant Kraus—Deputy Chief Counsel, The Board
Ruth Burdick—(alternate) Deputy Associate General Counsel, Division of Enforcement Litigation, Appellate and Supreme Court Litigation Branch

Authority: 5 U.S.C. 4314(c)(4).

By Direction of the Board.

Dated: October 23, 2024.

Roxanne L. Rothschild,

Executive Secretary.

[FR Doc. 2024-25036 Filed 10-28-24; 8:45 am]

BILLING CODE 7545-01-P

NUCLEAR REGULATORY COMMISSION

[NRC-2023-0206]

Information Collection: General Domestic Licenses for Byproduct Material

AGENCY: Nuclear Regulatory Commission.

ACTION: Notice of submission to the Office of Management and Budget; request for comment.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) has recently submitted a request for renewal of an existing collection of information to the Office of Management and Budget (OMB) for review. The information collection is entitled, "General Domestic Licenses for Byproduct Material."

DATES: Submit comments by November 29, 2024. Comments received after this date will be considered if it is practical to do so, but the Commission is able to ensure consideration only for comments received on or before this date.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to <https://www.reginfo.gov/public/do/PRAMain>. Find this particular information collection by selecting "Currently under Review—Open for Public Comments" or by using the search function.

FOR FURTHER INFORMATION CONTACT:

David Cullison, NRC Clearance Officer, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; telephone: 301-415-2084; email: Infocollects.Resource@nrc.gov.

SUPPLEMENTARY INFORMATION:

I. Obtaining Information and Submitting Comments

A. Obtaining Information

Please refer to Docket ID NRC-2023-0206 when contacting the NRC about the availability of information for this action. You may obtain publicly available information related to this action by any of the following methods:

- **Federal Rulemaking website:** Go to <https://www.regulations.gov> and search for Docket ID NRC-2023-0206.
- **NRC's Agencywide Documents Access and Management System (ADAMS):** You may obtain publicly available documents online in the ADAMS Public Documents collection at <https://www.nrc.gov/reading-rm/adams.html>. To begin the search, select "Begin Web-based ADAMS Search." For

problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, at 301-415-4737, or by email to PDR.Resource@nrc.gov. The supporting statement and burden spreadsheet are available in ADAMS under Accession Nos. ML24213A020 and ML24213A019, respectively.

- **NRC's PDR:** The PDR, where you may examine and order copies of publicly available documents, is open by appointment. To make an appointment to visit the PDR, please send an email to PDR.Resource@nrc.gov or call 1-800-397-4209 or 301-415-4737, between 8 a.m. and 4 p.m. eastern time (ET), Monday through Friday, except Federal holidays.

- **NRC's Clearance Officer:** A copy of the collection of information and related instructions may be obtained without charge by contacting the NRC's Clearance Officer, David Cullison, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; telephone: 301-415-2084; email: Infocollects.Resource@nrc.gov.

B. Submitting Comments

Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to <https://www.reginfo.gov/public/do/PRAMain>. Find this particular information collection by selecting "Currently under Review—Open for Public Comments" or by using the search function.

The NRC cautions you not to include identifying or contact information in comment submissions that you do not want to be publicly disclosed in your comment submission. All comment submissions are posted at <https://www.regulations.gov> and entered into ADAMS. Comment submissions are not routinely edited to remove identifying or contact information.

If you are requesting or aggregating comments from other persons for submission to the OMB, then you should inform those persons not to include identifying or contact information that they do not want to be publicly disclosed in their comment submission. Your request should state that comment submissions are not routinely edited to remove such information before making the comment submissions available to the public or entering the comment into ADAMS.

II. Background

Under the provisions of the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35), the NRC recently

submitted a request for renewal of an existing collection of information to OMB for review entitled, "General Domestic Licenses for Byproduct Material." The NRC hereby informs potential respondents that an agency may not conduct or sponsor, and that a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

The NRC published a **Federal Register** notice with a 60-day comment period on this information collection on May 24, 2024, 89 FR 45927.

1. *The title of the information collection:* General Domestic Licenses for Byproduct Material.

2. *OMB approval number:* 3150-0016.

3. *Type of submission:* Extension.

4. *The form number, if applicable:* Not applicable.

5. *How often the collection is required or requested:* Reports are submitted as events occur. General license registration requests may be submitted at any time. Changes to the information on the registration may be submitted as they occur. Devices meeting certain criteria must be registered annually.

6. *Who will be required or asked to respond:* Persons receiving, possessing, using, or transferring devices containing byproduct material.

7. *The estimated number of annual responses:* 172,694 (10,418 reporting responses + 226 third-party responses + 162,050 recordkeepers).

8. *The estimated number of annual respondents:* 162,050 (18,843 NRC licensee respondents + 143,207, Agreement State licensee respondents).

9. *The estimated number of hours needed annually to comply with the information collection requirement or request:* 45,116 hours.

10. *Abstract:* Part 31 of title 10 of the *Code of Federal Regulations* (10 CFR), "General Domestic Licenses for Byproduct Material" establishes general licenses for the possession and use of byproduct material in certain devices. General licensees are required to keep testing records and submit event reports identified in 10 CFR part 31, which assist the NRC in determining, with reasonable assurance, that devices are operated safely and without radiological hazard to users or the public.

Dated: October 24, 2024.

For the Nuclear Regulatory Commission.

David Cullison,

NRC Clearance Officer, Office of the Chief Information Officer.

[FR Doc. 2024-25093 Filed 10-28-24; 8:45 am]

BILLING CODE 7590-01-P

NUCLEAR REGULATORY COMMISSION

[Docket No. 70-7005; NRC-2024-0164]

Waste Control Specialists LLC; Environmental Assessment and Finding of No Significant Impact

AGENCY: Nuclear Regulatory Commission.

ACTION: Notice; issuance.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is issuing an environmental assessment (EA) and finding of no significant impact (FONSI) in support of the NRC's consideration of a request from Waste Control Specialists LLC (WCS) to continue to possess certain transuranic waste, which originated from the Los Alamos National Laboratory (LANL), without an NRC license under the terms of a 2023 Order. The 2023 Order exempted WCS from the NRC's regulations concerning special nuclear material (SNM). The current action is in response to a request by WCS dated May 24, 2024, to extend the possession time of certain waste at specific locations at the facility in Andrews County, Texas (WCS Site) until December 31, 2026.

DATES: October 29, 2024.

ADDRESSES: Please refer to Docket ID NRC-2024-0164 when contacting the NRC about the availability of information regarding this document. You may access publicly available information related to this document using any of the following methods:

- **Federal Rulemaking website:** Go to <https://www.regulations.gov> and search for Docket ID NRC-2024-0164. Address questions about Docket IDs in *Regulations.gov* to Stacy Schumann; telephone: 301-415-0624; email: Stacy.Schumann@nrc.gov. For technical questions, contact the individual listed in the **FOR FURTHER INFORMATION CONTACT** section of this document.

- **NRC's Agencywide Documents Access and Management System (ADAMS):** You may obtain publicly available documents online in the ADAMS Public Documents collection at <https://www.nrc.gov/reading-rm/adams.html>. To begin the search, select "Begin Web-based ADAMS Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, at 301-415-4737, or by email to PDR.Resource@nrc.gov. For the convenience of the reader, instructions about obtaining materials referenced in this document are provided in the "Availability of Documents" section.

- **NRC's PDR:** The PDR, where you may examine and order copies of

publicly available documents, is open by appointment. To make an appointment to visit the PDR, please send an email to PDR.Resource@nrc.gov or call 1-800-397-4209 or 301-415-4737, between 8 a.m. and 4 p.m. eastern time (ET), Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT:

Harry Felsher, Office of Nuclear Material Safety and Safeguards; U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; telephone: 301-415-6559; email: Harry.Felsher@nrc.gov.

SUPPLEMENTARY INFORMATION:

I. Discussion

The NRC is considering modifying a previously issued order condition that would allow Waste Control Specialists LLC (WCS) to continue possessing certain transuranic waste, which originated from the Los Alamos National Laboratory (LANL), without an NRC license for another two years at its Andrews County, Texas site. WCS possesses the transuranic waste at issue under the terms of the 2023 Order. Based on the results of the EA that follows, the NRC is issuing a FONSI and, therefore, does not need to prepare an environmental impact statement.

WCS operates a facility in Andrews County, Texas (WCS Site) that is licensed to process, store, and perform certain operations with certain types of radioactive material contained in low-level waste (LLW) and mixed waste. The WCS Site is also licensed to dispose of certain radioactive, hazardous, and toxic waste. Under an agreement authorized by the Atomic Energy Act of 1954, as amended, a State can assume regulatory authority over radioactive material. In 1963, Texas entered into such an agreement and assumed regulatory authority over source material, byproduct material, and SNM under critical mass. The WCS Site is licensed by the Texas Commission on Environmental Quality (TCEQ) for possession, treatment/operations, and storage of radioactive waste and disposal of LLW under Radioactive Materials License (RML) R04100.

Section 70.3 of title 10 of the *Code of Federal Regulations* (10 CFR) requires persons who own, acquire, deliver, receive, possess, use, or transfer SNM to obtain a license pursuant to the requirements of 10 CFR part 70. The licensing requirements in 10 CFR part 70 apply to persons in Agreement States possessing equal to or greater than critical mass quantities. However, pursuant to 10 CFR 70.17(a), “the Commission may . . . grant such

exemptions from the requirements of the regulations in this part as it determines are authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest.”

On September 25, 2000, WCS first requested an exemption from the licensing requirements in 10 CFR part 70. On November 21, 2001, the NRC issued an order to WCS (2001 Order) granting an exemption from certain NRC regulations and permitting WCS, under specified conditions, to possess waste containing SNM in greater quantities than specified in 10 CFR part 150, at the WCS Storage and Treatment Facility without obtaining an NRC license pursuant to 10 CFR part 70. The 2001 Order was published in the **Federal Register** on November 15, 2001. The NRC issued superseding Orders to WCS in 2004 (*i.e.*, modified list of reagents), 2009 (*i.e.*, modified sampling requirements), 2014 (*i.e.*, modified to include storage of LANL Waste), and 2023 (*i.e.* modified to allow certain movement of LANL Waste, to allow certain preparation for shipment operations with LANL Waste, to update storage of LANL Waste) that modified the conditions in the 2001 Order. In addition, WCS’ authorization to possess the LANL waste was previously extended in two-year increments in 2016, 2018, 2020, and 2022.

On February 14, 2014, a radiation release event occurred at the U.S. Department of Energy (DOE) Waste Isolation Pilot Plant (WIPP) Facility (WIPP Incident). In response, the DOE suspended operations at the WIPP Facility. In April 2014, WCS began receiving some specific waste from DOE that both WCS and DOE understood to meet both the U.S. Department of Transportation (DOT) shipping requirements and the conditions in the 2009 Order. WCS began storing that waste at the Treatment, Storage, and Disposal Facility (TSDF) (previously known as Storage and Treatment Facility) on the WCS Site, identified as the Storage and Processing Facility in RML R04100, which is the WCS TCEQ-issued license. The waste was DOE transuranic waste that originated at LANL that was destined to be disposed of at the DOE WIPP Facility (*i.e.*, “LANL Waste”). In June 2014, WCS received information from DOE that some of the LANL Waste being temporarily stored at the TSDF may be of concern as the waste is similar to the waste that caused an incident at WIPP. In response, WCS moved some of the LANL Waste from the TSDF to the WCS’ Federal Waste Facility (FWF) Disposal Cell for temporary storage.

By letter dated June 30, 2022, WCS requested a superseding NRC order to: (1) move the DOE LANL Waste from the FWF Disposal Cell to the TSDF Bin Storage Area-1 (BSA-1) Enclosure, (2) prepare the LANL Waste in the TSDF BSA-1 Enclosure for shipment, and (3) temporarily store the LANL Waste in the TSDF BSA-1 Enclosure until the DOE ships the LANL Waste off the WCS Site to a DOE determined location. By letter dated May 22, 2023, the NRC approved the WCS request and issued the superseding 2023 Order.

By letter dated May 24, 2024, WCS requested that the effectiveness of its exemption from NRC requirements in 10 CFR part 70 be extended with the modification of Condition 9.B.4 of the 2023 Order to extend the timeframe for temporarily allowing possession of the LANL Waste at the WCS Site to “until December 31, 2026.” That proposal is the subject of this EA.

II. Environmental Assessment

Description of the Proposed Action

The proposed action is to modify the 2023 Order Condition 9.B.4 to allow WCS to continue to possess the LANL Waste at specific locations at the WCS Site until December 31, 2026, without an NRC license.

Need for the Proposed Action

WCS made the request to continue to possess the LANL Waste while the DOE-led Interagency Project Team (including WCS, DOE, U.S. Environmental Protection Agency, NRC, the State of Texas, and the State of New Mexico) works to recommend a path forward for disposition of the LANL Waste. Also, while the DOE WIPP Facility has resumed operations, some of the LANL Waste at the WCS Site cannot be shipped off the site at this time because it does not meet DOT shipping requirements.

The purpose of this EA is to assess the potential environmental impacts of the WCS request to modify the 2023 Order Condition 9.B.4 to allow WCS to possess the LANL Waste at specific locations at the WCS Site until December 31, 2026, under the other 2023 Order Conditions. This EA does not approve or deny the requested action.

Environmental Impacts of the Proposed Action

The NRC does not expect changes in radiation hazards to workers or to the environment. WCS will continue to be required to ensure that the LANL Waste on the WCS Site is possessed safely and securely. WCS will continue to be required to notify the NRC of any events

as appropriate, as set out in the 2023 Order. No changes to its handling or associated hazards would occur as a result of granting the requested change. Other environmental impacts would be the same as evaluated in the EA that supported the 2023 Order, as applicable to the activities associated with the continued safe possession of the LANL Waste.

Environmental Impacts of the Alternatives to the Proposed Action

As an alternative to the proposed action, the NRC staff could deny the WCS request and, therefore, not issue a modification to the Order Condition 9.B.4 that would authorize continued possession of the LANL Waste at the WCS Site after December 31, 2024 (*i.e.*, the “no action” alternative).

Upon expiration of the timeframe in the 2023 Order Condition 9.B.4, WCS would still be required to maintain the material safely. In addition, the NRC authorization of any change to the current possession of the LANL Waste at the WCS Site would still be required. As a result, under this alternative, there would be no environmental impacts different from the proposed action, although WCS would be expected to secure a license or other regulatory authorization for the possession of LANL Waste or potentially be in violation of 10 CFR part 70 upon the

expiration of the term in the 2023 Order Condition 9.B.4. For the reasons noted in this notice, removing the material from the site prior to the expiration of the current term is not part of the no-action alternative.

Thus, the “no action” alternative would not result in changes to the environmental impacts evaluated in the NRC’s prior EAs that supported the 2023 Order or the previous NRC orders. Those prior EAs concluded that there would be no significant radiological or non-radiological environmental impacts associated with the possession of LANL Waste at the WCS Site, consistent with the conditions in those NRC orders.

Agencies and Persons Consulted

On October 1, 2024, the staff provided a copy of the draft EA to the TCEQ for its review and comment. The TCEQ provided its comments on October 1, 2024. The NRC staff updated the EA in response to the TCEQ comments, as appropriate.

The proposed action does not involve the development or disturbance of additional land. Hence, the NRC has determined that the proposed action will not affect listed endangered or threatened species or their critical habitat. Therefore, no further consultation is required under Section 7 of the Endangered Species Act. Likewise, the NRC staff has determined

that the proposed action does not have the potential to cause effects on historical properties even if present and no ground disturbing activities are associated with the proposed action. Therefore, no consultation is required under Section 106 of the National Historic Preservation Act.

III. Finding of No Significant Impact

The NRC has reviewed the WCS May 24, 2024, request to supplement the 2023 Order to extend the possession time of the LANL Waste at specific locations at the WCS Site. The NRC has found that effluent releases and potential radiological doses to the public are not anticipated to change as a result of this action and that occupational exposures are expected to remain within regulatory limits and as low as reasonably achievable. On the basis of this EA, the NRC concludes that the proposed action will not have a significant effect on the quality of the human environment.

Accordingly, the NRC has determined not to prepare an environmental impact statement for the proposed action.

IV. Availability of Documents

The documents identified in the following table are available to interested persons through one or more of the following methods, as indicated.

Document description	Adams accession No. / Federal Register citation
WCS Request to Extend Possession Timeframe of LANL Waste until December 31, 2026, dated May 24, 2024	ML24149A063
Environmental Assessment and Finding of No Significant Impact for 2023 NRC Order, dated May 15, 2023	88 FR 31829
2023 NRC Order, dated May 22, 2023	88 FR 34900
Environmental Assessment and Finding of No Significant Impact for 2020 NRC Letter, dated May 24, 2022	87 FR 32198
NRC Letter Approving Extending Possession Timeframe, dated June 8, 2022	ML22094A131
Environmental Assessment and Finding of No Significant Impact for 2020 NRC Letter, dated November 24, 2020	85 FR 77268
NRC Letter Approving Extending Possession Timeframe, dated December 7, 2020	ML20252A182
Environmental Assessment and Finding of No Significant Impact for 2018 NRC Letter, dated December 12, 2018	83 FR 64902
NRC Letter Approving Extending Possession Timeframe, dated December 19, 2018	ML18269A318
NRC Letter Approving Extending Possession Timeframe, dated September 23, 2016	ML16097A265
Environmental Assessment and Finding of No Significant Impact for 2014 NRC Order, dated October 30, 2014	79 FR 65999
2014 NRC Order, dated December 3, 2014	79 FR 73647
Environmental Assessment and Finding of No Significant Impact for 2009 NRC Order, dated October 7, 2009	74 FR 52981
2009 NRC Order, dated October 20, 2009	74 FR 55071
Environmental Assessment and Finding of No Significant Impact for 2004 NRC Order, dated October 14, 2004	69 FR 61697
2004 NRC Order, dated November 5, 2004	69 FR 65468
Environmental Assessment and Finding of No Significant Impact for 2001 NRC Order, dated October 18, 2001	66 FR 56358
2001 NRC Order, dated October 30, 2001	66 FR 57489
2000 WCS Request for Initial Order, dated September 25, 2000	ML003759584

Dated: October 24, 2024.

For the Nuclear Regulatory Commission.

Jane Marshall,

*Director, Division of Decommissioning,
Uranium Recovery, and Waste Programs,
Office of Nuclear Material Safety and
Safeguards.*

[FR Doc. 2024-25080 Filed 10-28-24; 8:45 am]

BILLING CODE 7590-01-P

NUCLEAR REGULATORY COMMISSION

[NRC-2024-0187]

Monthly Notice; Applications and Amendments to Facility Operating Licenses and Combined Licenses Involving No Significant Hazards Considerations

AGENCY: Nuclear Regulatory Commission.

ACTION: Monthly notice.

SUMMARY: Pursuant to section 189a.(2) of the Atomic Energy Act of 1954, as amended (the Act), the U.S. Nuclear Regulatory Commission (NRC) is publishing this regular monthly notice. The Act requires the Commission to publish notice of any amendments issued, or proposed to be issued, and grants the Commission the authority to issue and make immediately effective any amendment to an operating license or combined license, as applicable, upon a determination by the Commission that such amendment involves no significant hazards consideration (NSHC), notwithstanding the pendency before the Commission of a request for a hearing from any person.

DATES: Comments must be filed by November 29, 2024. A request for a hearing or petitions for leave to intervene must be filed by December 30, 2024. This monthly notice includes all amendments issued, or proposed to be issued, from September 13, 2024, to October 10, 2024. The last monthly notice was published on October 1, 2024.

ADDRESSES: You may submit comments by any of the following methods; however, the NRC encourages electronic comment submission through the Federal rulemaking website.

- *Federal rulemaking website:* Go to <https://www.regulations.gov> and search for Docket ID NRC-2024-0187. Address questions about Docket IDs in *Regulations.gov* to Stacy Schumann; telephone: 301-415-0624; email: Stacy.Schumann@nrc.gov. For technical questions, contact the individual listed in the **FOR FURTHER INFORMATION**

CONTACT section of this document.

- *Mail comments to:* Office of Administration, Mail Stop: TWFN-7-A60M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Program Management, Announcements and Editing Staff.

For additional direction on obtaining information and submitting comments,

see “Obtaining Information and Submitting Comments” in the **SUPPLEMENTARY INFORMATION** section of this document.

FOR FURTHER INFORMATION CONTACT:

Susan Lent, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; telephone: 301-415-1365; email: Susan.Lent@nrc.gov.

SUPPLEMENTARY INFORMATION:

I. Obtaining Information and Submitting Comments

A. Obtaining Information

Please refer to Docket ID NRC-2024-0187, facility name, unit number(s), docket number(s), application date, and subject when contacting the NRC about the availability of information for this action. You may obtain publicly available information related to this action by any of the following methods:

- *Federal Rulemaking Website:* Go to <https://www.regulations.gov> and search for Docket ID NRC-2024-0187.

- *NRC's Agencywide Documents Access and Management System (ADAMS):* You may obtain publicly available documents online in the ADAMS Public Documents collection at <https://www.nrc.gov/reading-rm/adams.html>. To begin the search, select “Begin Web-based ADAMS Search.” For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, at 301-415-4737, or by email to PDR.Resource@nrc.gov. For the convenience of the reader, instructions about obtaining materials referenced in this document are provided in the “Availability of Documents” section.

- *NRC's PDR:* The PDR, where you may examine and order copies of publicly available documents, is open by appointment. To make an appointment to visit the PDR, please send an email to PDR.Resource@nrc.gov or call 1-800-397-4209 or 301-415-4737, between 8 a.m. and 4 p.m. eastern time (ET), Monday through Friday, except Federal holidays.

B. Submitting Comments

The NRC encourages electronic comment submission through the Federal rulemaking website (<https://www.regulations.gov>). Please include Docket ID NRC-2024-0187, facility name, unit number(s), docket number(s), application date, and subject, in your comment submission.

The NRC cautions you not to include identifying or contact information that you do not want to be publicly disclosed in your comment submission. The NRC will post all comment

submissions at <https://www.regulations.gov> as well as enter the comment submissions into ADAMS. The NRC does not routinely edit comment submissions to remove identifying or contact information.

If you are requesting or aggregating comments from other persons for submission to the NRC, then you should inform those persons not to include identifying or contact information that they do not want to be publicly disclosed in their comment submission. Your request should state that the NRC does not routinely edit comment submissions to remove such information before making the comment submissions available to the public or entering the comment into ADAMS.

II. Notice of Consideration of Issuance of Amendments to Facility Operating Licenses and Combined Licenses and Proposed No Significant Hazards Consideration Determination

For the facility-specific amendment requests shown in this notice, the Commission finds that the licensees' analyses provided, consistent with section 50.91 of title 10 of the *Code of Federal Regulations* (10 CFR) “Notice for public comment; State consultation,” are sufficient to support the proposed determinations that these amendment requests involve NSHC. Under the Commission's regulations in 10 CFR 50.92, operation of the facilities in accordance with the proposed amendments would not (1) involve a significant increase in the probability or consequences of an accident previously evaluated; or (2) create the possibility of a new or different kind of accident from any accident previously evaluated; or (3) involve a significant reduction in a margin of safety.

The Commission is seeking public comments on these proposed determinations. Any comments received within 30 days after the date of publication of this notice will be considered in making any final determinations.

Normally, the Commission will not issue the amendments until the expiration of 60 days after the date of publication of this notice. The Commission may issue any of these license amendments before expiration of the 60-day period provided that its final determination is that the amendment involves NSHC. In addition, the Commission may issue any of these amendments prior to the expiration of the 30-day comment period if circumstances change during the 30-day comment period such that failure to act in a timely way would result, for example in derating or shutdown of the

facility. If the Commission takes action on any of these amendments prior to the expiration of either the comment period or the notice period, it will publish in the **Federal Register** a notice of issuance. If the Commission makes a final NSHC determination for any of these amendments, any hearing will take place after issuance. The Commission expects that the need to take action on any amendment before 60 days have elapsed will occur very infrequently.

A. Opportunity To Request a Hearing and Petition for Leave To Intervene

Within 60 days after the date of publication of this notice, any person (petitioner) whose interest may be affected by any of these actions may file a request for a hearing and petition for leave to intervene (petition) with respect to that action. Petitions shall be filed in accordance with the Commission's "Agency Rules of Practice and Procedure" in 10 CFR part 2. Interested persons should consult a current copy of 10 CFR 2.309. If a petition is filed, the Commission or a presiding officer will rule on the petition and, if appropriate, a notice of a hearing will be issued.

Petitions must be filed no later than 60 days from the date of publication of this notice in accordance with the filing instructions in the "Electronic Submissions (E-Filing)" section of this document. Petitions and motions for leave to file new or amended contentions that are filed after the deadline will not be entertained absent a determination by the presiding officer that the filing demonstrates good cause by satisfying the three factors in 10 CFR 2.309(c)(1)(i) through (iii).

If a hearing is requested, and the Commission has not made a final determination on the issue of no significant hazards consideration, the Commission will make a final determination on the issue of no significant hazards consideration, which will serve to establish when the hearing is held. If the final determination is that the amendment request involves no significant hazards consideration, the Commission may issue the amendment and make it immediately effective, notwithstanding the request for a hearing. Any hearing would take place after issuance of the amendment. If the final determination is that the amendment request involves a significant hazards consideration, then any hearing held would take place before the issuance of the amendment unless the Commission finds an imminent danger to the health or safety of the public, in which case it will issue

an appropriate order or rule under 10 CFR part 2.

A State, local governmental body, Federally recognized Indian Tribe, or designated agency thereof, may submit a petition to the Commission to participate as a party under 10 CFR 2.309(h) no later than 60 days from the date of publication of this notice. Alternatively, a State, local governmental body, Federally recognized Indian Tribe, or agency thereof may participate as a non-party under 10 CFR 2.315(c).

For information about filing a petition and about participation by a person not a party under 10 CFR 2.315, see ADAMS Accession No. ML20340A053 (<https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML20340A053>) and on the NRC's public website at <https://www.nrc.gov/about-nrc/regulatory/adjudicatory/hearing.html#participate>.

B. Electronic Submissions (E-Filing)

All documents filed in NRC adjudicatory proceedings, including documents filed by an interested State, local governmental body, Federally recognized Indian Tribe, or designated agency thereof that requests to participate under 10 CFR 2.315(c), must be filed in accordance with 10 CFR 2.302. The E-Filing process requires participants to submit and serve all adjudicatory documents over the internet, or in some cases, to mail copies on electronic storage media, unless an exemption permitting an alternative filing method, as further discussed, is granted. Detailed guidance on electronic submissions is located in the "Guidance for Electronic Submissions to the NRC" (ADAMS Accession No. ML13031A056) and on the NRC's public website at <https://www.nrc.gov/site-help/e-submittals.html>.

To comply with the procedural requirements of E-Filing, at least 10 days prior to the filing deadline, the participant should contact the Office of the Secretary by email at Hearing.Docket@nrc.gov, or by telephone at 301-415-1677, to (1) request a digital identification (ID) certificate, which allows the participant (or its counsel or representative) to digitally sign submissions and access the E-Filing system for any proceeding in which it is participating; and (2) advise the Secretary that the participant will be submitting a petition or other adjudicatory document (even in instances in which the participant, or its counsel or representative, already holds an NRC-issued digital ID certificate). Based upon this information, the Secretary will establish an electronic

docket for the proceeding if the Secretary has not already established an electronic docket.

Information about applying for a digital ID certificate is available on the NRC's public website at <https://www.nrc.gov/site-help/e-submittals/getting-started.html>. After a digital ID certificate is obtained and a docket created, the participant must submit adjudicatory documents in Portable Document Format. Guidance on submissions is available on the NRC's public website at <https://www.nrc.gov/site-help/electronic-sub-ref-mat.html>. A filing is considered complete at the time the document is submitted through the NRC's E-Filing system. To be timely, an electronic filing must be submitted to the E-Filing system no later than 11:59 p.m. ET on the due date. Upon receipt of a transmission, the E-Filing system time-stamps the document and sends the submitter an email confirming receipt of the document. The E-Filing system also distributes an email that provides access to the document to the NRC's Office of the General Counsel and any others who have advised the Office of the Secretary that they wish to participate in the proceeding, so that the filer need not serve the document on those participants separately. Therefore, applicants and other participants (or their counsel or representative) must apply for and receive a digital ID certificate before adjudicatory documents are filed to obtain access to the documents via the E-Filing system.

A person filing electronically using the NRC's adjudicatory E-Filing system may seek assistance by contacting the NRC's Electronic Filing Help Desk through the "Contact Us" link located on the NRC's public website at <https://www.nrc.gov/site-help/e-submittals.html>, by email to MSHD.Resource@nrc.gov, or by a toll-free call at 1-866-672-7640. The NRC Electronic Filing Help Desk is available between 9 a.m. and 6 p.m., ET, Monday through Friday, except Federal holidays.

Participants who believe that they have good cause for not submitting documents electronically must file an exemption request, in accordance with 10 CFR 2.302(g), with their initial paper filing stating why there is good cause for not filing electronically and requesting authorization to continue to submit documents in paper format. Such filings must be submitted in accordance with 10 CFR 2.302(b)-(d). Participants filing adjudicatory documents in this manner are responsible for serving their documents on all other participants. Participants granted an exemption under 10 CFR 2.302(g)(2) must still meet the electronic formatting requirement in

10 CFR 2.302(g)(1), unless the participant also seeks and is granted an exemption from 10 CFR 2.302(g)(1).

Documents submitted in adjudicatory proceedings will appear in the NRC's electronic hearing docket, which is publicly available at <https://adams.nrc.gov/ehd>, unless excluded pursuant to an order of the presiding officer. If you do not have an NRC-issued digital ID certificate as previously described, click "cancel" when the link requests certificates and you will be automatically directed to the NRC's electronic hearing docket where you will be able to access any publicly

available documents in a particular hearing docket. Participants are requested not to include personal privacy information such as social security numbers, home addresses, or personal phone numbers in their filings unless an NRC regulation or other law requires submission of such information. With respect to copyrighted works, except for limited excerpts that serve the purpose of the adjudicatory filings and would constitute a Fair Use application, participants should not include copyrighted materials in their submission.

The following table provides the plant name, docket number, date of application, ADAMS accession number, and location in the application of the licensees' proposed NSHC determinations. For further details with respect to these license amendment applications, see the applications for amendment, which are available for public inspection in ADAMS. For additional direction on accessing information related to this document, see the "Obtaining Information and Submitting Comments" section of this document.

LICENSE AMENDMENT REQUESTS

Florida Power & Light Company, et al.; St. Lucie Plant, Unit 2; St. Lucie County, FL

Docket No	50-389.
Application date	September 11, 2024.
ADAMS Accession No	ML24255A118.
Location in Application of NSHC	Pages 8-9 of Enclosure 1.
Brief Description of Amendment	The proposed license amendment would revise St. Lucie Plant, Unit 2, Technical Specification (TS) 5.6.3, "Core Operating Limits Report," by updating the listing of NRC-approved analytical methods used to determine the core operating limits. Specifically, changes to the fuel thermal-mechanics, core thermal-hydraulics, emergency core cooling, nuclear design, and select design basis event analyses are proposed using NRC-approved advanced codes and methods in support of a St. Lucie Plant, Unit 2, transition to 24-month fuel cycles.
Proposed Determination	NSHC.
Name of Attorney for Licensee, Mailing Address	James Petro, Managing Attorney—Nuclear, Florida Power & Light Company, 700 Universe Boulevard, MS LAW/JB, Juno Beach, FL 33408-0420.
NRC Project Manager, Telephone Number	Natreon Jordan, 301-415-7410.

Southern Nuclear Operating Company, Inc.; Edwin I. Hatch Nuclear Plant, Units 1 and 2; Appling County, GA

Docket Nos	50-321, 50-366.
Application date	September 11, 2024.
ADAMS Accession No	ML24255A892.
Location in Application of NSHC	Pages E-1 to E-3 of the Enclosure.
Brief Description of Amendments	The proposed amendments would modify the Edwin I. Hatch Nuclear Plant, Units 1 and 2, technical specifications (TS) to adopt Technical Specifications Task Force (TSTF)-591, "Revise Risk Informed Completion Time (RICT) Program." TSTF-591 revises TS Section 5.5 Program, "Risk Informed Completion Time Program," to reference Regulatory Guide 1.200, Revision 3 (instead of Revision 2) and to make other changes. Also, a new report would be added to TS Section 5.6, "Reporting Requirements," to inform the NRC of newly developed methods used to calculate a RICT.
Proposed Determination	NSHC.
Name of Attorney for Licensee, Mailing Address	Millicent Ronnlund, Vice President and General Counsel, Southern Nuclear Operating Co., Inc., P.O. Box 1295, Birmingham, AL 35201-1295.
NRC Project Manager, Telephone Number	Dawnmathews Kalathiveettil, 301-415-5905.

Southern Nuclear Operating Company, Inc.; Joseph M. Farley Nuclear Plant, Units 1 and 2; Houston County, AL

Docket Nos	50-348, 50-364.
Application date	September 4, 2024.
ADAMS Accession No	ML24248A273.
Location in Application of NSHC	Pages E-6 through E-8 of the Enclosure.
Brief Description of Amendments	The proposed amendments would revise Technical Specification (TS) 3.4.14, "[Reactor Coolant System] Pressure Isolation Valve (PIV) Leakage," Surveillance Requirement (SR) 3.4.14.3 Acceptance Criteria, remove obsolete requirements found in TS 3.4.14, TS SR 3.4.14.2, and TS 3.3.5, "Loss of Power [LOP] Diesel Generator (DG) Start Instrumentation," in addition to making editorial corrections resulting from these changes.
Proposed Determination	NSHC.
Name of Attorney for Licensee, Mailing Address	Millicent Ronnlund, Vice President and General Counsel, Southern Nuclear Operating Co., Inc., P.O. Box 1295, Birmingham, AL 35201-1295.
NRC Project Manager, Telephone Number	Zachary Turner 415-6303.

Tennessee Valley Authority; Sequoyah Nuclear Plant, Units 1 and 2; Hamilton County, TN

Docket Nos	50-327, 50-328.
Application date	August 28, 2024.

LICENSE AMENDMENT REQUESTS—Continued

ADAMS Accession No	ML24247A185 (Package).
Location in Application of NSHC	Pages E1–11–E1–13 of Enclosure 1.
Brief Description of Amendments	The proposed amendments would revise the Sequoyah Nuclear Plant, Units 1 and 2, fuel handling accident analysis, delete Technical Specification (TS) 3.9.4, “Containment Penetrations,” and modify TS 3.3.6, “Containment Ventilation Isolation Instrumentation.”
Proposed Determination	NSHC.
Name of Attorney for Licensee, Mailing Address	David Fountain, Executive VP and General Counsel, Tennessee Valley Authority, 400 West Summit Hill Drive, WT 6A–K, Knoxville, TN 37902.
NRC Project Manager, Telephone Number	Perry Buckberg, 301–415–1383.

Wolf Creek Nuclear Operating Corporation; Wolf Creek Generating Station, Unit 1; Coffey County, KS

Docket No	50–482.
Application date	August 14, 2024.
ADAMS Accession No	ML24227A556.
Location in Application of NSHC	Pages 3–4 of Attachment I.
Brief Description of Amendment	The proposed amendment would adopt Technical Specifications Task Force (TSTF) Traveler TSTF–569–A, Revision 2, “Revise Response Time Testing Definition.” The proposed changes would revise the technical specification definitions for engineered safety feature and reactor trip system response times.
Proposed Determination	NSHC.
Name of Attorney for Licensee, Mailing Address	Chris Johnson, Corporate Counsel Director, Evergy, One Kansas City Place, 1KC–Missouri HQ 16, 1200 Main Street, Kansas City, MO 64105.
NRC Project Manager, Telephone Number	Samson Lee, 301–415–3168.

III. Notice of Issuance of Amendments to Facility Operating Licenses and Combined Licenses

During the period since publication of the last monthly notice, the Commission has issued the following amendments. The Commission has determined for each of these amendments that the application complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission’s rules and regulations. The Commission has made appropriate findings as required by the Act and the Commission’s rules and regulations in 10 CFR chapter I, which are set forth in the license amendment.

A notice of consideration of issuance of amendment to facility operating

license or combined license, as applicable, proposed NSHC determination, and opportunity for a hearing in connection with these actions, were published in the **Federal Register** as indicated in the safety evaluation for each amendment.

Unless otherwise indicated, the Commission has determined that these amendments satisfy the criteria for categorical exclusion in accordance with 10 CFR 51.22. Therefore, pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared for these amendments. If the Commission has prepared an environmental assessment under the special circumstances provision in 10 CFR 51.22(b) and has

made a determination based on that assessment, it is so indicated in the safety evaluation for the amendment.

For further details with respect to each action, see the amendment and associated documents such as the Commission’s letter and safety evaluation, which may be obtained using the ADAMS accession numbers indicated in the following table. The safety evaluation will provide the ADAMS accession numbers for the application for amendment and the **Federal Register** citation for any environmental assessment. All of these items can be accessed as described in the “Obtaining Information and Submitting Comments” section of this document.

LICENSE AMENDMENT ISSUANCES

Constellation FitzPatrick, LLC and Constellation Energy Generation, LLC; James A. FitzPatrick Nuclear Power Plant; Oswego County, NY

Docket No	50–333.
Amendment Date	September 4, 2024.
ADAMS Accession No	ML24165A038.
Amendment No	356.
Brief Description of Amendment	The amendment revised the technical specifications to change the fuel handling accident analyses in support of the transition from the refuel bridge mast NF–400 (i.e., triangular mast) to the new NF–500 mast.
Public Comments Received as to Proposed NSHC (Yes/No).	No.

Entergy Operations, Inc.; Arkansas Nuclear One, Unit 2; Pope County, AR

Docket No	50–368.
Amendment Date	October 4, 2024.
ADAMS Accession No	ML24185A260.
Amendment No	335.
Brief Description of Amendment	The amendment corrected three typographical errors to Arkansas Nuclear One, Unit 2 (ANO–2) Technical Specification (TS) 6.5.18, “Surveillance Frequency Control Program,” and TS 6.6.8, “Specific Activity,” which were inadvertently introduced into the ANO–2 TSs by License Amendments Nos. 315 (ML19063B948) and 326 (ML21313A008).

LICENSE AMENDMENT ISSUANCES—Continued

Public Comments Received as to Proposed NSHC (Yes/No).	No.
Nebraska Public Power District; Cooper Nuclear Station; Nemaha County, NE	
Docket No	50–298.
Amendment Date	October 8, 2024.
ADAMS Accession No	ML24250A205.
Amendment No	278.
Brief Description of Amendment	The amendment revised Technical Specification (TS) Table 3.3.2.1–1, “Control Rod Block Instrumentation,” to reference the core operating limits report and added a reference to TS 5.6.5, “Core Operating Limits Report (COLR).”
Public Comments Received as to Proposed NSHC (Yes/No).	No.
NextEra Energy Seabrook, LLC; Seabrook Station, Unit No. 1; Rockingham County, NH	
Docket No	50–443.
Amendment Date	September 20, 2024.
ADAMS Accession No	ML24239A538.
Amendment No	175.
Brief Description of Amendment	The amendment modified technical specification limiting condition for operation (LCO) 3.8.1.1, “A.C. Sources—Operating,” by increasing the allowed outage time for an inoperable offsite circuit from 72 hours (3 days) to 240 hours (10 days). The change allowed Seabrook Station, Unit No. 1, to change plant modes from Cold Shutdown (MODE 5) to Startup (MODE 2) to support the replacement of the main generator breaker and outage startup activities while one independent circuit between the offsite transmission network and the onsite Class 1E Distribution System is out of service.
Public Comments Received as to Proposed NSHC (Yes/No).	No.
Nine Mile Point Nuclear Station, LLC and Constellation Energy Generation, LLC; Nine Mile Point Nuclear Station, Units 1 and 2; Oswego County, NY	
Docket Nos	50–220, 50–410.
Amendment Date	September 26, 2024.
ADAMS Accession No	ML24190A001.
Amendment Nos	252 (Unit 1), 197 (Unit 2).
Brief Description of Amendments	The amendments removed the Nine Mile Point 3 Nuclear Project, LLC, (NMP3) designation from the NMP1 and NMP2 technical specifications (TSs) which is not applicable to the current design features of the NMP site. Specifically, Section 5.0, “Design Features,” (Section 5.1, “Site” and Figure 5.1–1) in the NMP1 Technical Specifications (TSs) and Section 4.0, “Design Features,” (Figure 4.1–1) in the NMP2 TS is revised to reflect as the TSs were at the time Constellation Energy Nuclear Group, LLC, the previous owners of NMP1 and NMP2, were pursuing a combined license for NMP3. Additionally, the name “Entergy Nuclear FitzPatrick, LLC” is revised in NMP1 TS Figure 5.1–1 and NMP2 TS Figure 4.1–1 to “Constellation FitzPatrick, LLC,” to reflect the current owner for the James A. FitzPatrick nuclear power plant site.
Public Comments Received as to Proposed NSHC (Yes/No).	No.
Northern States Power Company; Monticello Nuclear Generating Plant; Wright County, MN	
Docket No	50–263.
Amendment Date	October 1, 2024.
ADAMS Accession No	ML24199A175.
Amendment No	212.
Brief Description of Amendment	The amendment revised Technical Specification 3.8.6, “Battery Parameters,” Surveillance Requirement 3.8.6.6, acceptance criteria for the capacity of the 125-volt direct current batteries.
Public Comments Received as to Proposed NSHC (Yes/No).	No.
Northern States Power Company; Prairie Island Nuclear Generating Plant, Units 1 and 2; Goodhue County, MN	
Docket Nos	50–282, 50–306.
Amendment Date	September 27, 2024.
ADAMS Accession No	ML24221A362.
Amendment Nos	245 (Unit 1), 233 (Unit 2).
Brief Description of Amendments	The amendments revised Technical Specification 3.8.1, AC [Alternating Current] Sources—Operating and Surveillance Requirement 3.8.1.2, Note 3, to remove details of a modified diesel generator start and reference to manufacturer’s recommendations.
Public Comments Received as to Proposed NSHC (Yes/No).	No.

LICENSE AMENDMENT ISSUANCES—Continued

Wolf Creek Nuclear Operating Corporation; Wolf Creek Generating Station, Unit 1; Coffey County, KS

Docket No	50–482.
Amendment Date	September 17, 2024.
ADAMS Accession No	ML24199A171.
Amendment No	241.
Brief Description of Amendment	The amendment revised Technical Specification 5.5.11.b for the Ventilation Filter Testing Program by changing the testing requirements for the in place test of the charcoal absorber penetration and system bypass.
Public Comments Received as to Proposed NSHC (Yes/No).	No.

Dated: October 22, 2024.

For the Nuclear Regulatory Commission.

Jamie Pelton,

Deputy Director, Division of Operating Reactor Licensing, Office of Nuclear Reactor Regulation.

[FR Doc. 2024–24963 Filed 10–28–24; 8:45 am]

BILLING CODE 7590–01–P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–101420; File No. SR-CboeBYX–2024–034]

Self-Regulatory Organizations; Cboe BYX Exchange, Inc.; Notice of Filing of a Proposed Rule Change With Respect to Amendments to the Seventh Amended and Restated Bylaws (the “CGM Bylaws”) of Its Parent Corporation, Cboe Global Markets, Inc. (“Cboe” or “Corporation”)

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (the “Act”),¹ and Rule 19b–4 thereunder,² notice is hereby given that on October 11, 2024, Cboe BYX Exchange, Inc. (the “Exchange” or “BYX”) filed with the Securities and Exchange Commission (“Commission”) the proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization’s Statement of the Terms of Substance of the Proposed Rule Change

Cboe BYX Exchange, Inc. (the “Exchange” or “BYX”) is filing with the Securities and Exchange Commission (the “Commission”) a proposed rule change with respect to amendments to the Seventh Amended and Restated Bylaws (the “CGM Bylaws”) of its parent corporation, Cboe Global Markets, Inc. (“Cboe” or “Corporation”).

The text of the proposed rule change is provided in Exhibit 5.

The text of the proposed rule change is also available on the Exchange’s website (http://markets.cboe.com/us/equities/regulation/rule_filings/byx/), at the Exchange’s Office of the Secretary, and at the Commission’s Public Reference Room.

II. Self-Regulatory Organization’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the Exchange included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

A. Self-Regulatory Organization’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

At Cboe’s annual meeting held on May 16, 2024, Cboe’s stockholders considered two advisory proposals that would provide Cboe stockholders with the right to call a special meeting of the stockholders provided that a certain threshold percentage of stockholders propose to call such a meeting. The two proposals were submitted separately. One of the proposals was submitted by an individual stockholder (“Stockholder Proposal”). The other proposal was submitted by Cboe Management (“Management Proposal”). The Stockholder Proposal, which did not pass but received 45% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 10% of Cboe’s voting power to call a special meeting of the stockholders. The Management Proposal, which passed with 65% of the votes cast, requested

that the CGM Board take steps to enable stockholders having at least 25% of Cboe’s voting power to call a special meeting of the stockholders.

The Nominating & Governance Committee of the CGM Board reviewed the voting results of the Stockholder Proposal and the Management Proposal and discussed the stockholder voting standards and rights contemplated by the CGM Bylaws. Following this review, the Nominating & Governance Committee recommended to the CGM Board, and the CGM Board approved, certain changes to the CGM Bylaws to implement the Management Proposal. The CGM Board also approved amending the CGM Bylaws to improve the governance processes of Cboe, to make certain provisions more consistent with Delaware General Corporation Law (“DGCL”), and to make clarifying and cleanup changes to the CGM Bylaws. The proposed rule change amends the CGM Bylaws to implement the changes approved by the CGM Board.

Proposed Changes to Article 2—Stockholders

Current Section 2.3 (Special Meeting) of the CGM Bylaws provides that only the Chair of the Board, the Chief Executive Officer or the CGM Board may call a special meeting of the stockholders. To respond to feedback from its stockholders, as discussed above, Cboe proposes to delete portions of this provision and add language that will provide Cboe stockholders with the right to call special stockholder meetings (a “Stockholder Requested Special Meeting”) after following particular procedures.

In defining the procedural requirements, Cboe’s goals are to ensure timely notice of a meeting request and to gather sufficient information about the proposing stockholder(s) and the proposed business itself. Among other things, this information will help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to adequately assess proposed business

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b–4.

submitted by stockholders. Additionally, Cboe notes that the proposed terms are common among public companies that have adopted a right for stockholders to call special meetings. The proposed changes to the CGM Bylaws to effect the stockholder special meeting right are set forth below.

Revisions to Section 2.3(a)

First, the proposed changes to Section 2.3(a) provide that a Stockholder Requested Special Meeting may be called: (i) at any time by the CGM Board pursuant to a resolution adopted by the affirmative vote of a majority of the total number of CGM directors then in office; or (ii) by Cboe's Corporate Secretary following the receipt of a written request in proper form for a special meeting (a "Special Meeting Request") by one or more stockholders. In order to call a special meeting, the stockholders must hold, in the aggregate, at least 25% of Cboe's outstanding shares of common stock entitled to vote on matters brought before the special meeting (the "Requisite Percentage").

The proposed changes to Section 2.3(a) also clarify that the Chair of the Board, the Chief Executive Officer or the President of Cboe may not individually call a special meeting of the stockholders. This change was made to vest authority within Cboe to call a special meeting in the Board. Without the proposed change, the Chair of the Board, Chief Executive Officer and the President could each call a special meeting of the stockholders without CGM Board approval. The proposed change to Section 2.3(a) simplifies this requirement to confirm that, within Cboe, only the CGM Board may call for a special meeting of the stockholders.

Proposed Section 2.3(b) and Section 2.3(c)

Proposed Section 2.3(b) and Section 2.3(c) set forth the procedures a stockholder must follow in order to submit a written request in proper form to call a Stockholder Requested Special Meeting. Stockholders must first submit a request to Cboe's Corporate Secretary to define a date on which the Requisite Percentage will be determined (the "Record Date"). A stockholder must sign any request to set a Record Date and also provide a reasonably brief description of the purpose or purposes of the special meeting of the stockholders. A stockholder is also required in the request to set a Record Date to disclose certain information regarding themselves and any individuals or entities such stockholder may be associated with (a "Stockholder Associated Person(s)"), as well as such

information concerning any nominees to the CGM Board ("Stockholder Nominee(s)") if such stockholder is so proposing. The information that a stockholder must disclose regarding Stockholder Associated Persons and Stockholder Nominees is contained in Section 2.11 of the CGM Bylaws and incorporated by reference in this Section 2.3(b). The information required to be provided in the request to set a Record Date provides Cboe with notice that a stockholder is seeking to bring business before the stockholders and assists with the logistical aspects of determining which stockholders will be counted for purposes of determining whether the Requisite Percentage is met.

Proposed Section 2.3(d) and Section 2.3(e)

Proposed Section 2.3(d) and Section 2.3(e) include detailed information on the requirements for a Special Meeting Request to have been properly delivered, subject to certain carve-outs for stockholders who submit their request in response to a solicitation for public consent by the Corporation made pursuant to Section 14 of the Exchange Act. Specifically, a Special Meeting Request must:

- be delivered within 60 days following the Record Date;
- be signed by each stockholder making up the Requisite Percentage;
- contain a reasonably brief description of the purpose of the special meeting;
- include details of each stockholder holding the Requisite Percentage, including:
 - The stockholder's name;
 - The stockholder's address;
 - information concerning the stockholder submitting the Special Meeting Request and any Stockholder Associated Persons;
 - information concerning any Stockholder Nominees; and
 - documentary evidence that the shares included in the Requisite Percentage are owned by such stockholder;
- include an acknowledgment that any reduction in the number of shares owned by such stockholders as of the date of such Special Meeting Request and through the meeting date will constitute a revocation of such Special Meeting Request with respect to such reduction;
- relate to an item of business that is a proper subject for stockholder action under applicable law;
- not include an item of business that did not appear on the request to set a Record Date;

- not be delivered during the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting and ending on the date of the next annual meeting; and

- otherwise comply with applicable law.

In defining the requirements for a Special Meeting Request, Cboe's goal is to gather sufficient information about the stockholder seeking to request a special meeting and the proposed business for both itself and its stockholders and to help ensure the efficient use of corporate resources by restricting a stockholder from raising items that could reasonably be addressed at an annual meeting of the stockholders, as in the requirement that a Special Meeting Request not be delivered in the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting. Overall, this information is designed to help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to assess the proposed business or Stockholder Nominee adequately.

Proposed Section 2.3(f)

Proposed Section 2.3(f) provides that the CGM Board may cancel a special meeting in its discretion if the percentage of stock held by the stockholders requesting a special meeting falls below the Requisite Percentage at any point after sixty (60) days from the first date on which a valid Special Meeting Request is delivered to Cboe. This provides the CGM Board with discretion to reevaluate the Special Meeting Request in the event the Special Meeting Request is revoked by stockholders holding a sufficient percentage of the stock of the Corporation.

Proposed Section 2.3(g)

Proposed Section 2.3(g) provides that within ten (10) days following the date on which the Secretary has received valid Special Meeting Requests, the CGM Board shall fix the record date and meeting date, time and location for the Stockholder Requested Special Meeting, provided that the date of any such Stockholder Requested Special Meeting shall not be more than ninety (90) days after the date on which a valid Special Meeting Request is received by Cboe. The CGM Board may submit its own proposal or proposals for consideration at any Stockholder Requested Special Meeting. Ninety (90) days allows the Corporation reasonable time to assess

the items proposed in the Special Meeting Request while also not imposing a potentially burdensome delay on the stockholders.

Proposed Section 2.3(h)

Proposed Section 2.3(h) provides that multiple Special Meeting Requests may be considered together if (i) each Special Meeting Request identifies the same or substantially the same purpose or purposes of the Stockholder Requested Special Meeting and the same or substantially the same items of business proposed to be brought before the Stockholder Requested Special Meeting, and (ii) such Special Meeting Requests have been dated and delivered to the Corporate Secretary within sixty (60) days of the delivery to the Corporate Secretary of the earliest dated Special Meeting Request relating to such item(s) of business. This proposed section helps to ensure the efficient use of corporate resources by preventing multiple stockholders from raising items that should reasonably be consolidated. The conditions under which the Corporation may combine multiple Special Meeting Requests are sufficiently limited to require that each unique item is addressed separately.

Revisions to Section 2.9

Section 2.9 of the CGM Bylaws governs proxy representation. It is proposed that language be added to clarify that any stockholder directly or indirectly soliciting proxies from other stockholders of the Corporation may use any proxy card color other than white, which shall be reserved for exclusive use by the CGM Board.

Revisions to Section 2.11

Section 2.11 of the CGM Bylaws, which are the “advance notice bylaws”,³ requires stockholders to notify Cboe, during a specified period in advance of an annual meeting or special meeting called by the CGM Board, of their intention to nominate one or more persons for election to the CGM Board or to present a business proposal for consideration by the stockholders at the meeting and provide certain information regarding such request. When designing the proposed procedural requirements for stockholders to call a special meeting, as outlined above, Cboe

evaluated the existing procedural requirements for stockholders to bring business before an annual meeting or to nominate director candidates at an annual meeting or special meeting. Cboe has determined that the advance notice bylaws may be enhanced to help achieve the core objectives of fulsome disclosure and accurate explanations from stockholders bringing business or potential nominees before a stockholder meeting. While advance notice bylaws are beneficial in providing a company and its stockholders with information regarding stockholders, and their Stockholder Associated Persons, seeking to bring business or potential nominees before a stockholder meeting, therefore permitting orderly meetings and election contests, and assisting the board’s information gathering and disclosure functions, the Delaware Supreme Court in *Kellner v. AIM ImmunoTech Inc.*⁴ has recently provided some guidance on circumstances where such requests may be overbroad or request information not sufficiently connected to the legitimate information gathering function these provisions serve. Therefore, as further detailed below, Cboe has determined that it would be beneficial to refine certain of the provisions in the CGM Bylaws to increase the clarity of the requests for information from stockholders seeking to bring business before a meeting.

First, Section 2.11(a)(iii)(C) of the CGM Bylaws currently defines the information required to be disclosed regarding a stockholder providing notice of nominations or other business, any Stockholder Associated Person(s) and any Stockholder Nominee(s). Cboe proposes certain amendments to this section to (i) clarify the information a stockholder is required to disclose relating to arrangements between the stockholder providing notice or any Stockholder Associated Person and any other stockholder with regard to the stockholder meeting and (ii) eliminate disclosures on performance related fees to which such stockholder or Stockholder Associated Person may be entitled as a result of any increase or decrease in the stock of Cboe, and the prospectus or similar document of the stockholder providing notice or any Stockholder Associated Person. Cboe believes that, while these provisions as currently written provide valuable information to the Corporation and its stockholders in assessing the proposed business or Stockholder Nominee, these requirements should be sufficiently

specific so as not to potentially dissuade stockholders from bringing business before a stockholder meeting and should otherwise comply with Delaware law. The proposed changes narrow the information required to be disclosed such that Cboe is able to help ensure the objectives of the provisions are met without burdening stockholders with potentially overbroad requests for information.

Section 2.11(a)(iii)(D) of the CGM Bylaws currently sets forth certain representations that must be made by a stockholder seeking to bring business or a Stockholder Nominee before a stockholder meeting regarding whether such stockholder is part of a group which intends to deliver or solicit proxies from stockholders in support of such proposed business. Cboe proposes changes to update this section in order to be more consistent with the universal proxy rules provided for in Rule 14a–19 of the Exchange Act by explicitly stating that any stockholder providing notice that they intend to solicit proxies in support of a proposed nominee must do so in accordance with Rule 14a–19 of the Exchange Act. Cboe also proposes to clarify that the representation must confirm whether the stockholder intends or is part of a group which intends to engage in a solicitation (within the meaning of Rule 14a–1(1) of the Exchange Act) with respect to the nomination of any proposed nominee or proposed business to be considered at the meeting.

Section 2.11(a)(iii)(F) of the CGM Bylaws currently requires that a Stockholder Nominee furnish any information that Cboe may determine is required for Cboe to determine the qualifications of such Stockholder Nominee to serve as a director of the Corporation. Cboe proposes to add language clarifying that the information Cboe may require must be consistent with the parameters set forth in Cboe’s Corporate Governance Guidelines or the CGM Board’s past practice in evaluating potential director nominees.

Proposed Section 2.11(c)(ii) of the CGM Bylaws requires the stockholder providing notice to notify the Secretary of any inaccuracy or change in any information submitted pursuant to Section 2.11 within two (2) business days of becoming aware of such inaccuracy or change. Cboe proposes to modify this requirement by narrowing the scope of circumstances in which a stockholder is required to provide notice of any inaccuracy or change of information that they have previously provided to material inaccuracies or changes.

³ “Advance notice bylaws” allow stockholder(s) to bring business before an annual or special meeting of stockholders, but set forth procedural requirements to help ensure that companies and boards have sufficient information about the proposal and the proposing stockholder(s), as well as adequate time to consider the proposal, by requiring the proposing stockholder(s) to give advance notice of the intention to bring the proposal before the annual or special meeting.

⁴ *Kellner v. AIM ImmunoTech Inc.*, C.A. 2023–0879–LWW (Del. Ch. Jan. 5, 2024).

Proposed Section 2.11(c)(iii) of the CGM Bylaws provides that any stockholder or Stockholder Associated Person providing notice with respect to any Stockholder Nominee is required to do so in a manner consistent with the requirements for universal proxy rules pursuant to Rule 14a–19 of the Exchange Act. Namely, the nomination of a Stockholder Nominee shall be disregarded if, among other things, there is no longer an intent to solicit proxies in support of a Stockholder Nominee or there is a failure to comply with the applicable requirements of Rule 14a–19. Upon request by the Corporation, if any stockholder providing notice or any Stockholder Associated Person provides notice pursuant to Rule 14a–19(b) under the Exchange Act, such stockholder providing notice shall deliver to the Corporate Secretary, no later than five (5) business days prior to the applicable meeting date, then reasonable evidence that the requirements of Rule 14a–19(a)(3) under the Exchange Act have been satisfied.

Currently Section 2.11(c)(vi) of the CGM Bylaws defines “Stockholder Associated Person” to mean, among other things, (i) any person who is a member of a “group” (used in Rule 13d–5 under the Exchange Act) with, or otherwise acting in concert with, any stockholder providing notice, (ii) any person that is directly or indirectly controlled by, or under common control with, such stockholder or such Stockholder Associated Person, or (iii) any person directly or indirectly controlling any such stockholder or any Stockholder Associated Person. The proposed rule change reflects recent developments in Delaware law to add specificity to the definition and limit which individuals may be determined to be a Stockholder Associated Person and makes other clarifying changes. Specifically, the proposed rule change adds the qualifier that a Stockholder Associated Person must be known by the stockholder to be acting in concert with such stockholder, removes from the definition any person directly or indirectly controlled by, or under common control with such stockholder and replaces it with any affiliate or associate of such stockholder providing notice, and deletes the reference in the definition to any person directly or indirectly controlling any such stockholder or Stockholder Associated Person. The proposed rule change also adds any Stockholder Nominee to the definition of Stockholder Associated Person.

Revisions to Other Sections of the Bylaws

Cboe also proposes to make changes to Section 2.11 to reflect recent developments in Delaware law and to provide clarifications and prevent confusion. Cboe proposes to add a note to Section 2.11(a)(ii) that any proposed business for a stockholder meeting must be a proper matter for stockholder action. Cboe also proposes to amend Section 2.11(a)(iii)(B) to state that a Stockholder Nominee’s written consent must be included in Cboe’s proxy statement before they may be brought before a meeting. Previously, Section 2.11(a)(iii)(B) had stated that the Stockholder Nominee’s written consent must be included in a proxy statement, but had not specifically defined it as Cboe’s proxy statement. Cboe also proposes to amend the same section to state that a Stockholder Nominee will not enter into any commitment to vote in a certain manner if nominated to the CGM Board. Previously, this section had simply stated that a Stockholder Nominee may not enter into any commitment to vote in a certain manner with respect to certain matters at any company, without defining Cboe specifically. Cboe also proposes to amend the same section to require that a Stockholder Nominee not omit facts that are necessary to ensure statements made are not misleading in any material respect. Previously, the Stockholder Nominee’s responsibility to not omit facts that are necessary to ensure statements are not misleading was not subject to materiality.

Cboe also proposes to make changes to Section 3.10 of the CGM Bylaws to provide that the Lead Director of Cboe may call a special meeting of the CGM Board. Section 3.10 currently permits, among other things, the Chair of the Board or the Chief Executive Officer to call a special meeting of the CGM Board. Revising this section to allow the Lead Director to call a special meeting of the CGM Board addresses a potential scenario in which the Chair of the Board and the Chief Executive Officer positions are jointly held by one individual and a special meeting of the CGM Board is not able to be called by individual independent directors.

2. Statutory Basis

The Exchange believes the proposed rule change is consistent with the Act and the rules and regulations thereunder applicable to the Exchange and, in particular, the requirements of Section 6(b) of the Act.⁵ Specifically,

the Exchange believes the proposed rule change is consistent with the Section 6(b)(5)⁶ requirements that the rules of an exchange be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.

In light of an advisory vote by the stockholders of Cboe, Cboe is proposing changes to its Bylaws to implement a right for stockholders to call a special meeting of the stockholders at a 25% threshold. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) of the Act because the proposed rule change would be consistent with and facilitate a governance and regulatory structure that is designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to, and perfect the mechanism of a free and open market and a national market system and, in general, to protect investors and the public interest. Particularly, the Exchange believes that, by permitting stockholders of Cboe to bring business or Stockholder Nominees before a special meeting, the proposed rule change strengthens the corporate governance of the Exchange’s ultimate parent company, which is beneficial to both investors and the public interest.

Additionally, the procedural requirements are designed to help protect investors by stating clearly and explicitly the procedures stockholders must follow in order to bring business or Stockholder Nominees before a special meeting. The informational requirements are designed to enhance investor protection by helping to ensure among other things, that the Corporation and its stockholders have full and accurate information about nominating stockholders and Stockholder Nominees and that such stockholders and nominees comply with applicable laws, regulations and other requirements.

The changes that the Exchange is proposing with regard to so-called “advance notice bylaws” in light of the

⁵ 15 U.S.C. 78f(b).

⁶ 15 U.S.C. 78f(b)(5).

recent developments in Delaware law are designed to help provide additional clarity to stockholders wishing to bring business before a stockholder meeting or propose a Stockholder Nominee. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) by simplifying the requirements and clarifying the information that must be disclosed by stockholders. This furthers the interests of investors and the public by removing potential impediments to raising business or proposing Stockholder Nominees that may otherwise restrict a stockholder's ability to participate in the corporate governance of the Corporation.

Finally, the remaining changes to existing provisions of the CGM Bylaws are clarifying in nature, and they enhance investor protection and the public interest by preventing confusion with respect to the operation of the Bylaw provisions.

B. Self-Regulatory Organization's Statement on Burden on Competition

Because the proposed rule change relates to the governance of the Corporation and not to the operations of the Exchange, the Exchange does not believe that the proposed rule change will impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. The proposed rule change is not designed to address any competitive issue or have any impact on competition; rather, adoption of a stockholder special meeting provision, updating "advance notice bylaws," and other bylaws updates by the Corporation are intended to enhance corporate governance and accountability to stockholders.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

The Exchange neither solicited nor received comments on the proposed rule change.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the Exchange consents, the Commission will:

A. by order approve or disapprove such proposed rule change, or

B. institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-CboeBYX-2024-034 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

All submissions should refer to file number SR-CboeBYX-2024-034. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR-CboeBYX-2024-034 and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁷

Sherry R. Haywood,

Assistant Secretary.

[FR Doc. 2024-25058 Filed 10-28-24; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-101411; File No. SR-BX-2024-041]

Self-Regulatory Organizations; Nasdaq BX, Inc.; Notice of Filing and Immediate Effectiveness of Proposed Rule Change To Allow Unlimited External Distribution of Derived Data From BX Options Trade Outline

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act"),¹ and Rule 19b-4 thereunder,² notice is hereby given that on October 9, 2024, Nasdaq BX, Inc. ("BX" or "Exchange") filed with the Securities and Exchange Commission ("Commission") a proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization's Statement of the Terms of Substance of the Proposed Rule Change

The Exchange proposes to amend the Exchange's fees to allow unlimited external distribution of Derived Data from BX Options Trade Outline.

The text of the proposed rule change is available on the Exchange's website at <https://listingcenter.nasdaq.com/rulebook/bx/rules>, at the principal office of the Exchange, and at the Commission's Public Reference Room.

II. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the Exchange included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of

⁷ 17 CFR 200.30-3(a)(12).

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

the most significant aspects of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

The purpose of the proposed rule change is to allow unlimited external distribution of Derived Data from BX Options Trade Outline for a monthly fee of \$3,000.³

BX Options Trade Outline

BX Options Trade Outline provides aggregate quantity and volume information for trades on the Exchange for all series⁴ during a trading session.⁵ Information is provided on an End of Day, Intra-Day, and historical basis in the following categories: (i) total exchange volume for Intra-Day information and total exchange and industry volume for End of Day information for each reported series; (ii) open interest for the series; (iii) aggregate quantity of trades and aggregate trade volume effected to open a position,⁶ characterized by origin type (Customers,⁷ Broker-Dealers,⁸ BX Options Market Makers,⁹ Firms,¹⁰ and

Professionals¹¹); and (iv) aggregate quantity of trades and aggregate trade volume effected to close a position,¹² characterized by origin type (Customers, Broker-Dealers, BX Options Market Makers, Firms, and Professionals).¹³

End of Day Information

The BX Trade Outline End of Day file provides opening buy, closing buy, opening sell and closing sell information, including option first trade price, option high trade price, option low trade price, and option last trade price. The End of Day file is updated during an overnight process with additional fields¹⁴ and is available the following morning, providing aggregate data for the entire trading session.

Intra-Day Information

Intra-Day information is released in scheduled "snapshots" available every 10 minutes for all options series over the course of the trading day. These snapshots are updated to reflect whatever activity occurred, or to indicate that no activity occurred.¹⁵

Historical Information

Historical data is available through ad hoc requests for information in both End of Day and Intra-Day formats for all option series traded for every calendar month after December 2014, based on specific request.¹⁶

³ This proposal was initially filed on September 27, 2024, as SR-BX-2024-039. On October 9, 2024, that filing was withdrawn and replaced with the instant filing to provide further clarification.

⁴ Every options series trades as a distinct symbol; the terms "series" and "symbol" are therefore synonyms.

⁵ See Securities Exchange Act Release No. 100792 (August 21, 2024), 89 FR 68676 (August 27, 2024) (SR-BX-2024-028).

⁶ This would include the aggregate number of "opening purchase transactions," defined as a BX Options Transaction that creates or increases a long position in an options contract, *see* Options 1, Section 1(a)(35), and the aggregate number of "opening writing transactions," defined as a BX Options Transaction that creates or increases a short position in an options contract. *See* Options 1, Section 1(a)(36).

⁷ The term "Customer" applies to any transaction that is identified by a Participant for clearing in the Customer range at The Options Clearing Corporation ("OCC") which is not for the account of broker or dealer or for the account of a "Professional" (as that term is defined in Options 1, Section 1(a)(48)). *See* Options 7, Section 1(a).

⁸ The term "Broker-Dealer" applies to any transaction which is not subject to any of the other transaction fees applicable within a particular category. *See* Options 7, Section 1(a).

⁹ The term "BX Options Market Maker" is a Participant that has registered as a Market Maker on BX Options pursuant to Options 2, Section 1, and must also remain in good standing pursuant to Options 2, Section 9. In order to receive Market Maker pricing in all securities, the Participant must be registered as a BX Options Market Maker in at least one security. *See* Options 7, Section 1(a).

¹⁰ The term "Firm" applies to any transaction that is identified by a Participant for clearing in the Firm range at OCC. *See* Options 7, Section 1(a).

¹¹ The term "Professional" means any person or entity that (i) is not a broker or dealer in securities, and (ii) places more than 390 orders in listed options per day on average during a calendar month for its own beneficial account(s) pursuant to Options 1, Section 1(a)(48). All Professional orders shall be appropriately marked by Participants. *See* Options 7, Section 1(a).

¹² This would include the aggregate number of "closing purchase transactions" in the affected series, defined as a BX Options Transaction that reduces or eliminates a short position in an options contract, *see* Options 1, Section 1(a)(19), and the aggregate number of "closing writing transactions," defined as a BX Options Transaction that reduces or eliminates a long position in an options contract. *See* Options 1, Section 1(a)(20).

¹³ These are the same types of information available on PHOTO, and the other trade outline products offered by Nasdaq exchanges.

¹⁴ The additional fields are: First Trade Price, High Trade Price, Low Trade Price, Last Trade Price, Underlying Close, Moneyness, Total Exchange volume, Total Industry Volume for the Series, and Open Interest.

¹⁵ Subscribers will receive the first snapshot at 9:42 a.m. ET, representing data captured from 9:30 a.m. to 9:40 a.m., and the second calculation at 9:52 a.m., representing data from both the most recent snapshot and previous snapshots, and continuing over the course of the trading day. The final Intra-Day snapshot will be distributed at 4:15 p.m.

¹⁶ Market participants generally use historical files for model testing and research, and the period of time required by a particular market participant will depend on its unique testing and research needs as well as whether it is using End of Day or Intra-Day information. Some customers, for example, may request years of data, while others

BX Options Trade Outline includes proprietary Exchange trading data and does not disseminate any intra-day trading data from any other exchange.¹⁷

The information provided, both in End of Day and Intra-Day formats, is not a real-time data feed.

BX Options Trade Outline is a completely voluntary product in that the Exchange is not required by any rule or regulation to make this data available and potential subscribers may purchase it only if they voluntarily choose to do so.

Nasdaq's experience is that investment banks, market makers, asset managers and other buy-side investors purchase trade outline products.

Proposed Fees

The Exchange proposes to allow unlimited external distribution of Derived Data from BX Options Trade Outline for a monthly fee of \$3,000. This will encourage Distributors to create and sell analytic products to the general investing public. External distribution of Derived Data is not currently permitted. The same Derived Data license is also offered by the Nasdaq PHLX, LLC ("Phlx"),¹⁸ Nasdaq ISE, LLC ("ISE"),¹⁹ and Nasdaq GEMX, LLC ("GEMX")²⁰ exchanges and the Nasdaq Stock Market LLC ("Nasdaq Options Market" or "NOM").²¹ A Derived Data license is also being proposed for the MRX exchange concurrently with this proposal.

Derived Data is "any information generated in whole or in part from Exchange Information²² such that the information generated cannot be reverse engineered to recreate Exchange Information, or be used to create other data that is recognizable as a reasonable substitute for such Exchange Information."

only months, or even a single month. The same principle applies to End of Day vs. Intra-Day information.

¹⁷ The End of Day report includes a field that presents Total Industry Volume for the Series.

¹⁸ See Securities Exchange Act Release No. 93293 (October 12, 2021), 86 FR 57716 (October 18, 2021) (SR-Phlx-2021-58).

¹⁹ See ISE Options 7, Section 10(A).

²⁰ See GEMX Options 7, Section 7(D).

²¹ See Nasdaq Options 7, Section 4.

²² "Exchange Information" is any data or information that has been collected, validated, processed and/or recorded by the Exchange and made available for transmission relating to: (i) eligible securities or other financial instruments, markets, products, vehicles, indicators, or devices; (ii) activities of the Exchange; or (iii) other information or data from the Exchange. Information includes, but is not limited to, any element of information used or processed in such a way that Exchange Information or a substitute for such Information can be identified, recalculated or re-engineered from the processed information.

Fees for external distribution of Derived Data from BX Options Trade Outline are in addition to fees for the End of Day product or the Intraday product, or both, as applicable.

The proposal is designed to promote the dissemination of a variety of analytical insights—generally used only by investment banks, market makers, asset managers and other buy-side investors—to the general investing public by creating an incentive for market data vendors to identify, develop, and sell sentiment indicators and other products. The proposal will spur competition among not only exchanges, but vendors as well, thereby promoting innovation and improving the dissemination of information to the general investing public.

2. Statutory Basis

The Exchange believes that its proposal is consistent with Section 6(b) of the Act,²³ in general, and furthers the objectives of Sections 6(b)(4) and 6(b)(5) of the Act,²⁴ in particular, in that it provides for the equitable allocation of reasonable dues, fees and other charges among members and issuers and other persons using any facility, and is not designed to permit unfair discrimination between customers, issuers, brokers, or dealers.

Equitable Allocation of Reasonable Dues, Fees and Other Charges

The proposed changes are an equitable allocation of reasonable dues, fees and other charges because: (i) the trade profile products offered by multiple exchanges are substitutes, and customers are free to choose which product they purchase; and (ii) the proposed fees are comparable to the fees charged by other exchanges, and customers are free to purchase other products if the Exchange has mistaken the value of its product.

Substitution

Products similar to Trade Outline are offered by many exchanges, including Nasdaq affiliates such as Phlx,²⁵ ISE,²⁶ GEMX,²⁷ and NOM,²⁸ and options

markets not affiliated with Nasdaq such as Cboe Options Exchange (“Cboe”),²⁹ NYSE American Options (“NYSE American”),³⁰ NYSE Arca Options (“NYSE Arca”),³¹ BOX Options Market LLC (“BOX”),³² and MIAAX Pearl Options Exchange (“Pearl”).³³

All of the trade outline products offered by the Nasdaq-affiliated exchanges include a license for the unlimited external distribution of Derived Data.³⁴ As noted above, MRX will be proposing the same license together with this proposal. All of these Derived Data licenses are direct substitutes.

The underlying trade outline data provided by one exchange is generally similar to that provided by other exchanges because order flow can move from one exchange to another, and market sentiment trends that appear on one exchange are likely to be similar to the sentiment trends on other exchanges. The key differentiator among trade outline products depends on the volume of transactions on a given exchange; the greater the volume of transactions, the greater the value of the data. Customers generally purchase sufficient data to provide a view of the market, but not more, as the value of data from each additional exchange yields diminishing returns. Because customers can substitute trade outline products among exchanges, customers can also substitute the proposed Derived Data license for BX with the Derived Data licenses of any of its affiliates.

The proposed Derived Data license is also subject to potential competition

from exchanges not affiliated with Nasdaq. Although the Exchange is not aware of any exchanges offering a Derived Data license for trade outline other than its own affiliates, any exchange that wishes to allow distribution of a Derived Data product based on options trading information would be able to do so with an immediately effective fee filing similar to this proposal.

All trade outline products are optional. Customers can, and do, choose to forego the information from Trade Outline or any of its competitor products when making a trade, and the same holds for Derived Data from trade outline products.

As the Commission and courts³⁵ have recognized, “[i]f competitive forces are operative, the self-interest of the exchanges themselves will work powerfully to constrain unreasonable or unfair behavior.”³⁶ Accordingly, “the existence of significant competition provides a substantial basis for finding that the terms of an exchange’s fee proposal are equitable, fair, reasonable, and not unreasonably or unfairly discriminatory.”³⁷ The Commission and the courts have repeatedly expressed their preference for competition over regulatory intervention in determining prices, products, and services in the securities markets. In Regulation NMS, while adopting a series of steps to improve the current market model, the Commission highlighted the importance of market forces in determining prices and SRO revenues, and also recognized that current regulation of the market system “has been remarkably successful in promoting market competition in its

²⁹ See, e.g., Securities Exchange Act Release No. 94913 (May 13, 2022), 87 FR 30534 (May 19, 2022) (SR-Cboe-2022-023) (describing End of Day and Intra-Day Open-Close Data as a summary of trading activity on the exchange at the option level by origin, side of the market, price, and transaction type).

³⁰ See, e.g., Securities Exchange Act Release No. 93803 (December 16, 2021), 86 FR 72647 (December 22, 2021) (SR-NYSEAMER-2021-46) (describing the NYSE Options Open-Close Volume Summary as a volume summary of trading activity on the exchange at the option level by origin, side of the market, contract volume and transaction type).

³¹ See, e.g., Securities Exchange Act Release No. 93132 (September 27, 2021), 86 FR 54499 (October 1, 2021) (SR-NYSEArca-2021-82) (describing the NYSE Options Open-Close Volume Summary as a volume summary of trading activity on the exchange at the option level by origin, side of the market, contract volume and transaction type).

³² See, e.g., Securities Exchange Act Release No. 97174 (March 21, 2023), 88 FR 18201 (March 27, 2023) (SR-BOX-2023-09) (describing the BOX exchange Open-Close Data report as providing volume by origin, buying/selling, and opening/closing criteria).

³³ See, e.g., Securities Exchange Act Release No. 91964 (May 21, 2021), 86 FR 28667 (May 27, 2021) (SR-PEARL-2021-24) (introducing the Open-Close Report).

³⁴ See *supra* notes 24–27.

³⁵ The decision of the United States Court of Appeals for the District of Columbia Circuit in *NetCoalition v. SEC*, 615 F.3d 525 (D.C. Cir. 2010) upheld the Commission’s reliance upon competitive markets to set reasonable and equitably allocated fees for market data. “In fact, the legislative history indicates that the Congress intended that the market system evolve through the interplay of competitive forces as unnecessary regulatory restrictions are removed and that the SEC wield its regulatory power in those situations where competition may not be sufficient, such as in the creation of a consolidated transactional reporting system.” *NetCoalition I* at 535 (quoting H.R. Rep. No. 94–229, at 92 (1975), as reprinted in 1975 U.S.C.A.N. 321, 323) (internal quotation marks omitted). The court agreed with the Commission’s conclusion that “Congress intended that competitive forces should dictate the services and practices that constitute the U.S. national market system for trading equity securities.” *Id.* (quoting Securities Exchange Act Release No. 59039 (December 2, 2008), 73 FR 74770, 74771 (December 9, 2008) (SR-NYSEArca-2006–21)).

³⁶ See Securities Exchange Act Release No. 59039 (December 2, 2008), 73 FR 74770 (December 9, 2008) (SR-NYSEArca-2006–21).

³⁷ See *id.*

²³ 15 U.S.C. 78f(b).

²⁴ 15 U.S.C. 78f(b)(4) and (5).

²⁵ See Securities Exchange Act Release No. 62887 (September 10, 2010), 75 FR 57092 (September 17, 2010) (SR-Phlx-2010–121) (introducing PHOTO on September 1, 2010).

²⁶ See Nasdaq ISE Rules, Options 7, Section 10(A) and (B) (Nasdaq ISE Open/Close Trade Profile End of Day; Nasdaq ISE Open/Close Trade Profile Intraday).

²⁷ See Nasdaq GEMX Rules, Options 7, Sections 7(D) (Nasdaq GEMX Open/Close End of Day Trade Profile) and 7(E) (Nasdaq GEMX Open/Close Intraday Trade Profile).

²⁸ See Nasdaq Rules, Options 7, Section 4 (Nasdaq Options Trade Outline (“NOTO”)).

broader forms that are most important to investors and listed companies.”³⁸

Because the proposed Derived Data license is currently subject to competition from other Nasdaq exchanges, and potentially subject to competition from other exchanges, the Exchange will be limited in what it is able to charge for the license, and the proposed fee is therefore a reasonable allocation of dues, fees and other charges.

Comparability

The proposed fees for the Derived Data license are comparable to the fees charged by similarly situated exchanges for the same license.

All of the Nasdaq-affiliated exchanges offer a Derived Data license for their trade outline products. As explained above, the value of any trade outline product is determined in part by the number of underlying transactions reflected in the data.

The proposed fees for the Derived Data license are the same as the fees charged by similarly situated exchanges. BX has a market share of approximately 2 percent, similar to that of GEMX (at approximately 3 percent).³⁹ The proposed monthly fee of \$3,000 for the unlimited external distribution of Derived Data is identical to the fee charged by GEMX.⁴⁰

The volume of trading on the BX exchange is also similar to that on the MRX exchange, which has a market share of approximately 4 percent.⁴¹ Together with this filing, MRX will propose the same monthly fee of \$3,000 as BX for the unlimited external distribution of Derived Data.

The Nasdaq-affiliated exchanges with larger market shares have comparably higher fees for the unlimited external distribution of Derived Data. Nasdaq Options Market, with a market share of approximately 5 percent,⁴² has a fee of \$4,000 per month for the unlimited external distribution of Derived Data.⁴³ ISE, with a market share of approximately 7 percent,⁴⁴ has a fee of \$4,500 per month for the unlimited external distribution of Derived Data.⁴⁵ PHLX, with a market share of

approximately 9 percent,⁴⁶ has a fee of \$5,000 per month for the unlimited external distribution of Derived Data.⁴⁷

The proposed fees are therefore comparable to those charged by similarly situated exchanges and consistent with the fees for Derived Data licenses in the market overall. If the Exchange is wrong in its assessment of fees, it will lose sales as a result.

The Proposal Does Not Permit Unfair Discrimination

The proposed Derived Data license is available to all market participants, including members and non-members, and all current and potential distributors, on the same terms. Nothing in the proposal treats any category of market participant any differently from any other category.

It is reasonable and not unfair discrimination to charge an external distributor of Derived Data a \$3,000 licensing fee that is not charged for internal usage. External distribution is fundamentally different than internal use. Vendors ordinarily charge a fee to their downstream customers for this service, and, even if the vendor is not charging a specific fee for this particular service, Derived Data products from the Exchange will be part of a suite of offerings that generally promote sales. It is not unfair discrimination to charge a licensing fee for a product that generates downstream revenue.

It is also not unfair discrimination to allow the redistribution of Derived Data, but not the underlying information. Neither exchanges nor vendors ordinarily allow redistribution of analytic products—such products are typically designed solely for the use of direct customers, not for redistribution to the customers of customers in the manner of a data feed.

The proposed licensing structure provides an incentive for vendors to innovate with new compelling and varied analytic products for the general investing public that will provide access to market sentiment insights currently available only to sophisticated investors.

B. Self-Regulatory Organization's Statement on Burden on Competition

The Exchange does not believe that the proposed rule change will impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. In terms of inter-market competition, the Exchange notes that it operates in a highly competitive market in which market

participants can readily favor competing venues if they deem fee levels at a particular venue to be excessive, or rebate opportunities available at other venues to be more favorable. In such an environment, the Exchange must continually adjust its fees to remain competitive with other exchanges and with alternative trading systems that have been exempted from compliance with the statutory standards applicable to exchanges. Because competitors are free to modify their own fees in response, and because market participants may readily adjust their order routing practices, the Exchange believes that the degree to which fee changes in this market may impose any burden on competition is extremely limited.

Intermarket Competition

Nothing in the proposal burdens inter-market competition (the competition among self-regulatory organizations). As discussed above, BX Trade Outline is subject to direct competition from other options exchanges that offer similar products. Any of these exchanges can replicate this proposal in full or in part, and nothing in the proposal would interfere with the ability of any exchange to do so.

Intra-Market Competition

Nothing in the proposal burdens intra-market competition (the competition among consumers of exchange data). Trade Outline is available to any customer under the same fee schedule as any other customer, and any market participant that wishes to purchase a license to distribute Derived Data can do so on a non-discriminatory basis.

Indeed, the proposal is designed to foster competition for vendors as well as exchanges by creating an incentive for market data vendors to identify, develop, and sell analytic indicators to help investors inform their investments strategies and analytic models.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

No written comments were either solicited or received.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

The foregoing rule change has become effective pursuant to Section 19(b)(3)(A)(ii) of the Act.⁴⁸

³⁸ See Securities Exchange Act Release No. 51808 (June 9, 2005), 70 FR 37496, 37499 (June 29, 2005) (“Regulation NMS Adopting Release”).

³⁹ See *NasdaqTrader.com*, “Options Market Statistics,” available at <https://www.nasdaqtrader.com/Trader.aspx?id=OptionsVolumeSummary>.

⁴⁰ See GEMX Options 7, Section 7(D).

⁴¹ See *supra* note 38.

⁴² See *id.*

⁴³ See Nasdaq Options 7, Section 4.

⁴⁴ See *supra* note 38.

⁴⁵ See ISE Options 7, Section 10(A).

⁴⁶ See *supra* note 38.

⁴⁷ See PHLX Options 7, Section 10.

⁴⁸ 15 U.S.C. 78s(b)(3)(A)(ii).

At any time within 60 days of the filing of the proposed rule change, the Commission summarily may temporarily suspend such rule change if it appears to the Commission that such action is: (i) necessary or appropriate in the public interest; (ii) for the protection of investors; or (iii) otherwise in furtherance of the purposes of the Act. If the Commission takes such action, the Commission shall institute proceedings to determine whether the proposed rule should be approved or disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-BX-2024-041 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.
- All submissions should refer to file number SR-BX-2024-041. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available

publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR-BX-2024-041 and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁴⁹

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2024-25050 Filed 10-28-24; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-101413; File No. SR-Phlx-2024-51]

Self-Regulatory Organizations; Nasdaq PHLX LLC; Notice of Filing of Proposed Rule Change To Amend FLEX Floor Trading Rules

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act"),¹ and Rule 19b-4 thereunder,² notice is hereby given that on October 8, 2024, Nasdaq PHLX LLC ("Phlx" or "Exchange") filed with the Securities and Exchange Commission ("SEC" or "Commission") the proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization's Statement of the Terms of Substance of the Proposed Rule Change

The Exchange proposes to amend Options 8, Section 34, FLEX Trading.³

The text of the proposed rule change is available on the Exchange's website at <https://listingcenter.nasdaq.com/rulebook/phlx/rules>, at the principal office of the Exchange, and at the Commission's Public Reference Room.

⁴⁹ 17 CFR 200.30-3(a)(12).

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

³ Phlx Options 8, Section 34 rule text was previously amended by two rule changes which are effective, but not yet operative. These two prior rule changes will be implemented at the same time as the rule changes proposed herein. See Securities Exchange Act Release Nos. 97658 (June 7, 2023), 88 FR 38562 (June 13, 2023) (SR-Phlx-2023-22); and 100321 (June 12, 2024), 89 FR 51580 (June 18, 2024) (SR-Phlx-2024-24). Phlx further delayed the implementation so that it could implement SR-Phlx-2023-22 while also completing an OCC industry rule change prior.

II. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the Exchange included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

The Exchange proposes to amend Options 8, Section 34, FLEX Trading. The Exchange also proposes a technical amendment to Options 8, Section 33, Accommodation Transactions.

Options 8, Section 34

FLEX Options are customized equity, index, and currency contracts that allow investors to tailor contract terms for exchange-listed equity and index options. By way of background, in 2023, the Exchange filed a rule change to amend the manner in which FLEX Options are transacted on Phlx's Trading Floor.⁴ Thereafter, the Exchange filed to delay the implementation of SR-Phlx-2023-22 to

⁴ See Securities Exchange Act Release No. 97658 (June 7, 2023), 88 FR 38562 (June 13, 2023) (SR-Phlx-2023-22) (Notice of Filing and Immediate Effectiveness of Proposed Rule Change To Amend Various Options 8 Rules). SR-Phlx-2023-22 amended FLEX Orders in 3 ways. First, the Exchange amended the rules to require FLEX Orders to be reported into Phlx's Options Floor Based Management System or "FBMS," thereby further automating the execution and reporting of FLEX Options. All executed FLEX contracts will be reported to OPRA and sent to the OCC for clearing, similar to all other equity, equity index and U.S. dollar-settled foreign currency options orders executed on the Exchange's trading floor. Second, the Exchange removed its RFQ process including the BBO Improvement Interval Process, with the rule change. Third, the Exchange reorganized Options 8, Section 34 to restructure the rule to include additional information which describes current FLEX trading on Phlx. With respect to Cabinet Orders, SR-Phlx-2023-22 amended Options 8, Section 33 to require Cabinet Orders to be reported into FBMS. With this change, members and member organizations will be required to record all Cabinet Orders represented in the trading crowd into FBMS. All executed contracts will be reported to OPRA and sent to OCC for clearing similar to all other equity, equity index and U.S. dollar-settled foreign currency options orders executed on the Exchange's trading floor.

on or before August 30, 2024.⁵ Finally, in 2024, Phlx filed a rule change to amend FLEX Options rules at Options 8, Section 34(b) and further delay the implementation of SR-Phlx-2023-22 to the end of Q4 2025.⁶ At this time, the Exchange proposes to further amend the rules proposed in SR-Phlx-2023-22 and SR-Phlx-2024-24, which are immediately effective, but not yet operative. The Exchange proposes to implement the amendments in Phlx-2023-22 and SR-Phlx-2024-24 at the same time as the proposed amendments.

Specifically, the Exchange proposes to (1) clarify the Options 8, Section 34 functionality that will be available with the implementation of SR-Phlx-2023-22 and SR-Phlx-2024-24; (2) list p.m.-settled FLEX Index Options whose exercise settlement value is derived from closing prices on the last trading day prior to expiration that expire on or within two business days of a third Friday-of-the-month expiration day for a non-FLEX Option; and (3) permit FLEX Options on certain Exchange-Traded Funds (“ETFs”) to be settled by delivery in cash if the underlying security meets prescribed criteria. Each change will be described below.

Options 8, Section 34

First, the Exchange proposes to capitalize certain terms uniformly throughout Options 8, Section 34. The Exchange proposes to capitalize the following terms: “FLEX Options,” “FLEX Equity Options,” “FLEX Index Options,” and “FLEX Currency Options.” The Exchange proposes to amend Options 8, Section 34(f)(4) to define FLEX U. S. dollar-settled foreign currency options as “FLEX Currency Options.”

Second, the Exchange proposes to exclude iShares Bitcoin Trust ETF (“IBIT”) from trading as a FLEX Option.

Third, the Exchange proposes to adopt a new Options 8, Section 34(f)(1)(B) to state, “an underlying equity security or index, as applicable (the index multiplier for FLEX Index Options is 100).” This proposed rule text reflects the current characteristics

of underlying interest for FLEX Option. The proposed rule text brings greater clarity to the Rule.

Fourth, the Exchange proposes to amend the language in Options 8, Section 34(f)(3) which was initially amended to state, “The Exchange may determine the smallest increment for exercise prices of FLEX Options not to exceed two decimal places.” While not substantively amending the exercise price, the Exchange proposes to amend this sentence to state, “The Exchange may determine the smallest increment for exercise prices of FLEX Options on a class-by-class basis without going lower than the \$0.01.” The Exchange believes that the proposed rule text brings greater clarity to Phlx’s rule text and is consistent with rule text in Cboe Rule 5.3(e)(3).⁷

Fifth, the Exchange proposes to amend the language in Options 8, Section 34(f)(5) to provide, “The expiration date may be any business day (specified to the day, month, and year) no more than 15 years from the date on which an executed FLEX equity and index option is submitted to the System and no more than 3 years from the date on which an executed FLEX currency option is submitted to the System with exercise settlement value on the expiration date determined by reference to the reported level of the index as derived from the opening prices of the component securities (“a.m. settlement”) or closing prices (“p.m. settlement”).”⁸ This amendment aligns the rule text related to settlement style required for a complex FLEX Order leg with rule text in Cboe 4.21(b)(4). The Exchange notes that Cboe recently received approval of its pilot program that permitted it to list p.m.-settled FLEX Index Options whose exercise settlement value is derived from closing prices on the last trading day prior to expiration that expire on or within two business days of a third Friday-of-the-month expiration day for a non-FLEX Option (“FLEX PM Third Friday Options”).⁹ Consistent with the

Commission’s approval of Cboe’s proposal, the Exchange is proposing to allow the listing of FLEX PM Third Friday Options on Phlx as well, and will align with Cboe Rule 4.21(b)(5)(B)(ii).¹⁰

Sixth, the Exchange proposes to re-style Options 8, Section 34(f)(6) to change the title from “Settlement” to “Settlement type.” The Exchange also proposes to add a title at (A), “FLEX Equity Options.” At proposed Options 8, Section 34(f)(6)(A)(1) the Exchange proposes to add rule text to state “FLEX Options, other than as permitted in subparagraph (2) below, are settled with physical delivery of the underlying security.” The Exchange proposes to also introduce FLEX Equity Options that are cash-settled in proposed Options 8, Section 34(f)(6)(A)(2). The Exchange will discuss cash-settled FLEX Equity Options in greater detail below. The Exchange proposes to amend Options 8, Section 34(f)(6)(A) to add a title for FLEX Index Options at (B) and change the current rule text¹¹ to instead provide that FLEX Index Options may be specified as the index value reported at the

(1) close (P.M.-settled); and (with exercise settlement value determined by reference to the reported level of the index derived from the reported closing prices of the component securities);

(2) opening (A.M.-settled) of trading on the Exchange (with exercise settlement value determined by reference to the reported level of the index derived from the reported opening prices of the component securities).

While not substantively amending the rule text, the Exchange believes that the proposed text adds clarity by noting how the exercise value is determined depending on whether the option is a.m.-settled or p.m.-settled. The Exchange proposes to add a title “FLEX Currency Options” to new Options 8, Section 34(f)(6)(C). The Exchange also

and a study by the Commission’s Division of Economic and Risk Analysis (“DERA”) staff. See FLEX Settlement Pilot Approval, notes 18 and 35.

¹⁰ Currently, the only broad-based index option that would be able to list as a FLEX PM Third Friday Option is the Nasdaq-100 Index option (“NDX” or “NDX options”). The Exchange also received approval to list a third-Friday-of-the-month p.m. expiration on its standardized market. See Securities Exchange Act Release No. 98950 (November 15, 2023), 88 FR 81172 (November 21, 2023) (SR-Phlx-2023-45) (Order Approving a Proposed Rule Change To Permit the Listing and Trading of P.M.-Settled Nasdaq-100 Index Options With a Third-Friday-of-the-Month Expiration).

¹¹ Initially, the Exchange stated at Options 8, Section 34(f)(6)(A) that “respecting FLEX index options, the settlement value may be specified as the index value reported at the: (i) close (P.M.-settled); and (ii) opening (A.M.-settled) of trading on the Exchange. American style index options exercised prior to the expiration date can only settle based on the closing value on the exercise date. FLEX index options are settled in U.S. dollars.”

⁵ See Securities Exchange Act Release No. 98919 (November 13, 2023), 88 FR 80363 (November 13, 2023) (SR-Phlx-2023-48) (Notice of Filing and Immediate Effectiveness of Proposed Rule Change To Delay the Implementation of the FLEX and Cabinet Automation).

⁶ See Securities Exchange Act Release No. 100321 (June 12, 2024), 89 FR 51580 (June 18, 2024) (SR-Phlx-2024-24) (Notice of Filing and Immediate Effectiveness of a Proposed Rule Change To Delay Implementation of Certain Exchange Options 8 Rules and Amend Options 8, Section 34(b)). Phlx further delayed the implementation so that it could implement SR-Phlx-2023-22 while also completing an OCC industry rule change prior.

⁷ Of note, the Exchange is not proposing to provide for Micro FLEX Index Options or to allow prices to be expressed as a percentage value, similar to Cboe, because the Exchange does not offer these features today.

⁸ The Exchange would remove the rule text in current Options 8, Section 34 (f)(5) that provides, “except that (i) a FLEX index option that expires on or within two business days prior or subsequent to a third Friday-of-the-month expiration day for a non-FLEX option (except quarterly expiring index options) or underlying currency may only have an.”

⁹ See Securities Exchange Act Release No. 99222 (December 21, 2023), 88 FR 89771 (December 28, 2023) (SR-CBOE-2023-018) (“FLEX Settlement Pilot Approval”). In support of making the pilot a permanent program, Cboe cited to its own review of pilot data during the course of the pilot program

proposes a technical amendment to underline “Market Maker” in Options 8, Section 34(g)(3). SR–Phlx–2023–22 inadvertently did not underline that text, thereby designating it as new text.

Seventh, the Exchange proposes to amend Position Limits in Options 8, Section 34(i) to add a new paragraph stating that,

There shall be no position limits for FLEX Equity Options, other than as set forth in this paragraph and (4) below. Position limits for FLEX Equity Options where the underlying security is an ETF that is settled in cash pursuant to subparagraph (f)(6)(A) shall be subject to the position limits set forth in Options 9, Section 13, and subject to the exercise limits set forth in Options 9, Section 15. Positions in such cash-settled FLEX Options shall be aggregated with positions in physically-settled options on the same underlying ETF for the purpose of calculating the position limits set forth in Options 9, Section 13, and the exercise limits set forth in Options 9, Section 15.

The Exchange will describe position limits for an ETF that is settled in cash below with the description of its proposal to permit a cash-settled ETF.

The Exchange proposes to remove certain numbering as unnecessary in proposed Options 8, Section 34(i)(2), which is currently Options 8, Section 34(i)(1). The Exchange would create a new Options 8, Section 34(i)(2) and title it “Reports.” The Exchange would remove “However” from this new paragraph and start the paragraph with “Each.”

The Exchange proposes to add the title “Additional Margin Requirements” to proposed Options 8, Section 34(i)(3).

The Exchange proposes to amend proposed Options 8, Section 34(i)(3), current Options 8, Section 34(i)(3), by renumbering it to “(4)” and adding a title “Aggregation of FLEX Positions.” Further, the Exchange proposes to note that, “For purposes of the position limits and reporting requirements set forth in this Rule, FLEX Option positions shall not be aggregated with positions in non-FLEX Options other than as noted in this subparagraphs (i)(3) and (4), and positions in FLEX Index Options on a given index shall not be aggregated with options on any stocks included in the index or with FLEX Index Option positions on another index.”¹² Pursuant to proposed Options 8, Section 34(i)(4)(a), commencing at the close of trading two business days prior to the last trading day of the calendar quarter, positions in P.M.-settled FLEX Index Options (*i.e.*, FLEX Index Options having an exercise settlement value determined by the level of the index at

the close of trading on the last trading day before expiration) shall be aggregated with positions in Quarterly Options Series on the same index with the same expiration and shall be subject to the position limits set forth in Options 4A, Section 6.¹³ Pursuant to proposed Options 8, Section 34(i)(4)(b), commencing at the close of trading two business days prior to the last trading day of the week, positions in FLEX Index Options that are cash settled¹⁴ shall be aggregated with positions in Short Term Option Series on the same underlying (*e.g.*, same underlying index as a FLEX Index Option) with the same means for determining exercise settlement value (*e.g.*, opening or closing prices of the underlying index) and same expiration, and shall be subject to the position limits set forth in Options 4A, Section 6.¹⁵ Pursuant to proposed Options 8, Section 34(i)(4)(c), as long as the options positions remain open, positions in FLEX Options that expire on a third Friday-of-the-month expiration day shall be aggregated with positions in non-FLEX Options on the same underlying, and shall be subject to the position limits set forth in Options 4A, Section 6, or Options 9, Section 13, as applicable, and the exercise limits set forth in Options 9, Section 15, as applicable.¹⁶

Eighth, the Exchange proposes to amend Exercise Limits in Options 8, Section 34(j) to provide further detail and rearrange the rule text. The Exchange proposes to relocate the rule text in Options 8, Section 34(j)(1) that provides, “Positions in FLEX options shall not be taken into account when calculating exercise limits for non-FLEX options, except as provided in paragraph (d) above. The minimum exercise size shall be the lesser of \$1 million underlying equivalent value for FLEX index options, and 25 contracts for FLEX equity and currency options, or the remaining size of the position.” Instead, the Exchange proposes to provide at Options 8, Section 34(j)(1)(a) that, “The minimum value size for FLEX Equity Option exercises shall be 25 contracts or the remaining size of the position, whichever is less.” Proposed Options 8, Section 34(j)(1)(b) will require that the minimum value size for

FLEX Index Option exercises be \$1 million Underlying Equivalent Value (as defined below) or the remaining Underlying Equivalent Value of the position, whichever is less.¹⁷ Proposed Options 8, Section 34(j)(1)(c) will stipulate that except as provided in proposed subparagraph (i) and (i)(4) above,¹⁸ FLEX Options shall not be taken into account when calculating exercise limits for non-FLEX Option contracts.¹⁹ Proposed Options 8, Section 34(j)(1)(d) will set forth the definition of Underlying Equivalent Value as the aggregate value of a FLEX Index Option (index multiplier times the current index value) multiplied by the number of FLEX Index Options.²⁰ Finally, the Exchange proposes to add a sentence to the end of Options 8, Section 34(j) that provides, “There shall be no exercise limits for broad-based FLEX Index Options (including reduced value option contracts) on the broad-based index options listed in Options 4A, Section 6(a).”

Options 8, Section 33

The Exchange also proposes to make a technical amendment to Options 8, Section 33, Accommodation Transactions, at paragraph (e) to remove correct improperly placed parentheticals from SR–Phlx–2024–22.

Cash-Settled Exchange Traded Funds (“ETFs”)

Generally, FLEX Equity Options will be settled by physical delivery of the underlying security,²¹ while all FLEX Index Options will be settled by delivery in cash.²² The Exchange proposes to allow FLEX Equity Options where the underlying security is an ETF to be settled by delivery in cash if the underlying security meets prescribed criteria. The Exchange notes that cash-settled FLEX ETF Options will be subject to the same trading rules and procedures described in Options 8, Section 34 that will govern the trading

¹⁷ See Cboe Rule 8.42(g)(2) for materially identical provisions.

¹⁸ As described above, proposed Options 8, Section 34(i)(4) will govern the aggregation of FLEX positions generally, while proposed Options 8, Section 34(i)(1) will govern the aggregation of cash-settled FLEX Equity Options specifically and that positions in such cash-settled FLEX Equity Options will be aggregated with positions in physically settled options on the same underlying ETF. Cash-settled FLEX Equity Options will be discussed later in this filing.

¹⁹ See Cboe Rule 8.42(g)(3) for materially identical provisions.

²⁰ See Phlx Options 8, Section 34(b)(8)(D) for materially identical provisions.

²¹ See proposed Options 8, Section 34(f)(6)(A)(1).

²² See proposed Options 8, Section 34(f)(6)(A)(2). As discussed below, cash settlement is also permitted in the OTC market.

¹² The Exchange also proposes to change “shall” to “will in two places in this paragraph.

¹³ See Cboe Rule 8.35(d)(1) for materially identical provisions.

¹⁴ The Exchange notes that all FLEX Index Options will be cash settled. Cash-settled ETFs will be described later in this proposal.

¹⁵ This is based on Cboe Rule 8.35(d)(2), except the Exchange does not currently list Credit Default Options and will therefore not incorporate the applicable portion into its proposed rule.

¹⁶ See Cboe Rule 8.35(d)(3) for materially identical provisions.

of other FLEX Options on the Exchange, with the exception of the rules to accommodate the cash-settlement feature proposed as follows. Today, NYSE American Rule 903G²³ and Cboe Rule 4.21(b)(5)(A)²⁴ allow for cash-settled FLEX ETF Options as well.

To permit cash settlement of certain FLEX ETF Options, the Exchange proposes rule text in Options 8, Section 34(f)(6)(A)(2) to provide that the exercise settlement for a FLEX ETF Option may be by physical delivery of the underlying ETF or by delivery in cash if the underlying security, measured over a defined six-month period,²⁵ has an average daily notional value of \$500 million or more and a national average daily volume (“ADV”) of at least 4,680,000 shares.²⁶

The Exchange also proposes in Options 8, Section 34(f) that a FLEX Equity Option overlying an ETF (cash- or physically-settled) may not be the same type (put or call) and may not have the same exercise style, expiration date, and exercise price as a non-FLEX Equity Option overlying the same ETF.²⁷ In other words, regardless of whether a FLEX Equity Option overlying an ETF is cash or physically settled, at least one of the exercise style (*i.e.*, American-style or European-style), expiration date, and exercise price of that FLEX Option must differ from those terms of a non-FLEX Option overlying the same ETF in order to list such a FLEX Equity Option. For example, suppose a non-FLEX SPY option (which is physically settled, p.m.-settled and American-style) with a specific September expiration and exercise price of 475 is listed for trading. A FLEX Trader could not submit an order to trade a FLEX SPY option (which is p.m.-settled) that is cash-settled (or

physically settled) and American-style with the same September expiration and exercise price of 475.

In addition, the Exchange proposes new Options 8, Section 34(f)(6)(A)(2)(a), which would provide that the Exchange will determine bi-annually the underlying ETFs that satisfy the notional value and trading volume requirements in (f)(6)(A)(2) by using trading statistics for the defined six-month period.²⁸ The proposed rule would further provide that the Exchange will permit cash settlement as a contract term on no more than 50 underlying ETFs that meet the criteria in this subparagraph (f)(6)(A)(2) and that if more than 50 underlying ETFs satisfy the notional value and trading volume requirements, then the Exchange would select the top 50 ETFs that have the highest average daily volume.²⁹

Proposed new Options 8, Section 34(f)(6)(A)(2)(b) would further provide that if the Exchange determines pursuant to the bi-annual review that an underlying ETF ceases to satisfy the requirements under proposed (f)(6)(A)(2)(a), any new position overlying such ETF entered into will be required to have exercise settlement by physical delivery, and any open cash-settled FLEX ETF Option positions may be traded only to close the position.³⁰

The Exchange believes it is appropriate to introduce cash settlement as an alternative contract term to the select group of ETFs because they are among the most highly liquid and actively traded ETF securities. As described more fully below, the Exchange believes that the deep liquidity and robust trading activity in the ETFs identified by the Exchange as meeting the criteria mitigate against historic concerns regarding susceptibility to manipulation.

Characteristics of ETFs

ETFs are funds that have their value derived from assets owned. The net asset value (“NAV”) of an ETF is a daily calculation that is based off the most recent closing prices of the assets in the fund and an actual accounting of the total cash in the fund at the time of calculation. The NAV of an ETF is calculated by taking the sum of the assets in the fund, including any securities and cash, subtracting out any liabilities, and dividing that by the number of shares outstanding.

Additionally, each ETF is subject to a creation and redemption mechanism to ensure the price of the ETF does not fluctuate too far away from its NAV—which mechanisms reduce the potential for manipulative activity. Each business day, ETFs are required to make publicly available a portfolio composition file that describes the makeup of their creation and redemption “baskets” (*i.e.*, a specific list of names and quantities of securities or other assets designed to track the performance of the portfolio as a whole). ETF shares are created when an Authorized Participant,³¹ typically a market maker or other large institutional investor, deposits the daily creation basket or cash with the ETF issuer. In return for the creation basket or cash (or both), the ETF issues to the Authorized Participant a “creation unit” that consists of a specified number of ETF shares. For instance, IWM is designed to track the performance of the Russell 2000 Index. An Authorized Participant will purchase all the Russell 2000 constituent securities in the exact same weight as the index prescribes, then deliver those shares to the ETF issuer. In exchange, the ETF issuer gives the Authorized Participant a block of equally valued ETF shares, on a one-for-one fair value basis. This process can also work in reverse. A redemption is achieved when the Authorized Participant accumulates a sufficient number of shares of the ETF to constitute a creation unit and then exchanges these ETF shares with the ETF issuer, thereby decreasing the supply of ETF shares in the market.

The principal, and perhaps most important, feature of ETFs is their reliance on an “arbitrage function” performed by market participants that influences the supply and demand of ETF shares and, thus, trading prices relative to NAV. As noted above, new

²³ See Securities Exchange Act Release No. 88131 (February 5, 2020), 85 FR 7806 (February 11, 2020) (SR-NYSEAmex-2019-38) (Notice of Filing of Amendment No. 1 and Order Granting Accelerated Approval of a Proposed Rule Change, as Modified by Amendment No. 1, To Allow Certain Flexible Equity Options To Be Cash Settled).

²⁴ Cboe also filed an immediately effective rule change to allow certain FLEX Options to be cash settled. See Securities Exchange Act Release No. 98044 (August 2, 2023), 88 FR 53548 (August 8, 2023) (SR-Cboe-2023-036) (Notice of Filing and Immediate Effectiveness of a Proposed Rule Change To Allow Certain Flexible Exchange Equity Options To Be Cash Settled).

²⁵ As noted below, the Exchange plans to conduct the bi-annual review on January 1 and July 1 of each year. As such, the six-month periods will be from January to June, and from July to December each year.

²⁶ See Cboe Rule 4.21(b)(5)(A)(ii) for materially identical provisions.

²⁷ See introductory paragraph of Cboe Rule 4.21(b) for materially identical provisions. All non-FLEX Equity Options (including on ETFs) are physically settled. Note all FLEX and non-FLEX Equity Options (including ETFs) are p.m.-settled.

²⁸ See proposed Options 8, Section 34(f)(6)(A)(2)(b), which is based on Cboe Rule 4.21(b)(5)(A)(ii)(a). The Exchange plans to conduct the bi-annual review on January 1 and July 1 of each year. As such, the six-month periods will be from January to June, and from July to December each year. The results of the bi-annual review will be announced via an Options Trader Alert and any new securities that qualify would be permitted to have cash settlement as a contract term beginning on February 1 and August 1 of each year. If the Exchange initially begins listing cash-settled FLEX Equity Options on a different date (*e.g.*, September 1), it would initially list securities that qualified as of the last bi-annual review (*e.g.*, the one conducted on July 1).

²⁹ See proposed Options 8, Section 34(f)(6)(A)(2)(a), which is based on Cboe Rule 4.21(b)(5)(A)(ii)(a).

³⁰ See proposed Options 8, Section 34(f)(6)(A)(2)(b), which is based on Cboe Rule 4.21(b)(5)(A)(ii)(b). If a listing is closing only, pursuant to Options 4, Section 4(a), opening transactions by Market Makers executed to accommodate closing transactions of other market participants are permitted.

³¹ “Authorized Participant” means a member or participant of a clearing agency registered with the Commission, which has a written agreement with the exchange-traded fund or one of its service providers that allows the authorized participant to place orders for the purchase and redemption of creation units. See SEC Rule 6c-11(a)(1).

ETF shares can be created and existing shares redeemed based on investor demand; thus, ETF supply is open-ended. This arbitrage function helps to keep an ETF's price in line with the value of its underlying portfolio, *i.e.*, it minimizes deviation from NAV. Generally, in the Exchange's view, the higher the liquidity and trading volume of an ETF, the more likely the price of the ETF will not deviate from the value of its underlying portfolio, making such ETFs less susceptible to price manipulation.

Trading Data for the ETFs Proposed for Cash Settlement

The Exchange believes that average daily notional value is an appropriate proxy for selecting underlying securities that are not readily susceptible to manipulation for purposes of establishing a settlement price. Average daily notional value considers both the trading activity and the price of an underlying security. As a general matter, the more expensive an underlying security's price, the less cost-effective

manipulation could become. Further, manipulation of the price of a security encounters greater difficulty the more volume that is traded. To calculate average daily notional value (provided in the table below), the Exchange summed the notional value of each trade for each symbol (*i.e.*, the number of shares times the price for each execution in the security) and divided that total by the number of trading days in the six-month period (from January 1, 2024 through June 30, 2024) reviewed by the Exchange.

Further, the Exchange proposes that qualifying ETFs also meet an ADV standard. The purpose for this second criteria is to prevent unusually expensive underlying securities from qualifying under the average daily notional value standard while not being one of the most actively traded securities. The Exchange believes an ADV requirement of 4,680,000 shares a day is appropriate because it represents average trading in the underlying ETF of 200 shares per second. While no security is immune from all

manipulation, the Exchange believes that the combination of average daily notional value and ADV as prerequisite requirements would limit cash settlement of FLEX ETF Options to those underlying ETFs that would be less susceptible to manipulation in order to establish a settlement price.

The Exchange believes that the proposed objective criteria would ensure that only the most robustly traded and deeply liquid ETFs would qualify to have cash settlement as a contract term. As provided in the below table, from January 1, 2024 to June 30, 2024, the Exchange would be able to provide cash settlement as a contract term for FLEX ETF Options on 48 underlying ETFs, as only this group of securities would currently meet the requirement of \$500 million or more average daily notional value and a minimum ADV of 4,680,000 shares. The table below provides the list of the 48 ETFs that, for the period covering January 1, 2024 through June 30, 2024, would be eligible to have cash settlement as a contract term.³²

Symbol	Security name	Average daily notional value (in dollars) (1/1/24–6/30/24)	Average daily volume (in shares) (1/1/24–6/30/24)
AGG	iShares Core U.S. Aggregate Bond ETF	\$806,096,032	8,295,918
ARKK	ARK Innovation ETF	588,267,283	12,516,087
BIL	SPDR Bloomberg 1–3 Month T-Bill ETF	618,700,170	6,753,925
BND	Vanguard Total Bond Market Index Fund ETF	514,223,054	7,130,093
EEM	iShares MSCI Emerging Markets ETF	1,164,586,979	28,535,696
EFA	iShares MSCI EAFE ETF	1,104,421,854	14,216,699
EMB	iShares JPMorgan USD Emerging Markets Bond ETF	542,748,575	6,149,042
EWJ	iShares MSCI Japan ETF	509,554,399	7,481,823
EWZ	iShares MSCI Brazil ETF	683,919,536	21,690,846
FXI	iShares China Large-Cap ETF	1,027,752,868	42,009,611
GBTC	Grayscale Bitcoin Trust*	683,447,931	13,105,251
GDV	VanEck Gold Miners ETF	774,584,258	24,682,952
GLD	SPDR Gold Shares	1,511,241,142	7,344,884
HYG	iShares iBoxx \$ High Yield Corporate Bond ETF	2,850,542,598	37,011,783
IBIT	iShares Bitcoin Trust ETF*	1,338,731,551	35,140,151
IEF	iShares 7–10 Year Treasury Bond ETF	743,974,086	7,917,457
IEFA	iShares Core MSCI EAFE ETF	577,266,076	7,997,376
IEMG	iShares Core MSCI Emerging Markets ETF	519,063,454	10,129,994
IVV	iShares Core S&P 500 ETF	2,774,452,994	5,417,239
IWM	iShares Russell 2000 ETF	6,731,230,018	33,649,687
IYR	iShares U.S. Real Estate ETF	537,339,035	6,177,644
KRE	SPDR S&P Regional Banking ETF	676,589,675	13,902,921
KWEB	KraneShares CSI China Internet ETF	555,987,739	20,766,407
LQD	Shares iBoxx \$ Investment Grade Corporate Bond ETF	3,007,311,016	27,902,549
NVDL	GraniteShares 2x Long NVDA Daily ETF	682,096,758	11,387,201
QQQ	Invesco QQQ Trust	17,916,413,637	41,065,771
RSP	Invesco S&P 500 Equal Weight ETF	982,482,303	6,062,567
SLV	iShares Silver Trust	602,178,901	24,515,577
SMH	VanEck Semiconductor ETF	1,783,514,710	8,199,564
SOXL	Direxion Daily Semiconductor Bull 3x Shares	2,703,451,838	64,700,251
SOXS	Direxion Daily Semiconductor Bear 3x Shares	695,294,352	92,188,004
SPXL	Direxion Daily S&P 500 Bull 3X Shares	737,685,244	6,096,062
SPY	SPDR S&P 500 ETF Trust	33,559,628,313	66,151,690
SQQQ	ProShares UltraPro Short QQQ ETF	1,461,906,416	131,905,524
TLT	iShares 20+ Year Treasury Bond ETF	3,779,166,025	40,682,936
TNA	Direxion Daily Small Cap Bull 3X Shares	697,479,128	18,832,200

³² As noted below, options on GBTC and IBIT are not yet available.

Symbol	Security name	Average daily notional value (in dollars) (1/1/24–6/30/24)	Average daily volume (in shares) (1/1/24–6/30/24)
TQQQ	ProShares UltraPro QQQ	3,796,209,774	64,941,840
VCIT	Vanguard Intermediate-Term Corp Bond Idx Fund ETF	597,752,071	7,484,828
VEA	Vanguard Tax Managed Fund FTSE Developed Markets ETF	517,396,977	10,583,858
VOO	Vanguard S&P 500 ETF	2,425,398,743	5,177,005
XBI	SPDR S&P Biotech ETF	979,943,806	10,728,380
XLE	Energy Select Sector SPDR Fund	1,411,567,713	15,798,449
XLF	Financial Select Sector SPDR Fund	1,736,012,363	43,157,138
XLI	Industrial Select Sector SPDR Fund	1,114,661,946	9,277,779
XLK	Technology Select Sector SPDR Fund	1,274,025,061	6,202,031
XLP	Consumer Staples Select Sector SPDR Fund	907,491,273	12,108,426
XLU	Utilities Select Sector SPDR Fund	944,774,031	14,540,920
XLV	Health Care Select Sector SPDR Fund	1,127,277,467	7,876,680

* Options on this ETF are not yet available.

The Exchange believes that permitting cash settlement as a contract term for FLEX ETF Options for the ETFs in the above table would broaden the base of investors that use FLEX Equity Options to manage their trading and investment risk, including investors that currently trade in the OTC market for customized options, where settlement restrictions do not apply.

The Exchange notes that the SEC has previously approved a rule filing of another exchange that allowed for the trading of cash-settled options³³ and, specifically, cash-settled FLEX ETF Options (which the Exchange proposes to list in the same manner as that exchange).³⁴

³³ See, e.g., PHLX FX Options traded on Nasdaq PHLX and S&P 500® Index Options traded on Cboe Options Exchange. The Commission approved, on a pilot basis, the listing and trading of RealDay™ Options on the SPDR S&P 500 Trust on the BOX Options Exchange LLC (“BOX”). See Securities Exchange Act Release No. 79936 (February 2, 2017), 82 FR 9886 (February 8, 2017) (“RealDay Pilot Program”). The RealDay Pilot Program was extended until February 2, 2019. See Securities Exchange Act Release No. 82414 (December 28, 2017), 83 FR 577 (January 4, 2018) (SR–BOX–2017–38). The RealDay Pilot Program was never implemented by BOX. See also Securities Exchange Act Release Nos. 56251 (August 14, 2007), 72 FR 46523 (August 20, 2007) (SR–Amex–2004–27) (Order approving listing of cash-settled Fixed Return Options (“FROs”)); and 71957 (April 16, 2014), 79 FR 22563 (April 22, 2014) (SR–NYSEMKT–2014–06) (Order approving name change from FROs to ByRDs and re-launch of these products, with certain modifications).

³⁴ See Securities Exchange Act Release Nos. 88131 (February 5, 2020), 85 FR 7806 (February 11, 2020) (SR–NYSEAMER–2019–38) (Order Approving a Proposed Rule Change, as Modified by Amendment No. 1, to Allow Certain Flexible Equity Options To Be Cash Settled); 97231 (March 31, 2023), 88 FR 20587 (April 6, 2023) (SR–NYSEAMER–2023–22) (Notice of Filing and Immediate Effectiveness of Proposed Change to Make a Clarifying Change to the Term Settlement Style Applicable to Flexible Exchange Options); and 98044 (August 2, 2023), 88 FR 53548 (August 8, 2023) (SR–Cboe–2023–036) (Notice of Filing and Immediate Effectiveness of a Proposed Rule Change To Allow Certain Flexible Exchange Equity Options To Be Cash Settled).

Today, equity options are settled physically at The Options Clearing Corporation (“OCC”), i.e., upon exercise, shares of the underlying security must be assumed or delivered. Physical settlement may possess certain risks with respect to volatility and movement of the underlying security at expiration against which market participants may need to hedge. The Exchange believes cash settlement may be preferable to physical delivery in some circumstances as it does not present the same risk. If an issue with the delivery of the underlying security arises, it may become more expensive (and time consuming) to reverse the delivery because the price of the underlying security would almost certainly have changed. Reversing a cash payment, on the other hand, would not involve any such issue because reversing a cash delivery would simply involve the exchange of cash. Additionally, with physical settlement, market participants that have a need to generate cash would have to sell the underlying security while incurring the costs associated with liquidating their position as well as the risk of an adverse movement in the price of the underlying security.

With respect to position and exercise limits, cash-settled FLEX ETF Options would be subject to the position limits set forth in proposed Options 8, Section 34(i). Accordingly, the Exchange proposes to add Options 8, Section 34(i)(1), which would provide that a position in FLEX Equity Options where the underlying security is an ETF that is settled in cash pursuant to Options 8, Section 34(f)(6)(A) shall be subject to the position limits set forth in Options 9, Section 13, and subject to the exercise limits set forth in Options 9, Section 15.³⁵ The proposed rule would further

³⁵ The Exchange proposes to add to proposed Options 8, Section 34(i)(1) a cross reference to

state that positions in such cash-settled FLEX Equity Options shall be aggregated with positions in physically settled options on the same underlying ETF for the purpose of calculating the position limits set forth in Options 9, Section 13 and the exercise limits set forth in Options 9, Section 15.³⁶ The Exchange further proposes to add in Options 8, Section 34(i)(1) a cross-reference to subparagraph (f)(6)(A), as subparagraph (i)(1) would also contain provisions about position limits for FLEX Equity Options that would be exceptions to the first sentence in this paragraph stating that FLEX Equity Options have no position limits. The Exchange also proposes to add in paragraph (i)(4), a cross-reference to proposed subparagraphs (i)(1) as the proposed rule adds language regarding aggregation of positions for purposes of position limits, which will be covered by paragraph (i)(4). Given that each of the underlying ETFs that would currently be eligible to have cash-settlement as a contract term have established position and exercise limits applicable to physically settled options, the Exchange believes it is appropriate for the same position and exercise limits to also apply to cash-settled options. Accordingly, of the 48 underlying securities that would currently be

proposed subparagraph (f)(6)(A), as proposed Section 34(i)(1) also contains provisions about position limits for FLEX Equity Options that would be exceptions to the statement in proposed Section (i)(1) that FLEX Equity Options have no position limits (in addition to the language in proposed 34(i)(1)). The Exchange also proposes to add to proposed Options 8, Section 34(i)(4) a cross-reference to proposed subparagraph (i)(1), as the proposed rule adds language regarding aggregation of positions for purposes of position limits, which will be covered in proposed Section 34(i)(4).

³⁶ See proposed Options 8, Section 34(i)(1), which is based on Cboe Rule 8.35(c)(1)(B). The aggregation of position and exercise limits would include all positions on physically settled FLEX and non-FLEX Options on the same underlying ETFs.

eligible to have cash settlement as a FLEX contract term, 33 would have a position limit of 250,000 contracts pursuant to Options 9, Section 13(d)(5).³⁷ Further, pursuant to Supplementary Material .01 to Options 9, Section 13, seven would have a position limit of 500,000 contracts (EWJ, EWZ, TLT, HYG, XLF, LQD, and GDX); four (EEM, FXI, IWM, and EFA) would have a position limit of 1,000,000 contracts; one (QQQ) would have a position limit of 1,800,000 contracts; and one (SPY) would have a position limit of 3,600,000.³⁸

The Exchange understands that cash-settled ETF options are currently traded in the OTC market by a variety of market participants, *e.g.*, hedge funds, proprietary trading firms, and pension funds.³⁹ These options are not fungible with the exchange listed options. The Exchange believes some of these market participants would prefer to trade comparable instruments on an exchange, where they would be cleared and settled through a regulated clearing agency. The Exchange expects that users of these OTC products would be among the primary users of exchange-traded cash-settled FLEX ETF Options. The Exchange also believes that the trading of cash-settled FLEX ETF Options would allow these same market participants to better manage the risk associated with the volatility of underlying equity positions given the enhanced liquidity that an exchange-traded product would bring.

In the Exchange's view, cash-settled FLEX ETF Options traded on the

Exchange would have three important advantages over the contracts that are traded in the OTC market. First, as a result of greater standardization of contract terms, exchange-traded contracts should develop more liquidity. Second, counter-party credit risk would be mitigated by the fact that the contracts are issued and guaranteed by OCC. Finally, the price discovery and dissemination provided by the Exchange and its members would lead to more transparent markets. The Exchange believes that its ability to offer cash-settled FLEX ETF Options would aid it in competing with the OTC market and at the same time expand the universe of products available to interested market participants. The Exchange believes that an exchange-traded alternative may provide a useful risk management and trading vehicle for market participants and their customers. Further, the Exchange believes listing cash-settled FLEX ETF Options would provide investors with competition on an exchange platform, as other options exchanges have received Commission approval to list the same options.⁴⁰

The Exchange notes that OCC has received approval from the Commission for rule changes that will accommodate the clearance and settlement of cash-settled ETF options.⁴¹ The Exchange has also analyzed its capacity and represents that it and The Options Price Reporting Authority ("OPRA") have the necessary systems capacity to handle the additional traffic associated with the listing of cash-settled FLEX ETF Options. The Exchange believes any additional traffic that would be generated from the introduction of cash-settled FLEX ETF Options would be manageable. The Exchange expects that members will not have a capacity issue as a result of this proposed rule change. The Exchange also does not believe this proposed rule change will cause fragmentation of liquidity. The Exchange will monitor the trading volume associated with the additional options series listed as a result of this proposed rule change and the effect (if any) of these additional series on market fragmentation and on the capacity of the Exchange's automated systems.

The Exchange does not believe that allowing cash settlement as a contract term would render the marketplace for equity options more susceptible to manipulative practices. The Exchange believes that manipulating the settlement price of cash-settled FLEX

ETF Options would be difficult based on the size of the market for the underlying ETFs that are the subject of this proposed rule change. The Exchange notes that each underlying ETF in the table above is sufficiently active to alleviate concerns about potential manipulative activity. Further, in the Exchange's view, the vast liquidity in the 48 underlying ETFs that would currently be eligible to be traded as cash-settled FLEX options under the proposal ensures a multitude of market participants at any given time. Moreover, given the high level of participation among market participants that enter quotes and/or orders in physically settled options on these ETFs, the Exchange believes it would be very difficult for a single participant to alter the price of the underlying ETF or options overlying such ETF in any significant way without exposing the would-be manipulator to regulatory scrutiny. The Exchange further believes any attempt to manipulate the price of the underlying ETF or options overlying such ETF would also be cost prohibitive. As a result, the Exchange believes there is significant participation among market participants to prevent manipulation of cash-settled FLEX ETF Options.

Still, the Exchange believes it has an adequate surveillance program in place and intends to apply the same program procedures to cash-settled FLEX ETF Options that it applies to the Exchange's other options products.⁴² FLEX options products and their respective symbols will be integrated into the Exchange's existing surveillance system architecture and will thus be subject to the relevant surveillance processes, as applicable. The Exchange believes that the existing surveillance procedures at the Exchange are capable of properly identifying unusual and/or illegal trading activity, which procedures the Exchange would utilize to surveil for aberrant trading in cash-settled FLEX ETF Options.

With respect to regulatory scrutiny, the Exchange believes its existing surveillance technologies and procedures adequately address potential concerns regarding possible manipulation of the settlement value at or near the close of the market. The Exchange notes that the regulatory program operated by and overseen by

³⁷ Options 9, Section 13(d)(5) provides that to be eligible for the 250,000 contract limit, either the most recent six (6) month trading volume of the underlying security must have totalled at least 100 million shares or the most recent six-month trading volume of the underlying security must have totalled at least seventy-five (75) million shares and the underlying security must have at least 300 million shares currently outstanding. Further as noted above, options on GBTC and IBIT are not yet available.

³⁸ These were based on position limits as of September 13, 2024. Position limits are available on at <https://www.theocc.com>. Position limits for ETFs are always determined in accordance with the Exchange's Rules regarding position limits.

³⁹ As noted above, other options exchanges have received approval to list certain cash-settled FLEX ETF Options. See Securities Exchange Act Release No. 88131 (February 5, 2020), 85 FR 7806 (February 11, 2020) (SR-NYSEAmex-2019-38) (Notice of Filing of Amendment No. 1 and Order Granting Accelerated Approval of a Proposed Rule Change, as Modified by Amendment No. 1, To Allow Certain Flexible Equity Options To Be Cash Settled). Cboe also filed an immediately effective rule change to allow certain FLEX Options to be cash settled. See Securities Exchange Act Release No. 98044 (August 2, 2023), 88 FR 53548 (August 8, 2023) (SR-Cboe-2023-036) (Notice of Filing and Immediate Effectiveness of a Proposed Rule Change To Allow Certain Flexible Exchange Equity Options To Be Cash Settled).

⁴⁰ See *supra* note 39.

⁴¹ See Securities Exchange Act Release No. 34-94910 (May 13, 2022), 87 FR 30531 (May 19, 2022) (SR-OCC-2022-003).

⁴² For example, the regulatory program for the Exchange includes surveillance designed to identify manipulative and other improper options trading, including, spoofing, marking the close, front running, wash sales, etc.

Phlx⁴³ includes cross-market surveillance designed to identify manipulative and other improper trading, including spoofing, algorithm gaming, marking the close and open, as well as more general, abusive behavior related to front running, wash sales, and quoting/routing, which may occur on the Exchange or other markets.⁴⁴ These cross-market patterns incorporate relevant data from various markets beyond the Exchange and its affiliates and from markets not affiliated with the Exchange. The Exchange represents that, today, its existing trading surveillances are adequate to monitor trading in the underlying ETFs and subsequent trading of options on those securities listed on the Exchange. Further, with the introduction of cash-settled FLEX ETF Options, the Exchange would leverage its existing surveillances to monitor trading in the underlying ETFs and subsequent trading of options on those securities listed on the Exchange with respect to cash-settled FLEX ETF options.⁴⁵

Additionally, for options, the Exchange utilizes an array of patterns that monitor manipulation of options, or manipulation of equity securities (regardless of venue) for the purpose of impacting options prices on the Exchange (*i.e.*, mini-manipulation strategies). That surveillance coverage is initiated once options begin trading on the Exchange. Accordingly, the Exchange believes that the cross-market surveillance performed by the Exchange or FINRA, on behalf of the Exchange, coupled with Phlx's own monitoring for violative activity on the Exchange comprise a comprehensive surveillance program that is adequate to monitor for manipulation of the underlying ETF and overlying option. Furthermore, the Exchange believes that the existing

surveillance procedures at the Exchange are capable of properly identifying unusual and/or illegal trading activity, which the Exchange would utilize to surveil for aberrant trading in cash-settled FLEX ETF Options.

In addition to the surveillance procedures and processes described above, improvements in audit trails (*i.e.*, the Consolidated Audit Trail), recordkeeping practices, and inter-exchange cooperation over the last two decades have greatly increased the Exchange's ability to detect and punish attempted manipulative activities. In addition, the Exchange is a member of the Intermarket Surveillance Group ("ISG"). The ISG members work together to coordinate surveillance and investigative information sharing in the stock and options markets. For surveillance purposes, the Exchange would therefore have access to information regarding trading activity in the pertinent underlying securities.

The proposed rule change is designed to allow investors seeking to effect cash-settled FLEX ETF Options with the opportunity for a different method of settling option contracts at expiration if they choose to do so. As noted above, market participants may choose cash settlement because physical settlement possesses certain risks with respect to volatility and movement of the underlying security at expiration that market participants may need to hedge against. The Exchange believes that offering innovative products flows to the benefit of the investing public. A robust and competitive market requires that exchanges respond to members' evolving needs by constantly improving their offerings. Such efforts would be stymied if exchanges were prohibited from offering innovative products for reasons that are generally debated in academic literature. The Exchange believes that introducing cash-settled FLEX ETF Options would further broaden the base of investors that use FLEX Equity Options to manage their trading and investment risk, including investors that currently trade in the OTC market for customized options, where settlement restrictions do not apply. The proposed rule change is also designed to encourage market makers to shift liquidity from the OTC market onto the Exchange, which, it believes, would enhance the process of price discovery conducted on the Exchange through increased order flow. The Exchange also believes that this may open up cash-settled FLEX ETF Options to more retail investors. The Exchange does not believe that this proposed rule change raises any unique regulatory concerns because existing safeguards—such as

position limits (and the aggregation of cash-settled positions with physically-settled positions), exercise limits (and the aggregation of cash-settled positions with physically-settled positions), and reporting requirements—would continue to apply. The Exchange believes the proposed position and exercise limits may further help mitigate the concerns that the limits are designed to address about the potential for manipulation and market disruption in the options and the underlying securities.⁴⁶

Given the novel characteristics of cash-settled FLEX ETF Options, the Exchange will conduct a review of the trading in cash-settled FLEX ETF Options over an initial five-year period. The Exchange will furnish five reports to the Commission based on this review, the first of which would be provided within 60 days after the first anniversary of the initial listing date of the first cash-settled FLEX ETF Option under the proposed rule and each subsequent annual report to be provided within 60 days after the second, third, fourth and fifth anniversary of such initial listing. At a minimum, each report will provide a comparison between the trading volume of all cash-settled FLEX ETF Options listed under the proposed rule and physically settled options on the same underlying security, the liquidity of the market for such options products and the underlying ETF, and any manipulation concerns arising in connection with the trading of cash-settled FLEX ETF Options under the proposed rule. The Exchange will also provide additional data as requested by the Commission during this five year period. The reports will also discuss any recommendations the Exchange may have for enhancements to the listing standards based on its review. The Exchange believes these reports will allow the Commission and the Exchange to evaluate, among other things, the impact such options have, and any potential adverse effects, on price volatility and the market for the underlying ETFs, the component securities underlying the ETFs, and the options on the same underlying ETFs and make appropriate recommendations, if any, in response to the reports.

Implementation

The Exchange proposes to implement this rule change on or before December 23, 2024. The Exchange will announce

⁴⁶ See proposed Options 8, Section 34(i)(1), which is based on Cboe Rule 8.35(c)(1)(B). The aggregation of position and exercise limits would include all positions on physically settled FLEX and non-FLEX Options on the same underlying ETFs.

⁴³ Phlx maintains a regulatory services agreement with Financial Industry Regulatory Authority, Inc. ("FINRA") whereby FINRA provides certain regulatory services to the exchanges, including cross-market surveillance, investigation, and enforcement services.

⁴⁴ As it relates to Reg SHO violations, the Exchange will enforce this through its Stock-Tied Reg SHO price protections in Options 3, Section 16(b). See *supra* note 65 for Stock-Tied Reg SHO discussion. NES will only execute the underlying covered security component of a Complex Order if the underlying covered security component is in accordance with Rule 201 of Regulation SHO. Additionally, FINRA's regulatory program addresses Reg SHO compliance for its member firms (which includes Exchange Members).

⁴⁵ Such surveillance procedures generally focus on detecting securities trading subject to opening price manipulation, closing price manipulation, layering, spoofing or other unlawful activity impacting an underlying security, the option, or both. The Exchange has price movement alerts, unusual market activity and order book alerts active for all trading symbols.

an implementation date by issuing an Options Trader Alert.

2. Statutory Basis

The Exchange believes that its proposal is consistent with Section 6(b) of the Act,⁴⁷ in general, and furthers the objectives of Section 6(b)(5) of the Act.⁴⁸ Specifically, the Exchange believes the proposed rule change is consistent with the Section 6(b)(5)⁴⁹ requirements that the rules of an exchange be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.

Permissible Series

The Exchange's proposal to not authorize for trading a FLEX Option on iShares Bitcoin Trust ETF ("IBIT") is consistent with ISE's Approval Order of iShares Bitcoin Trust.⁵⁰ ISE stated that the position limit for IBIT options shall be 25,000 contracts.⁵¹ Phlx proposes to exclude IBIT Options from trading as a FLEX Options to continue to limit the position limits for IBIT Options.

Characteristics of ETFs

The Exchange's proposal to provide in Options 8, Section 34(f)(1)(B) that, "an underlying equity security or index, as applicable (the index multiplier for FLEX Index Options is 100)" is consistent with the Act and will protect investors and the general public because this rule text adds transparency to the current characteristics of underlying interest for FLEX Option.

Minimum Trading Increments

The Exchange's proposal to amend Options 8, Section 34(f)(3) to provide that, "The Exchange may determine the smallest increment for exercise prices of FLEX Options on a class-by-class basis without going lower than the \$0.01." is consistent with the Act and will protect investors and the general public because

this rule text provides clear, transparent language regarding the minimum trading increments for FLEX Options. The language is consistent with Cboe Rule 5.3(e)(3) except the Exchange is not proposing to provide for Micro FLEX Index Options or to allow prices to be expressed as a percentage value because the Exchange does not offer these features today.

FLEX PM Third Friday Options

The Exchange's proposal to amend Options 8, Section 34(f)(5) to allow the listing of FLEX PM Third Friday Options, is consistent with the Commission's recent approval of Cboe's proposal to make its pilot a permanent program.⁵² The Exchange believes that aligning to Cboe will allow Phlx to compete effectively with Cboe's product offering. Like Cboe, the Exchange believes that FLEX PM Third Friday Options will provide investors with greater trading opportunities and flexibility. The Exchange notes that the Commission recently approved proposals to make other pilots permitting p.m.-settlement of index options permanent after finding those pilots were consistent with the Act and the options subject to those pilots had no significant impact on the market.⁵³

The Exchange further believes that permitting Phlx to list FLEX PM Third Friday Options, similar to Cboe, will remove impediments to and perfect the mechanism of a free and open market and a national market system and

protect investors, while maintaining a fair and orderly market. As described in the FLEX Settlement Pilot Approval, Cboe observed no significant adverse market impact or identified any meaningful regulatory concerns during the nearly 14-year operation of the FLEX PM Third Friday Program as a pilot nor during the 15 years since P.M.-settled index options (SPX) were reintroduced to the marketplace.⁵⁴

As discussed in the FLEX Settlement Pilot Approval, the DERA staff study and corresponding Cboe study concluded that a significantly larger amount of non-FLEX p.m.-settled index options had no significant adverse market impact and caused no meaningful regulatory concerns. Therefore, the Exchange believes it is reasonable to conclude that the relatively small amount of FLEX Index Option volume would similarly have no significant adverse market impact or cause no meaningful regulatory concerns.⁵⁵

The Exchange also believes the introduction of FLEX PM options had

⁵⁴ Notably, Cboe did not identify any significant economic impact (including on pricing or volatility or in connection with reversals) on related futures, the underlying indexes, or the underlying component securities of the underlying indexes surrounding the close as a result of the quantity of FLEX PM Third Friday Options or the amount of expiring open interest in FLEX PM Third Friday Options, nor any demonstrated capacity for options hedging activity to impact volatility in the underlying markets. See Securities Exchange Act Release No. 99222 (December 21, 2023), 88 FR 89771 (December 28, 2023) (SR-CBOE-2023-018) ("FLEX Settlement Pilot Approval"). In support of making the pilot a permanent program, Cboe cited to its own review of pilot data during the course of the pilot program and a study by the Commission's Division of Economic and Risk Analysis ("DERA") staff. See FLEX Settlement Pilot Approval, notes 18 and 35.

⁵⁵ See Securities Exchange Act Release No. 99222 (December 21, 2023), 88 FR 89771 (December 28, 2023) (SR-CBOE-2023-018) ("FLEX Settlement Pilot Approval"). In support of making the pilot a permanent program, Cboe cited to its own review of pilot data during the course of the pilot program and a study by the Commission's Division of Economic and Risk Analysis ("DERA") staff. See FLEX Settlement Pilot Approval, notes 18 and 35. Additionally, these studies measured any impact on related futures, the underlying indexes, or the underlying component securities of the underlying indexes surrounding the close. Despite FLEX SPX options (which represent approximately half of the year-to-date 2023 volume of FLEX Index Options but only approximately 0.3% of total SPX volume) not being included in the DERA staff study and corresponding Cboe study, those studies concluded that during the time periods covered (which included the period of time in which the Pilot Program has been operating), there was no significant economic impact on the underlying index or related products. Therefore, the Exchange believes it is reasonable to conclude that any FLEX SPX Options that executed during the timeframes covered by the studies had no significant impact on the underlying index or related products, as neither DERA staff nor Cboe observed any significant economic impact on the underlying index or related product.

⁴⁷ 15 U.S.C. 78f(b).

⁴⁸ 15 U.S.C. 78f(b)(5).

⁴⁹ 15 U.S.C. 78f(b)(5).

⁵⁰ See Securities Exchange Act Release No. 101128 (September 20, 2024), 89 FR 78942 (September 26, 2024) (SR-ISE-2024-03) (Notice of Filing of Amendment Nos. 4 and 5 and Order Granting Accelerated Approval of a Proposed Rule Change, as Modified by Amendment Nos. 1, 4, and 5, To Permit the Listing and Trading of Options on the iShares Bitcoin Trust).

⁵¹ *Id.*

⁵² See Securities Exchange Act Release No. 99222 (December 21, 2023), 88 FR 89771 (December 28, 2023) (SR-CBOE-2023-018) ("FLEX Settlement Pilot Approval"). In support of making the pilot a permanent program, Cboe cited to its own review of pilot data during the course of the pilot program and a study by the Commission's Division of Economic and Risk Analysis ("DERA") staff. See FLEX Settlement Pilot Approval, notes 18 and 35.

⁵³ See Securities Exchange Act Release Nos. 98454 (September 20, 2023) (SR-CBOE-2023-005) (order approving proposed rule change to make permanent the operation of a program that allows the Exchange to list p.m.-settled third Friday-of-the-month SPX options series) ("SPXPM Approval"); 98455 (September 20, 2023) (SR-CBOE-2023-019) (order approving proposed rule change to make permanent the operation of a program that allows the Exchange to list p.m.-settled third Friday-of-the-month XSP and MRUT options series) ("XSP and MRUT Approval"); and 98456 (September 20, 2023) (SR-CBOE-2023-020) (order approving proposed rule change to make the nonstandard expirations pilot program permanent) ("Nonstandard Approval"). See also Securities Exchange Act Release Nos. 98451 (September 20, 2023), 88 FR 66088 (September 26, 2023) (SR-Phlx-2023-07) (Order Granting Approval of a Proposed Rule Change, as Modified by Amendment No. 1, To Make Permanent Certain P.M.-Settled Pilots); and 98950 (November 15, 2023), 88 FR 81172 (November 21, 2023) (SR-Phlx-2023-45) (Order Approving a Proposed Rule Change To Permit the Listing and Trading of P.M.-Settled Nasdaq-100 Index Options With a Third-Friday-of-the-Month Expiration).

no significant impact on the market quality of corresponding a.m.-settled options or other options. As discussed in the FLEX Settlement Pilot Approval, Cboe's analysis conducted after the introduction of SPXW options with Tuesday and Thursday expirations demonstrated no statistically significant impact on the bid-ask or effective spreads of SPXW options with Monday, Wednesday, and Friday expirations after trading in the SPXW options with Tuesday and Thursday expirations began.⁵⁶ Further, Cboe concluded that large FLEX PM Third Friday Options trades had no material negative impact (and likely no impact) on quote quality of non-FLEX a.m.-settled options overlying the same index with similar terms as the FLEX PM Third Friday Option upon evaluating data that showed that the spreads were relatively stable before and after large trades.⁵⁷ Therefore, the Exchange believes Cboe's evaluation effectively demonstrates it is likely that FLEX PM Third Friday Options have had no significant negative impact on the market quality of non-FLEX Options with a.m.-settlement.⁵⁸

Additionally, the significant changes in the closing procedures of the primary markets in recent decades, including considerable advances in trading systems and technology, has significantly minimized risks of any potential impact of FLEX PM Third Friday Options on the underlying cash markets. As such, the Exchange believes

that this proposal does not raise any unique or prohibitive regulatory concerns and that such trading has not, and will not, adversely impact fair and orderly markets on expiration Fridays for the underlying indexes or their component securities.

FLEX Options Terms

The Exchange's proposal to amend Options 8, Section 34(f)(6)(A) to note how the exercise value is determined depending on whether it is a.m.-settled or p.m.-settled is consistent with the Act and will protect investors and the general public because this rule text adds transparency to the current settlement of FLEX Index Options.

Position and Exercise Limits

Position and exercise limits are designed to address potential manipulative schemes and adverse market impacts surrounding the use of options, such as disrupting the market in the security underlying the options. While position and exercise limits should address and discourage the potential for manipulative schemes and adverse market impact, if such limits are set too low, participation in the options market may be discouraged. The Exchange believes that any decision regarding imposing position and exercise limits for FLEX Options must therefore be balanced between mitigating concerns of any potential manipulation and the cost of inhibiting potential hedging activity that could be used for legitimate economic purposes.

As it relates to FLEX Index Options, the Exchange believes that the proposed amendments to position and exercise limits in Options 8, Section 34(i) and (j) are reasonably designed to prevent a member organization from using FLEX Index Options to evade the position limits applicable to comparable non-FLEX Index Options. Further, by establishing the proposed position and exercise limits for FLEX Index Options and, importantly, aggregating such positions in the manner described in proposed Options 8, Section 34(i)(4) the Exchange believes that the position and exercise limit requirements for FLEX Index Options should help to ensure that the trading of FLEX Index Options would not increase the potential for manipulation or market disruption and could help to minimize such incentives. The Exchange also notes that proposed position and exercise limits are consistent with the rules of other options exchanges that offer FLEX Index Options, as well as the rules of its own standard non-FLEX index options

market, and therefore raise no novel issues for the Commission.⁵⁹

As it relates to FLEX Equity Options, while no position limits are proposed for FLEX Equity Options, there are several mitigating factors, which include aggregation of FLEX Equity Option and non-FLEX Equity Option positions that expire on a third Friday-of-the-month and subjecting those positions to position and exercise limits, and daily monitoring of market activity. Similar to the other exchanges that trade FLEX Equity Options, the Exchange believes that eliminating position and exercise limits for FLEX Equity Options, while requiring positions in FLEX Equity Options that expire on a third Friday-of-the-month to be aggregated with positions in non-FLEX Equity Options on the same underlying security,⁶⁰ removes impediments to and perfects the mechanism of a free and open market and a national market system because it allows the Exchange to create a product and market that is an improved but comparable alternative to the OTC market in customized options. OTC transactions occur through bilateral agreements, the terms of which are not publicly disclosed to the marketplace. As such, OTC transactions do not contribute to the price discovery process that exists on a public exchange.

The Exchange believes that the proposed elimination of position and exercise limits for FLEX Equity Options may encourage market participants to transfer their liquidity demands from OTC markets to exchanges and enable liquidity providers to provide additional liquidity to Phlx through transactions in FLEX Equity Options. The Exchange notes that the Commission previously approved the elimination of position and exercise limits for FLEX Equity Options, finding that such elimination would allow exchanges "to better compete with the growing OTC market in customized equity options, thereby encouraging fair competition among brokers and dealers and exchange markets."⁶¹ The Commission has also stated that the elimination of position and exercise limits for FLEX Equity

⁵⁶ See Securities Exchange Act Release No. 99222 (December 21, 2023), 88 FR 89771 (December 28, 2023) (SR-CBOE-2023-018) ("FLEX Settlement Pilot Approval"). In support of making the pilot a permanent program, Cboe cited to its own review of pilot data during the course of the pilot program and a study by the Commission's Division of Economic and Risk Analysis ("DERA") staff. See FLEX Settlement Pilot Approval, notes 18 and 35.

⁵⁷ Specifically, Cboe evaluated each FLEX PM Third Friday Options trade for more than 500 contracts that occurred on Cboe during a two-year timeframe and analyzed the market quality (specifically, the average time-weighted quote spread and size 30 minutes prior to the trade and the average time-weighted quote spread and size 30 minutes after the trade) of series non-FLEX a.m.-settled options overlying the same index with similar terms as the FLEX PM Third Friday Option that traded (time to expiration, type (call or put), and strike price) as set forth in the Cboe's data. See Securities Exchange Act Release No. 99222 (December 21, 2023), 88 FR 89771 (December 28, 2023) (SR-CBOE-2023-018) ("FLEX Settlement Pilot Approval"). In support of making the pilot a permanent program, Cboe cited to its own review of pilot data during the course of the pilot program and a study by the Commission's Division of Economic and Risk Analysis ("DERA") staff. See FLEX Settlement Pilot Approval, notes 18 and 35.

⁵⁸ The Exchange acknowledges that, while FLEX PM Third Friday Options has historically represented a very small percentage of overall volume, it is possible trading in these options may grow in the future.

⁵⁹ See Cboe Rules 8.35(a), (b), (d), and 8.42(g) and Phlx Options 4A, Sections 6(a), 9(a)(13), and 9(a)(14).

⁶⁰ See proposed Options 8, Section 34(i)(4)(c) and Section 34(j)(1)(c). See also Cboe Rules 8.35(d)(3) and 8.42(g)(3); NYSE Arca Rules 5.35-O(a)(iii), (b) and 5.36-O; NYSE American Rules 906G and 907G; and Phlx Options 8, Section 34(e) and (f).

⁶¹ See Securities Exchange Act Release No. 42223 (December 10, 1999), 64 FR 71158, 71159 (December 20, 1999) (SR-Amex-99-40) (SR-PCX-99-41) (SR-CBOE-99-59) (Order Granting Accelerated Approval to Proposed Rule Change Relating to the Permanent Approval of the Elimination of Position and Exercise Limits for FLEX Equity Options).

Options “could potentially expand the depth and liquidity of the FLEX equity market without significantly increasing concerns regarding intermarket manipulations or disruptions of the options or the underlying securities.”⁶²

Additionally, the Exchange believes that requiring positions in FLEX Equity Options that expire on a third Friday-of-the-month to be aggregated with positions in non-FLEX Equity Options on the same underlying security subjects FLEX Equity Options and non-FLEX Equity Options to the same position and exercise limits on third Friday-of-the-month expirations. These limitations are intended to serve as a safeguard against potential adverse effects of large FLEX Equity Option positions expiring on the same day as non-FLEX Equity Option positions. As noted above, Cboe Rules 8.35(d)(3) and 8.42(g)(3) have the same requirements.

The Exchange believes that any potential risk of manipulative activity is mitigated by existing surveillance technologies, procedures, and reporting requirements at the Exchange, which allows the Exchange to properly identify disruptive and/or manipulative trading activity. In addition to its own surveillance programs, the Exchange also works with other SROs and exchanges on intermarket surveillance related issues. Through its participation in ISG, the Exchange shares information and coordinates inquiries and investigations with other exchanges designed to address potential intermarket manipulation and trading abuses. The Exchange also notes that FINRA conducts cross-market surveillances on behalf of the Exchange pursuant to a regulatory services agreement.⁶³ The Exchange also represents that it is reviewing its procedures to detect potential manipulation in light of any changes required for FLEX Options to confirm appropriate surveillance coverage. These procedures utilize daily monitoring of market activity via automated surveillance techniques to identify unusual activity in both options and their underlying securities and are designed to protect investors and the public interest by ensuring that the Exchange has an adequate surveillance program in place.

Lastly, the Exchange notes that other exchanges currently trading FLEX options have similar position and exercise limits described above.⁶⁴

Cash-Settled Exchange Traded Funds (“ETFs”)

Introducing cash-settled FLEX ETF Options will increase order flow to the Exchange, increase the variety of options products available for trading, and provide a valuable tool for investors to manage risk.

The Exchange believes that the proposal to permit cash settlement as a contract term for options on the specified group of equity securities would remove impediments to and perfect the mechanism of a free and open market as cash-settled FLEX ETF Options would enable market participants to receive cash in lieu of shares of the underlying security, which would, in turn provide greater opportunities for market participants to manage risk through the use of a cash-settled product to the benefit of investors and the public interest. The Exchange does not believe that allowing cash settlement as a contract term for options on the specified group of equity securities would render the marketplace for equity options more susceptible to manipulative practices. As illustrated in the table above, each of the qualifying underlying securities is actively traded and highly liquid and thus would not be susceptible to manipulation because, over a six-month period, each security had an average daily notional value of at least \$500 million and an ADV of at least 4,680,000 shares, which indicates that there is substantial liquidity present in the trading of these securities, and that there is significant depth and breadth of market participants providing liquidity and of investor interest. The Exchange believes the proposed bi-annual review to determine eligibility for an underlying ETF to have cash settlement as a contract term would remove impediments to and perfect the mechanism of a free and open market as it would permit the Exchange to select only those underlying ETFs that are actively traded and have robust liquidity as each qualifying ETF would be required to meet the average daily notional value and average daily volume requirements, as well as to select the same underlying ETFs on which other exchanges may list cash-settled FLEX ETF Options.⁶⁵

⁶⁵ See Securities Exchange Act Release No. 88131 (February 5, 2020), 85 FR 7806 (February 11, 2020) (SR–NYSEAmex–2019–38) (Notice of Filing of Amendment No. 1 and Order Granting Accelerated Approval of a Proposed Rule Change, as Modified by Amendment No. 1, To Allow Certain Flexible Equity Options To Be Cash Settled). Cboe also filed an immediately effective rule change to allow certain FLEX Options to be cash settled. See Securities Exchange Act Release No. 98044 (August 2, 2023), 88 FR 53548 (August 8, 2023) (SR–Cboe–

The Exchange believes the proposed change that, for FLEX ETF Options, at least one of exercise style, expiration date, and exercise price must differ from options in the non-FLEX market will provide clarity and eliminate confusion regarding permissible terms of FLEX ETF Options, including the proposed cash-settled FLEX ETF Options.

The Exchange believes that the data provided by the Exchange supports the supposition that permitting cash settlement as a FLEX term for the 48 underlying ETFs that would currently qualify to have cash settlement as a contract term would broaden the base of investors that use FLEX Equity Options to manage their trading and investment risk, including investors that currently trade in the OTC market for customized options, where settlement restrictions do not apply.

The Exchange believes that the proposal to permit cash settlement for certain FLEX ETF options would remove impediments to and perfect the mechanism of a free and open market because the proposed rule change would provide members and member organizations with enhanced methods to manage risk by receiving cash if they choose to do so instead of the underlying security. In addition, this proposal would promote just and equitable principles of trade and protect investors and the general public because cash settlement would provide investors with an additional tool to manage their risk. Further, the Exchange notes that another exchange has previously received approval that allows for the trading of cash-settled options, and, specifically, cash-settled FLEX ETF Options in an identical manner as the Exchange proposes to list them pursuant to this rule filing.⁶⁶ The proposed rule change therefore should not raise issues for the Commission that it has not previously addressed.

The proposed rule change to permit cash settlement as a contract term for options on up to 50 ETFs is designed to promote just and equitable principles of trade in that the availability of cash settlement as a contract term would give market participants an alternative to trading similar products in the OTC market. By trading a product in an exchange-traded environment (that is currently traded in the OTC market), the Exchange would be able to compete more effectively with the OTC market. The Exchange believes the proposed

2023–036) (Notice of Filing and Immediate Effectiveness of a Proposed Rule Change To Allow Certain Flexible Exchange Equity Options To Be Cash Settled).

⁶⁶ See *supra* note 39.

⁶² See *id.*

⁶³ The Exchange notes that it is responsible for FINRA’s performance under this regulatory services agreement.

⁶⁴ See Cboe Rules 8.35(d) and 8.42(g).

rule change is designed to prevent fraudulent and manipulative acts and practices in that it would lead to the migration of options currently trading in the OTC market to trading on the Exchange. Also, any migration to the Exchange from the OTC market would result in increased market transparency. Additionally, the Exchange believes the proposed rule change is designed to remove impediments to and to perfect the mechanism for a free and open market and a national market system, and, in general, to protect investors and the public interest in that it should create greater trading and hedging opportunities and flexibility. The proposed rule change should also result in enhanced efficiency in initiating and closing out positions and heightened contra-party creditworthiness due to the role of OCC as issuer and guarantor of the proposed cash-settled options. Further, the proposed rule change would result in increased competition by permitting the Exchange to offer products that are currently available for trading only in the OTC market and are approved to trade on another options exchange.

The Exchange believes that establishing position limits for cash-settled FLEX ETF Options to be the same as physically settled options on the same underlying security, and aggregating positions in cash-settled FLEX ETF Options with physically settled options on the same underlying security for purposes of calculating position limits is reasonable and consistent with the Act. By establishing the same position limits for cash-settled FLEX ETF Options as for physically settled options on the same underlying security and, importantly, aggregating such positions, the Exchange believes that the position limit requirements for cash-settled FLEX ETF Options should help to ensure that the trading of cash-settled FLEX ETF Options would not increase the potential for manipulation or market disruption and could help to minimize such incentives. For the same reasons, the Exchange believes the proposed exercise limits are reasonable and consistent with the Act.

Finally, the Exchange represents that it has an adequate surveillance program in place to detect manipulative trading in cash-settled FLEX ETF Options and the underlying ETFs. Regarding the proposed cash settlement, the Exchange would use the same surveillance procedures currently utilized for the Exchange's other FLEX Options. For surveillance purposes, the Exchange would have access to information regarding trading activity in the pertinent underlying ETFs. The

Exchange believes that limiting cash settlement to no more than 50 underlying ETFs (currently, 48 ETFs would be eligible to have cash-settlement as a contract term) would minimize the possibility of manipulation due to the robust liquidity in both the equities and options markets.

As a self-regulatory organization, the Exchange recognizes the importance of surveillance, among other things, to detect and deter fraudulent and manipulative trading activity as well as other violations of Exchange rules and the federal securities laws. As discussed above, Phlx has adequate surveillance procedures in place to monitor trading in cash-settled FLEX ETF Options and the underlying securities, including to detect manipulative trading activity in both the options and the underlying ETF.⁶⁷ The Exchange further notes the liquidity and active markets in the underlying ETFs, and the high number of market participants in both the underlying ETFs and existing options on the ETFs, helps to minimize the possibility of manipulation. The Exchange further notes that under Section 19(g) of the Act, the Exchange, as a self-regulatory organization, is required to enforce compliance by its members and persons associated with its members with the Act, the rules and regulations thereunder, and the rules of the Exchange.⁶⁸ The Exchange believes

⁶⁷ Among other things, Phlx's regulatory program includes cross-market surveillance designed to identify manipulative and other improper trading, including spoofing, algorithm gaming, marking the close and open, as well as more general abusive behavior related to front running, wash sales, and quoting/routing, which may occur on the Exchange and other markets. Furthermore, the Exchange stated that it has access to information regarding trading activity in the pertinent underlying securities as a member of ISG. As it relates to Reg SHO violations, the Exchange will enforce this through its Stock-Tied Reg SHO price protections in Options 3, Section 16(b). Specifically, Options 3, Section 16(b) provides that when the short sale price test in Rule 201 of Regulation SHO is triggered for a covered security, NES will not execute a short sale order in the underlying covered security component of a Complex Order if the price is equal to or below the current national best bid. However, NES will execute a short sale order in the underlying covered security component of a Complex Order if such order is marked "short exempt," regardless of whether it is at a price that is equal to or below the current national best bid. If NES cannot execute the underlying covered security component of a Complex Order in accordance with Rule 201 of Regulation SHO, the Exchange will cancel back the Complex Order to the entering member organization. For purposes of this paragraph, the term "covered security" shall have the same meaning as in Rule 201(a)(1) of Regulation SHO. NES will only execute the underlying covered security component of a Complex Order if the underlying covered security component is in accordance with Rule 201 of Regulation SHO.

⁶⁸ 15 U.S.C. 78s(g).

its surveillance, along with the liquidity criteria and position and exercise limits requirements, are reasonably designed to mitigate manipulation and market disruption concerns and will permit it to enforce compliance with the proposed rules and other Exchange rules in accordance with Section 19(g) of the Act. The Exchange performs ongoing evaluations of its surveillance program to ensure its continued effectiveness and will continue to review its surveillance procedures on an ongoing basis and make any necessary enhancements and/or modifications that may be needed for the cash settlement of FLEX ETF Options.

Additionally, the Exchange will monitor any effect additional options series listed under the proposed rule change may have on market fragmentation and the capacity of the Exchange's automated systems. The Exchange will take prompt action, including timely communication with the Commission and with other self-regulatory organizations responsible for oversight of trading in options, the underlying ETFs, and the ETFs' component securities, should any unanticipated adverse market effects develop.

B. Self-Regulatory Organization's Statement on Burden on Competition

The Exchange does not believe that the proposed rule change will impose any burden on competition that is not necessary or appropriate in furtherance of the purposes of the Act.

The Exchange does not believe that the proposed rule change will impose any burden on intra-market competition that is not necessary or appropriate in furtherance of the purposes of the Act, as all member organizations who wish to trade FLEX Options will be able to trade such options in the same manner. Additionally, positions in FLEX Options of all member organizations will be subject to the same position limits, and such positions will be aggregated in the same manner as described in proposed Options 8, Section 34(i)(4).

The Exchange also does not believe that the proposed rule change will impose any burden on inter-market competition that is not necessary or appropriate in furtherance of the purposes of the Act. The proposal promotes inter-market competition by providing another alternative (*i.e.*, exchange markets) to bilateral OTC trading of options with flexible terms. Exchange markets, in contrast with bilateral OTC trading, are centralized, transparent, and have the guarantee of OCC for options traded.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

No written comments were either solicited or received.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period (i) as the Commission may designate up to 90 days of such date if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the Exchange consents, the Commission shall: (a) by order approve or disapprove such proposed rule change, or (b) institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-Phlx-2024-51 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.
- All submissions should refer to file number SR-Phlx-2024-51. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and

printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR-Phlx-2024-51 and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁶⁹

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2024-25052 Filed 10-28-24; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-101415; File No. SR-CBOE-2024-041]

Self-Regulatory Organizations; Cboe Exchange, Inc.; Notice of Filing of a Proposed Rule Change With Respect to Amendments to the Seventh Amended and Restated Bylaws (the "CGM Bylaws") of Its Parent Corporation, Cboe Global Markets, Inc. ("Cboe" or "Corporation")

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (the "Act"),¹ and Rule 19b-4 thereunder,² notice is hereby given that on October 11, 2024, Cboe Exchange, Inc. (the "Exchange" or "Cboe Options") filed with the Securities and Exchange Commission ("Commission") the proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization's Statement of the Terms of Substance of the Proposed Rule Change

Cboe Exchange, Inc. (the "Exchange" or "Cboe Options") is filing with the Securities and Exchange Commission

(the "Commission") a proposed rule change with respect to amendments to the Seventh Amended and Restated Bylaws (the "CGM Bylaws") of its parent corporation, Cboe Global Markets, Inc. ("Cboe" or "Corporation"). The text of the proposed rule change is provided in Exhibit 5.

The text of the proposed rule change is also available on the Exchange's website (<http://www.cboe.com/AboutCBOE/CBOELegalRegulatoryHome.aspx>), at the Exchange's Office of the Secretary, and at the Commission's Public Reference Room.

II. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the Exchange included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

At Cboe's annual meeting held on May 16, 2024, Cboe's stockholders considered two advisory proposals that would provide Cboe stockholders with the right to call a special meeting of the stockholders provided that a certain threshold percentage of stockholders propose to call such a meeting. The two proposals were submitted separately. One of the proposals was submitted by an individual stockholder ("Stockholder Proposal"). The other proposal was submitted by Cboe Management ("Management Proposal"). The Stockholder Proposal, which did not pass but received 45% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 10% of Cboe's voting power to call a special meeting of the stockholders. The Management Proposal, which passed with 65% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 25% of Cboe's voting power to call a special meeting of the stockholders.

The Nominating & Governance Committee of the CGM Board reviewed the voting results of the Stockholder

⁶⁹ 17 CFR 200.30-3(a)(12).

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

Proposal and the Management Proposal and discussed the stockholder voting standards and rights contemplated by the CGM Bylaws. Following this review, the Nominating & Governance Committee recommended to the CGM Board, and the CGM Board approved, certain changes to the CGM Bylaws to implement the Management Proposal. The CGM Board also approved amending the CGM Bylaws to improve the governance processes of Cboe, to make certain provisions more consistent with Delaware General Corporation Law ("DGCL"), and to make clarifying and cleanup changes to the CGM Bylaws. The proposed rule change amends the CGM Bylaws to implement the changes approved by the CGM Board.

Proposed Changes to Article 2—Stockholders

Current Section 2.3 (Special Meeting) of the CGM Bylaws provides that only the Chair of the Board, the Chief Executive Officer or the CGM Board may call a special meeting of the stockholders. To respond to feedback from its stockholders, as discussed above, Cboe proposes to delete portions of this provision and add language that will provide Cboe stockholders with the right to call special stockholder meetings (a "Stockholder Requested Special Meeting") after following particular procedures.

In defining the procedural requirements, Cboe's goals are to ensure timely notice of a meeting request and to gather sufficient information about the proposing stockholder(s) and the proposed business itself. Among other things, this information will help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to adequately assess proposed business submitted by stockholders. Additionally, Cboe notes that the proposed terms are common among public companies that have adopted a right for stockholders to call special meetings. The proposed changes to the CGM Bylaws to effect the stockholder special meeting right are set forth below.

Revisions to Section 2.3(a)

First, the proposed changes to Section 2.3(a) provide that a Stockholder Requested Special Meeting may be called: (i) at any time by the CGM Board pursuant to a resolution adopted by the affirmative vote of a majority of the total number of CGM directors then in office; or (ii) by Cboe's Corporate Secretary following the receipt of a written request in proper form for a special meeting (a "Special Meeting Request")

by one or more stockholders. In order to call a special meeting, the stockholders must hold, in the aggregate, at least 25% of Cboe's outstanding shares of common stock entitled to vote on matters brought before the special meeting (the "Requisite Percentage").

The proposed changes to Section 2.3(a) also clarify that the Chair of the Board, the Chief Executive Officer or the President of Cboe may not individually call a special meeting of the stockholders. This change was made to vest authority within Cboe to call a special meeting in the Board. Without the proposed change, the Chair of the Board, Chief Executive Officer and the President could each call a special meeting of the stockholders without CGM Board approval. The proposed change to Section 2.3(a) simplifies this requirement to confirm that, within Cboe, only the CGM Board may call for a special meeting of the stockholders.

Proposed Section 2.3(b) and Section 2.3(c)

Proposed Section 2.3(b) and Section 2.3(c) set forth the procedures a stockholder must follow in order to submit a written request in proper form to call a Stockholder Requested Special Meeting. Stockholders must first submit a request to Cboe's Corporate Secretary to define a date on which the Requisite Percentage will be determined (the "Record Date"). A stockholder must sign any request to set a Record Date and also provide a reasonably brief description of the purpose or purposes of the special meeting of the stockholders. A stockholder is also required in the request to set a Record Date to disclose certain information regarding themselves and any individuals or entities such stockholder may be associated with (a "Stockholder Associated Person(s)"), as well as such information concerning any nominees to the CGM Board ("Stockholder Nominee(s)") if such stockholder is so proposing. The information that a stockholder must disclose regarding Stockholder Associated Persons and Stockholder Nominees is contained in Section 2.11 of the CGM Bylaws and incorporated by reference in this Section 2.3(b). The information required to be provided in the request to set a Record Date provides Cboe with notice that a stockholder is seeking to bring business before the stockholders and assists with the logistical aspects of determining which stockholders will be counted for purposes of determining whether the Requisite Percentage is met.

Proposed Section 2.3(d) and Section 2.3(e)

Proposed Section 2.3(d) and Section 2.3(e) include detailed information on the requirements for a Special Meeting Request to have been properly delivered, subject to certain carve-outs for stockholders who submit their request in response to a solicitation for public consent by the Corporation made pursuant to Section 14 of the Exchange Act. Specifically, a Special Meeting Request must:

- be delivered within 60 days following the Record Date;
- be signed by each stockholder making up the Requisite Percentage;
- contain a reasonably brief description of the purpose of the special meeting;
- include details of each stockholder holding the Requisite Percentage, including:
 - The stockholder's name;
 - The stockholder's address;
 - information concerning the stockholder submitting the Special Meeting Request and any Stockholder Associated Persons;
 - information concerning any Stockholder Nominees; and
 - documentary evidence that the shares included in the Requisite Percentage are owned by such stockholder;
- include an acknowledgment that any reduction in the number of shares owned by such stockholders as of the date of such Special Meeting Request and through the meeting date will constitute a revocation of such Special Meeting Request with respect to such reduction;
- relate to an item of business that is a proper subject for stockholder action under applicable law;
- not include an item of business that did not appear on the request to set a Record Date;
- not be delivered during the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting and ending on the date of the next annual meeting; and
- otherwise comply with applicable law.

In defining the requirements for a Special Meeting Request, Cboe's goal is to gather sufficient information about the stockholder seeking to request a special meeting and the proposed business for both itself and its stockholders and to help ensure the efficient use of corporate resources by restricting a stockholder from raising items that could reasonably be addressed at an annual meeting of the

stockholders, as in the requirement that a Special Meeting Request not be delivered in the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting. Overall, this information is designed to help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to assess the proposed business or Stockholder Nominee adequately.

Proposed Section 2.3(f)

Proposed Section 2.3(f) provides that the CGM Board may cancel a special meeting in its discretion if the percentage of stock held by the stockholders requesting a special meeting falls below the Requisite Percentage at any point after sixty (60) days from the first date on which a valid Special Meeting Request is delivered to Cboe. This provides the CGM Board with discretion to reevaluate the Special Meeting Request in the event the Special Meeting Request is revoked by stockholders holding a sufficient percentage of the stock of the Corporation.

Proposed Section 2.3(g)

Proposed Section 2.3(g) provides that within ten (10) days following the date on which the Secretary has received valid Special Meeting Requests, the CGM Board shall fix the record date and meeting date, time and location for the Stockholder Requested Special Meeting, provided that the date of any such Stockholder Requested Special Meeting shall not be more than ninety (90) days after the date on which a valid Special Meeting Request is received by Cboe. The CGM Board may submit its own proposal or proposals for consideration at any Stockholder Requested Special Meeting. Ninety (90) days allows the Corporation reasonable time to assess the items proposed in the Special Meeting Request while also not imposing a potentially burdensome delay on the stockholders.

Proposed Section 2.3(h)

Proposed Section 2.3(h) provides that multiple Special Meeting Requests may be considered together if (i) each Special Meeting Request identifies the same or substantially the same purpose or purposes of the Stockholder Requested Special Meeting and the same or substantially the same items of business proposed to be brought before the Stockholder Requested Special Meeting, and (ii) such Special Meeting Requests have been dated and delivered to the Corporate Secretary within sixty (60)

days of the delivery to the Corporate Secretary of the earliest dated Special Meeting Request relating to such item(s) of business. This proposed section helps to ensure the efficient use of corporate resources by preventing multiple stockholders from raising items that should reasonably be consolidated. The conditions under which the Corporation may combine multiple Special Meeting Requests are sufficiently limited to require that each unique item is addressed separately.

Revisions to Section 2.9

Section 2.9 of the CGM Bylaws governs proxy representation. It is proposed that language be added to clarify that any stockholder directly or indirectly soliciting proxies from other stockholders of the Corporation may use any proxy card color other than white, which shall be reserved for exclusive use by the CGM Board.

Revisions to Section 2.11

Section 2.11 of the CGM Bylaws, which are the “advance notice bylaws”,³ requires stockholders to notify Cboe, during a specified period in advance of an annual meeting or special meeting called by the CGM Board, of their intention to nominate one or more persons for election to the CGM Board or to present a business proposal for consideration by the stockholders at the meeting and provide certain information regarding such request. When designing the proposed procedural requirements for stockholders to call a special meeting, as outlined above, Cboe evaluated the existing procedural requirements for stockholders to bring business before an annual meeting or to nominate director candidates at an annual meeting or special meeting. Cboe has determined that the advance notice bylaws may be enhanced to help achieve the core objectives of fulsome disclosure and accurate explanations from stockholders bringing business or potential nominees before a stockholder meeting. While advance notice bylaws are beneficial in providing a company and its stockholders with information regarding stockholders, and their Stockholder Associated Persons, seeking to bring business or potential nominees before a stockholder meeting, therefore permitting orderly meetings and

³ “Advance notice bylaws” allow stockholder(s) to bring business before an annual or special meeting of stockholders, but set forth procedural requirements to help ensure that companies and boards have sufficient information about the proposal and the proposing stockholder(s), as well as adequate time to consider the proposal, by requiring the proposing stockholder(s) to give advance notice of the intention to bring the proposal before the annual or special meeting.

election contests, and assisting the board’s information gathering and disclosure functions, the Delaware Supreme Court in *Kellner v. AIM ImmunoTech Inc.*⁴ has recently provided some guidance on circumstances where such requests may be overbroad or request information not sufficiently connected to the legitimate information gathering function these provisions serve. Therefore, as further detailed below, Cboe has determined that it would be beneficial to refine certain of the provisions in the CGM Bylaws to increase the clarity of the requests for information from stockholders seeking to bring business before a meeting.

First, Section 2.11(a)(iii)(C) of the CGM Bylaws currently defines the information required to be disclosed regarding a stockholder providing notice of nominations or other business, any Stockholder Associated Person(s) and any Stockholder Nominee(s). Cboe proposes certain amendments to this section to (i) clarify the information a stockholder is required to disclose relating to arrangements between the stockholder providing notice or any Stockholder Associated Person and any other stockholder with regard to the stockholder meeting and (ii) eliminate disclosures on performance related fees to which such stockholder or Stockholder Associated Person may be entitled as a result of any increase or decrease in the stock of Cboe, and the prospectus or similar document of the stockholder providing notice or any Stockholder Associated Person. Cboe believes that, while these provisions as currently written provide valuable information to the Corporation and its stockholders in assessing the proposed business or Stockholder Nominee, these requirements should be sufficiently specific so as not to potentially dissuade stockholders from bringing business before a stockholder meeting and should otherwise comply with Delaware law. The proposed changes narrow the information required to be disclosed such that Cboe is able to help ensure the objectives of the provisions are met without burdening stockholders with potentially overbroad requests for information.

Section 2.11(a)(iii)(D) of the CGM Bylaws currently sets forth certain representations that must be made by a stockholder seeking to bring business or a Stockholder Nominee before a stockholder meeting regarding whether such stockholder is part of a group which intends to deliver or solicit

⁴ *Kellner v. AIM ImmunoTech Inc.*, C.A. 2023–0879–LWW (Del. Ch. Jan. 5, 2024)

proxies from stockholders in support of such proposed business. Cboe proposes changes to update this section in order to be more consistent with the universal proxy rules provided for in Rule 14a–19 of the Exchange Act by explicitly stating that any stockholder providing notice that they intend to solicit proxies in support of a proposed nominee must do so in accordance with Rule 14a–19 of the Exchange Act. Cboe also proposes to clarify that the representation must confirm whether the stockholder intends or is part of a group which intends to engage in a solicitation (within the meaning of Rule 14a–1(1) of the Exchange Act) with respect to the nomination of any proposed nominee or proposed business to be considered at the meeting.

Section 2.11(a)(iii)(F) of the CGM Bylaws currently requires that a Stockholder Nominee furnish any information that Cboe may determine is required for Cboe to determine the qualifications of such Stockholder Nominee to serve as a director of the Corporation. Cboe proposes to add language clarifying that the information Cboe may require must be consistent with the parameters set forth in Cboe's Corporate Governance Guidelines or the CGM Board's past practice in evaluating potential director nominees.

Proposed Section 2.11(c)(ii) of the CGM Bylaws requires the stockholder providing notice to notify the Secretary of any inaccuracy or change in any information submitted pursuant to Section 2.11 within two (2) business days of becoming aware of such inaccuracy or change. Cboe proposes to modify this requirement by narrowing the scope of circumstances in which a stockholder is required to provide notice of any inaccuracy or change of information that they have previously provided to material inaccuracies or changes.

Proposed Section 2.11(c)(iii) of the CGM Bylaws provides that any stockholder or Stockholder Associated Person providing notice with respect to any Stockholder Nominee is required to do so in a manner consistent with the requirements for universal proxy rules pursuant to Rule 14a–19 of the Exchange Act. Namely, the nomination of a Stockholder Nominee shall be disregarded if, among other things, there is no longer an intent to solicit proxies in support of a Stockholder Nominee or there is a failure to comply with the applicable requirements of Rule 14a–19. Upon request by the Corporation, if any stockholder providing notice or any Stockholder Associated Person provides notice pursuant to Rule 14a–19(b) under the Exchange Act, such stockholder

providing notice shall deliver to the Corporate Secretary, no later than five (5) business days prior to the applicable meeting date, then reasonable evidence that the requirements of Rule 14a–19(a)(3) under the Exchange Act have been satisfied.

Currently Section 2.11(c)(vi) of the CGM Bylaws defines "Stockholder Associated Person" to mean, among other things, (i) any person who is a member of a "group" (used in Rule 13d–5 under the Exchange Act) with, or otherwise acting in concert with, any stockholder providing notice, (ii) any person that is directly or indirectly controlled by, or under common control with, such stockholder or such Stockholder Associated Person, or (iii) any person directly or indirectly controlling any such stockholder or any Stockholder Associated Person. The proposed rule change reflects recent developments in Delaware law to add specificity to the definition and limit which individuals may be determined to be a Stockholder Associated Person and makes other clarifying changes. Specifically, the proposed rule change adds the qualifier that a Stockholder Associated Person must be known by the stockholder to be acting in concert with such stockholder, removes from the definition any person directly or indirectly controlled by, or under common control with such stockholder and replaces it with any affiliate or associate of such stockholder providing notice, and deletes the reference in the definition to any person directly or indirectly controlling any such stockholder or Stockholder Associated Person. The proposed rule change also adds any Stockholder Nominee to the definition of Stockholder Associated Person.

Revisions to Other Sections of the Bylaws

Cboe also proposes to make changes to Section 2.11 to reflect recent developments in Delaware law and to provide clarifications and prevent confusion. Cboe proposes to add a note to Section 2.11(a)(ii) that any proposed business for a stockholder meeting must be a proper matter for stockholder action. Cboe also proposes to amend Section 2.11(a)(iii)(B) to state that a Stockholder Nominee's written consent must be included in Cboe's proxy statement before they may be brought before a meeting. Previously, Section 2.11(a)(iii)(B) had stated that the Stockholder Nominee's written consent must be included in a proxy statement, but had not specifically defined it as Cboe's proxy statement. Cboe also proposes to amend the same section to

state that a Stockholder Nominee will not enter into any commitment to vote in a certain manner if nominated to the CGM Board. Previously, this section had simply stated that a Stockholder Nominee may not enter into any commitment to vote in a certain manner with respect to certain matters at any company, without defining Cboe specifically. Cboe also proposes to amend the same section to require that a Stockholder Nominee not omit facts that are necessary to ensure statements made are not misleading in any material respect. Previously, the Stockholder Nominee's responsibility to not omit facts that are necessary to ensure statements are not misleading was not subject to materiality.

Cboe also proposes to make changes to Section 3.10 of the CGM Bylaws to provide that the Lead Director of Cboe may call a special meeting of the CGM Board. Section 3.10 currently permits, among other things, the Chair of the Board or the Chief Executive Officer to call a special meeting of the CGM Board. Revising this section to allow the Lead Director to call a special meeting of the CGM Board addresses a potential scenario in which the Chair of the Board and the Chief Executive Officer positions are jointly held by one individual and a special meeting of the CGM Board is not able to be called by individual independent directors.

2. Statutory Basis

The Exchange believes the proposed rule change is consistent with the Act and the rules and regulations thereunder applicable to the Exchange and, in particular, the requirements of Section 6(b) of the Act.⁵ Specifically, the Exchange believes the proposed rule change is consistent with the Section 6(b)(5)⁶ requirements that the rules of an exchange be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.

In light of an advisory vote by the stockholders of Cboe, Cboe is proposing changes to its Bylaws to implement a right for stockholders to call a special meeting of the stockholders at a 25% threshold. The Exchange believes that

⁵ 15 U.S.C. 78f(b).

⁶ 15 U.S.C. 78f(b)(5).

this filing furthers the objectives of Section 6(b)(5) of the Act because the proposed rule change would be consistent with and facilitate a governance and regulatory structure that is designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to, and perfect the mechanism of a free and open market and a national market system and, in general, to protect investors and the public interest. Particularly, the Exchange believes that, by permitting stockholders of Cboe to bring business or Stockholder Nominees before a special meeting, the proposed rule change strengthens the corporate governance of the Exchange's ultimate parent company, which is beneficial to both investors and the public interest.

Additionally, the procedural requirements are designed to help protect investors by stating clearly and explicitly the procedures stockholders must follow in order to bring business or Stockholder Nominees before a special meeting. The informational requirements are designed to enhance investor protection by helping to ensure among other things, that the Corporation and its stockholders have full and accurate information about nominating stockholders and Stockholder Nominees and that such stockholders and nominees comply with applicable laws, regulations and other requirements.

The changes that the Exchange is proposing with regard to so-called "advance notice bylaws" in light of the recent developments in Delaware law are designed to help provide additional clarity to stockholders wishing to bring business before a stockholder meeting or propose a Stockholder Nominee. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) by simplifying the requirements and clarifying the information that must be disclosed by stockholders. This furthers the interests of investors and the public by removing potential impediments to raising business or proposing Stockholder Nominees that may otherwise restrict a stockholder's ability to participate in the corporate governance of the Corporation.

Finally, the remaining changes to existing provisions of the CGM Bylaws are clarifying in nature, and they enhance investor protection and the public interest by preventing confusion with respect to the operation of the Bylaw provisions.

B. Self-Regulatory Organization's Statement on Burden on Competition

Because the proposed rule change relates to the governance of the Corporation and not to the operations of the Exchange, the Exchange does not believe that the proposed rule change will impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. The proposed rule change is not designed to address any competitive issue or have any impact on competition; rather, adoption of a stockholder special meeting provision, updating "advance notice bylaws," and other bylaws updates by the Corporation are intended to enhance corporate governance and accountability to stockholders.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

The Exchange neither solicited nor received comments on the proposed rule change.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the Exchange consents, the Commission will:

- A. by order approve or disapprove such proposed rule change, or
- B. Institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-CBOE-2024-041 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

All submissions should refer to file number SR-CBOE-2024-041. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR-CBOE-2024-041 and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁷

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2024-25053 Filed 10-28-24; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Investment Company Act Release No. 35328A; 812-15596]

Gemcorp Capital Advisors LLC and Gemcorp Commodities Alternative Products Fund

October 23, 2024.

AGENCY: Securities and Exchange Commission ("Commission" or "SEC").
ACTION: Notice.

Notice of an application under section 6(c) of the Investment Company Act of 1940 (the "Act") for an exemption from

⁷ 17 CFR 200.30-3(a)(12).

sections 18(a)(2), 18(c) and 18(i) of the Act, under sections 6(c) and 23(c) of the Act for an exemption from rule 23c-3 under the Act, and for an order pursuant to section 17(d) of the Act and rule 17d-1 under the Act.

SUMMARY OF APPLICATION: Applicants request an order to permit certain registered closed-end investment companies to issue multiple classes of shares and to impose asset-based distribution and/or service fees and early withdrawal charges.¹

APPLICANTS: Gemcorp Capital Advisors LLC and Gemcorp Commodities Alternative Products Fund.

FILING DATES: The application was filed on June 28, 2024, and amended on July 11, 2024, August 23, 2024, and October 22, 2024.

HEARING OR NOTIFICATION OF HEARING: An order granting the requested relief will be issued unless the Commission orders a hearing. Interested persons may request a hearing on any application by emailing the SEC's Secretary at Secretaries-Office@sec.gov and serving the Applicants with a copy of the request by email, if an email address is listed for the relevant Applicant below, or personally or by mail, if a physical address is listed for the relevant Applicant below. Hearing requests should be received by the Commission by 5:30 p.m. on November 13, 2024, and should be accompanied by proof of service on the Applicants, in the form of an affidavit, or, for lawyers, a certificate of service. Pursuant to rule 0-5 under the Act, hearing requests should state the nature of the writer's interest, any facts bearing upon the desirability of a hearing on the matter, the reason for the request, and the issues contested. Persons who wish to be notified of a hearing may request notification by emailing the Commission's Secretary.

ADDRESSES: The Commission: Secretaries-Office@sec.gov. Applicants: Sally-Jane Miller, sjmiller@gemcorp.net, with a copy to Kaitlin McGrath, Esq., Dechert LLP, One International Place, 40th Floor, 100 Oliver Street, Boston, Massachusetts 02110-2605.

FOR FURTHER INFORMATION CONTACT: Trace W. Rakestraw, Senior Special Counsel, at (202) 551-6825 (Division of Investment Management, Chief Counsel's Office).

SUPPLEMENTARY INFORMATION: For Applicants' representations, legal analysis, and conditions, please refer to Applicants' application, dated October

22, 2024, which may be obtained via the Commission's website by searching for the file number at the top of this document, or for an Applicant using the Company name search field on the SEC's EDGAR system. The SEC's EDGAR system may be searched at <https://www.sec.gov/edgar/searchedgar/legacy/companysearch.html>. You may also call the SEC's Public Reference Room at (202) 551-8090.

For the Commission, by the Division of Investment Management, under delegated authority.

Sherry R. Haywood,

Assistant Secretary.

[FR Doc. 2024-25046 Filed 10-28-24; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-101418; File No. SR-SAPPHIRE-2024-32]

Self-Regulatory Organizations; MIAx Sapphire, LLC; Notice of Filing and Immediate Effectiveness of a Proposed Rule Change by MIAx Sapphire, LLC To Adopt Connectivity and Certain Port Fees for Members and Non-Members

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act"),¹ and Rule 19b-4 thereunder,² notice is hereby given that on October 10, 2024, MIAx Sapphire, LLC ("MIAx Sapphire" or "Exchange") filed with the Securities and Exchange Commission ("Commission") a proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization's Statement of the Terms of Substance of the Proposed Rule Change

The Exchange is filing a proposal to amend the MIAx Sapphire Options Exchange Fee Schedule (the "Fee Schedule") to adopt certain non-transaction fees. The text of the proposed rule change is available on the Exchange's website at <https://www.miaxglobal.com/markets/us-options/miax-sapphire/rule-filings>, at the Exchange's principal office, and at the Commission's Public Reference Room.

II. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the Exchange included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

On July 15, 2024, the U.S. Securities and Exchange Commission ("Commission") approved the Exchange's Form 1 application to register as a national securities exchange under Section 6 of the Exchange Act.³ The Exchange commenced electronic operations on August 12, 2024.⁴ The Exchange proposes to establish the following sections of the Fee Schedule, including proposed fee structures and amounts (the majority of which the Exchange proposes to waive for a specified time, as discussed further below): (1) connectivity fees for Members⁵ and non-Members; and (2) certain port fees for Members and non-Members.⁶ The Exchange initially filed this proposal on August 9, 2024 (SR-SAPPHIRE-2024-21). The Exchange withdrew SR-SAPPHIRE-2024-21 on August 14, 2024 and submitted SR-SAPPHIRE-2024-22. On October 10, 2024, the Exchange withdrew SR-

³ See Securities Exchange Act Release No. 100539 (July 15, 2024), 89 FR 58848 (July 19, 2024) (File No. 10-240) (the "Approval Order").

⁴ See MIAx Sapphire News Alert, dated August 13, 2024, available at <https://www.miaxglobal.com/alert/2024/08/13/miami-international-holdings-announces-successful-launch-miax-sapphire?nav=all>.

⁵ The term "Member" means an individual or organization that is registered with the Exchange pursuant to Chapter II of the Exchange's Rules for purposes of trading on the Exchange as an "Electronic Exchange Member" or "Market Maker." Members are deemed "members" under the Exchange Act. See Exchange Rule 100.

⁶ The Exchange filed a separate rule filing to establish fees for Purge Ports. See SR-SAPPHIRE-2024-15. "Purge Ports" provide Market Makers with the ability to send quote purge messages to the MIAx Sapphire System. Purge Ports are not capable of sending or receiving any other type of messages or information. See the Definitions section of the Fee Schedule. Fees for all other types of ports are proposed in this filing.

¹ The Commission issued a notice of application on September 19, 2024. Applicants subsequently amended the application on October 22, 2024, so a new notice is being issued.

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

SAPPHIRE–2024–22 and submitted this proposal.

Connectivity Fees

The Exchange proposes to establish Section 5), System Connectivity Fees, which will describe network connectivity fees. The Exchange proposes to offer to both Members and non-Members the choice of a 1 Gigabit (“Gb”) fiber connection or the 10Gb ultra-low latency (“ULL”) fiber connection to the Exchange’s primary and secondary facilities, as well as its disaster recovery facility. The 1Gb and 10Gb ULL fees will be charged to both Members and non-Members for connectivity to the Exchange’s primary/secondary facility and to its disaster recovery facility.

The Exchange proposes to establish monthly fees of \$1,400 per 1Gb connection and \$13,500 per 10Gb ULL connection that will be assessed to Members and non-Members for connecting to the primary/secondary facility. The Exchange proposes to establish monthly fees of \$550 per 1Gb connection and \$2,750 per 10Gb ULL connection that will be assessed to Members and non-Members for connecting to the disaster recovery facility.

Monthly network connectivity fees for Members and non-Members for connectivity with the primary/secondary facility will be assessed in any month the Member or non-Member is credentialed to use any of the MIAX Sapphire Application Programming Interfaces (“APIs”) or market data feeds in the production environment. Further, the Exchange proposes to pro-rate the monthly fees when a Member or non-Member makes a change to the connectivity (by adding or deleting connections) with such pro-rated fees based on the number of trading days that the Member or non-Member has been credentialed to utilize any of the MIAX Sapphire APIs or market data feeds in the production environment through such connection, divided by the total number of trading days in such month multiplied by the applicable monthly rate. Monthly network connectivity fees for Members and non-Members for connectivity to the disaster recovery facility will be assessed in each month during which the Member or non-Member has established connectivity to the disaster recovery facility.

The Exchange proposes that Members and non-Members utilizing the MENI⁷

⁷ The term “MENI” means the MIAX Express Network Interconnect, which is a network infrastructure which provides Members and non-

to connect to the trading platforms, market data systems, and disaster recovery facilities of the Exchange or its affiliated options markets (MIAX, MIAX Pearl, and MIAX Emerald)⁸ via a single, shared 1Gb connection will only be assessed one monthly network connectivity fee per connection, regardless of the trading platforms, market data systems, and disaster recovery facilities accessed via such connection.

Waiver Period for Connectivity Fees.

The Exchange proposes to waive the monthly Member and non-Member network connectivity fees for the 1Gb connections to the primary/secondary facility and disaster recovery facility, and the 10Gb ULL connections to the disaster recovery facility for the partial month in which the Exchange launches operations, plus an additional three full calendar months. The proposed monthly Member and non-Member network connectivity fees for the 1Gb connections to the primary/secondary facility and disaster recovery facility, and 10Gb ULL connections to the disaster recovery facility will be discounted by 50% for the three full calendar months thereafter.

The Exchange proposes to waive the monthly Member and non-Member network connectivity fees for the first two 10Gb ULL connections on each switch⁹ to the primary/secondary facility for the partial month in which the Exchange launches operations, plus an additional three full calendar months. The Exchange proposes that the monthly Member and non-Member network connectivity fees for the first

Members network connectivity to the MIAX Sapphire trading platform, market data systems, test systems, and disaster recovery facilities. When utilizing a shared 1Gb cross-connect, the MENI can also be configured to offer network connectivity to the trading platforms, market data systems, test systems, and disaster recovery facilities of the Exchange’s affiliates, MIAX, MIAX Pearl and MIAX Emerald. When utilizing a Dedicated cross-connect, the MENI can only be configured to offer network connectivity to the trading platforms, market data systems, and test systems of MIAX Sapphire. See the Definitions section of the Fee Schedule.

⁸ The term “MIAX” means Miami International Securities Exchange, LLC. See Exchange Rule 100. The term “MIAX Pearl” means MIAX PEARL, LLC. All references to “MIAX Pearl” in this filing are to the options trading facility of MIAX PEARL, LLC. References to “MIAX Pearl Equities” are to the equities trading facility of MIAX PEARL, LLC. See MIAX Pearl Rule 1901. The term “MIAX Emerald” means MIAX Emerald, LLC. See Exchange Rule 100. MIAX, MIAX Pearl and MIAX Emerald are collectively referred to herein as the “affiliated markets.”

⁹ The network switches are the first layer of access to the trading platform that firms connect to before being able to access the Exchange’s matching engines, each of which pertain to a certain list of underlying symbols. The Exchange notes that it is possible to reach each matching engine from a single switch.

two 10Gb ULL connections on each switch to the primary/secondary facility will be discounted by 50% for the three full calendar months thereafter. Any subsequent 10Gb ULL connections on each switch will be charged the full monthly rate of \$13,500 per 10Gb ULL connection.

For clarity, the Exchange provides the below examples regarding connectivity fees, utilizing the launch date of August 12, 2024:

- Members and non-Members that subscribe to the 1Gb connection to the primary/secondary facility and/or disaster recovery facility, and/or subscribe to the 10Gb ULL connection to the disaster recovery facility, will not be charged the proposed rates (*i.e.*, \$1,400 for 1Gb connections to the primary/secondary facility, \$550 for 1Gb connections to the disaster recovery facility, or \$2,750 for 10Gb ULL connections to the disaster recovery facility) for the remaining days in August, as well as for the entire period covering the months of September 2024 through November 2024. Thereafter, Members and non-Members will receive a 50% discount for each 1Gb connection to the primary/secondary facility and disaster recovery facility, and for each 10Gb ULL connection to the disaster recovery facility for entire period covering December 2024 through February 2025.

- Members and non-Members that subscribe to the 10Gb ULL connection to the primary/secondary facility will not be charged the proposed rate (\$13,500) for the first two 10Gb ULL connections on each switch to the primary/secondary facility for the remaining days in August, as well as the entire period cover the months of September through November 2024. Thereafter, Members and non-Members will receive a 50% discount for the first two 10Gb ULL connections on each switch to the primary/secondary facility for entire period covering December 2024 through February 2025. For each 10Gb ULL connection on each switch greater than two (*i.e.*, three or more), Members and non-Members will be assessed the entire amount of the proposed rate beginning upon the launch of the Exchange.

The Exchange previously communicated to market participants that the Exchange intends to waive the monthly Member and non-Member network connectivity fees in the manner described above.¹⁰ Even though the

¹⁰ See Fee Change Alert, MIAX Sapphire Options Exchange—Updated Summary of Proposed Non-Transaction Fees to Clarify Application of

Exchange proposes to waive the Member and non-Member network connectivity fees for the periods of time described above, the Exchange believes that it is appropriate to provide market participants with the overall structure of the fees by outlining the structure and amounts in the Fee Schedule, so that there is general awareness that the Exchange intends to assess such fees in the future. The Exchange notes that its affiliated markets, MIAX, MIAX Pearl and MIAX Emerald, provide for the same structure and amounts, absent the waiver and discount periods described above, for connectivity fees assessed to their Members and non-Members.¹¹

Port Fees

The Exchange proposes to establish Section 5(d), Port Fees, which will provide the fee structure and amounts for the different types of ports offered by the Exchange, which are described below.¹² MIAX Sapphire has primary and secondary data centers and a disaster recovery center. Each port provides access to all Exchange data centers for a single fee. The Exchange notes that, unless otherwise specifically set forth in the Fee Schedule, the port fees include the information communicated through the port. That is, unless otherwise specifically set forth in the Fee Schedule, there is no additional charge for the information that is communicated through the port apart from what the user is assessed for each port.

Waiver Period. The Exchange proposes to waive all port fees during the Initial Waiver Period.¹³ Even though the Exchange proposes to fully waive all port fees during the Initial Waiver Period upon launching operations, the Exchange believes that is appropriate to provide market participants with the overall structure of the fees by outlining the structure and amounts in the Fee Schedule, so that there is general awareness that the Exchange intends to

assess such fees upon the expiration of the defined period of the Initial Waiver Period.

FIX Port Fees¹⁴

The Exchange proposes to establish Section 5(d)i), FIX Port Fees, pursuant to which the Exchange will assess FIX Port fees to Members in each month the Member is credentialed to use a FIX Port in the production environment and based upon the number of credentialed FIX Ports. In particular, the Exchange proposes to assess Members the following monthly FIX Port fees: (i) \$275 for the 1st FIX Port; (ii) \$175 per port for the 2nd through 5th FIX Ports; and (iii) \$75 per port for the 6th FIX Port and each additional FIX Port. FIX Port fees will be waived during the Initial Waiver Period.

MEO Port Fees¹⁵

The Exchange proposes to establish Section 5(d)ii), MEO Port Fees, pursuant to which the Exchange will assess MEO Port fees based upon the different types of MEO Ports offered by the Exchange. MIAX Sapphire offers different types of MEO Ports depending on the services required by Members.

The Exchange proposes to assess monthly Full Service MEO Port¹⁶ fees to Market Makers¹⁷ based upon the number of classes or class volume accessed by the Market Maker. MIAX Sapphire will assess monthly Full Service MEO Port fees to Market Makers in each month the Market Maker has been credentialed to use the Full Service MEO Port in the production environment and has registered to quote in at least one class.

Specifically, the Exchange proposes to establish the following monthly Full Service MEO Port fees: (i) \$2,500 for Market Maker registrations in up to 10 option classes or up to 20% of option classes by volume; (ii) \$3,750 for Market

Maker registrations in up to 40 option classes or up to 35% of option classes by volume; (iii) \$5,000 for Market Maker registrations in up to 100 option classes or up to 50% of option classes by volume; and (iv) \$6,000 for Market Maker registrations in over 100 option classes or over 50% of option classes by volume up to all option classes listed on MIAX Sapphire.

The Exchange also proposes to adopt footnote "b." for its Full Service MEO Port fees that will apply to the Market Makers who fall within the following Full Service MEO Port fee levels, which represent the 3rd and 4th levels of the fee table: Market Makers who have (i) registrations in up to 100 option classes or up to 50% of option classes by volume, and (ii) registrations in over 100 option classes or over 50% of option classes by volume up to all option classes listed on MIAX Sapphire. The Exchange proposes that for these monthly Full Service MEO Port tier levels, if the Market Maker's total monthly executed volume during the relevant month is less than 0.015% of the total monthly executed volume reported by OCC in the Market Maker account type for MIAX Sapphire-listed option classes for that month, then the fee will be \$4,000 instead of the fee otherwise applicable to such level (*i.e.*, \$5,000 or \$6,000).

The purpose of this proposed lower monthly Full Service MEO Port fee is to provide a lower fixed cost to those Market Makers who quote the entire Exchange market (or substantial amount of the Exchange market), as objectively measured by either number of classes assigned or national average daily volume ("ADV"), but who do not otherwise execute a significant amount of volume on the Exchange. The Exchange believes that, by offering lower fixed costs to Market Makers that execute less volume, the Exchange will retain and attract smaller-scale Market Makers, which are an integral component of the option industry marketplace, but have been decreasing in number in recent years, due to industry consolidation and lower market maker profitability. Since these smaller-scale Market Makers utilize less Exchange capacity due to lower overall volume executed, the Exchange believes it is reasonable and appropriate to offer such Market Makers a lower fixed cost. The Exchange notes that its affiliated markets, MIAX, MIAX Pearl, and MIAX Emerald, offer a similar reduced fee for their full service MEO/MEI ports for

Production Connectivity Waiver Period, dated July 26, 2024, available at <https://www.miaxglobal.com/alert/2024/07/26/miax-sapphire-options-exchange-updated-summary-proposed-non-transaction>.

¹¹ See MIAX Fee Schedule, Sections 5(a)–(b); MIAX Pearl Fee Schedule, Sections 5(a)–(b); and MIAX Emerald Fee Schedule, Sections 5(a)–(b).

¹² The Exchange notes that this filing includes proposed fees for FIX Ports, Full Service MEO Ports, Limited Service MEO Ports, Clearing Trade Drop Ports, and FIX Drop Copy Ports. The Exchange separately filed to establish fees for Purge Ports. See SR-SAPPHIRE-2024-26. The Exhibit 5 reflects the separate filing to establish fees for Purge Ports.

¹³ The term "Initial Waiver Period" means, for each applicable fee, the period of time from the initial effective date of the MIAX Sapphire Fee Schedule plus an additional six (6) full calendar months after the completion of the partial month of the Exchange launch. See the Definitions Section of the Fee Schedule.

¹⁴ The term "FIX Interface" means the Financial Information Exchange interface used for submitting certain order types (as set forth in Rule 516) to the MIAX Sapphire System. See Exchange Rule 100. The term "FIX Port" means a FIX port that allows Members to send orders and other messages using the FIX protocol. See the Definitions section of the Fee Schedule.

¹⁵ The term "MEO Interface" or "MEO" means a binary order interface for certain order types as set forth in Rule 516 into the MIAX Sapphire System. See Exchange Rule 100 and the Definitions section of the Fee Schedule.

¹⁶ The term "Full Service MEO Port" means an MEO port that supports all MEO input message types and binary bulk order entry. See the Definitions section of the Fee Schedule.

¹⁷ The term "Market Maker" or "MM" means a Member registered with the Exchange for the purpose of making markets in options contracts traded on the Exchange and that is vested with the rights and responsibilities specified in Chapter VI of the Exchange's Rules. See Exchange Rule 100.

smaller-scale Market Makers.¹⁸ Accordingly, this concept is not novel.

For the calculation of the monthly Full Service MEO Port fees, the applicable fee rate is the lesser of either the per class basis or percentage of total national ADV measurement. The amount of the monthly Full Service MEO Port fee will be based upon the number of classes in which the Market Maker was registered to quote on any given day within the calendar month, or upon the class volume percentages set forth in the table in Section 5(d)ii) of the Fee Schedule. A Market Maker is determined to be registered in a class if that Market Maker has been registered in one or more series in that class.¹⁹ The Exchange will assess MIAx Sapphire Market Makers the monthly Full Service MEO Port fee based on the greatest number of classes listed on MIAx Sapphire that the MIAx Sapphire Market Maker registered to quote in on any given day within a calendar month. The class volume percentage is based on the total national average daily volume in classes listed on MIAx Sapphire in the prior calendar quarter. Newly listed option classes are excluded from the calculation of the monthly Full Service MEO Port fee until the calendar quarter following their listing, at which time the newly listed option classes will be included in both the per class count and the percentage of total national average daily volume.

MEO Port users will be allocated two (2) Full Service MEO Ports and four (4) Limited Service MEO Ports per Matching Engine²⁰ to which they connect. MEO Port fees include MEO Ports at the primary, secondary and disaster recovery data centers. Market Makers may request additional Limited Service MEO Ports for which MIAx Sapphire proposes to assess Market Makers \$250 per month per additional Limited Service MEO Port for each Matching Engine in excess of the four

(4) Limited Service MEO Ports described above.

Full Service MEO Port fees and Limited Service MEO Port fees will be waived during the Initial Waiver Period.

Clearing Trade Drop Port Fees²¹

The Exchange proposes to establish Section 5(d)iv), Clearing Trade Drop Port Fees. The Exchange proposes to assess a CTD Port fee of \$450 per month. This fixed fee structure and amount is the same as the CTD Port fee in place at the Exchange's affiliate, MIAx Emerald.²² CTD Port fees will be waived during the Initial Waiver Period.

FIX Drop Copy Port Fees²³

The Exchange proposes to establish Section 5(d)v), Fix Drop Copy Port Fees. The Exchange proposes to assess an FXD Port fee of \$250 per month. This fixed fee structure is the same as the FXD Port fee structure in place at the Exchange's affiliate, MIAx Emerald, and is half the price of the FXD Port fee for MIAx Emerald.²⁴ FXD Port fees will be waived during the Initial Waiver Period.

* * * * *

As described more fully below, the Exchange provides a cost analysis to support its proposed connectivity and port fees that includes, among other things, descriptions of how the Exchange allocated costs among it and its affiliated markets (MIAx, MIAx Pearl, and MIAx Emerald) to ensure no cost was allocated more than once, as

²¹ A "CTD Port" or "Clearing Trade Drop Port" provides an Exchange Member with a real-time clearing trade updates. The updates include the Member's clearing trade messages on a low latency, real-time basis. The trade messages are routed to a Member's connection containing certain information. The information includes, among other things, the following: (i) trade date and time; (ii) symbol information; (iii) trade price/size information; (iv) Member type (for example, and without limitation, Market Maker, Electronic Exchange Member, Broker-Dealer); and (v) Exchange MPID for each side of the transaction, including Clearing Member MPID. See the Definitions section of the Fee Schedule. The term "Electronic Exchange Member" or "EEM" means the holder of a Trading Permit who is a Member representing as agent Public Customer Orders or Non-Customer Orders on the Exchange and those non-Market Maker Members conducting proprietary trading. Electronic Exchange Members are deemed "members" under the Exchange Act. See Exchange Rule 100.

²² See MIAx Emerald Fee Schedule, Section 5(d)iii).

²³ The term "FXD" or "FIX Drop Copy Port" means a messaging interface that provides a copy of real-time trade execution, trade correction and trade cancellation information to FIX Drop Copy Port users who subscribe to the service. FXD Port users are those users who are designated by an EEM to receive the information and the information is restricted for use by the EEM only. See the Definitions section of the Fee Schedule.

²⁴ See MIAx Emerald Fee Schedule, Section 5(d)iv).

well as additional detail supporting its cost allocation processes. The Exchange proposes connectivity and port fees that are intended to cover the Exchange's cost of providing connectivity and ports, with a reasonable mark-up over those costs.

2. Statutory Basis

The Exchange believes that the proposed fees are consistent with Section 6(b) of the Act²⁵ in general, and furthers the objectives of Section 6(b)(4) of the Act²⁶ in particular, in that it provides for the equitable allocation of reasonable dues, fees and other charges among Members and other persons using any facility or system which the Exchange operates or controls. The Exchange also believes the proposed fees further the objectives of Section 6(b)(5) of the Act²⁷ in that they are designed to promote just and equitable principles of trade, remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general protect investors and the public interest and are not designed to permit unfair discrimination between customers, issuers, brokers and dealers.

Cost Analysis

In general, the Exchange believes that exchanges, in setting fees of all types, should meet very high standards of transparency to demonstrate why each new fee or fee increase meets the Exchange Act requirements that fees be reasonable, equitably allocated, not unfairly discriminatory, and not create an undue burden on competition among members and markets. In particular, the Exchange believes that each exchange should take extra care to be able to demonstrate that these fees are based on its costs and reasonable business needs.

In proposing to charge fees for connectivity and port services, the Exchange is especially diligent in assessing those fees in a transparent way against its own aggregate costs of providing the related service, and in carefully and transparently assessing the impact on Members—both generally and in relation to other Members, *i.e.*, to assure the fee will not create a financial burden on any participant and will not have an undue impact in particular on smaller Members and competition among Members in general. The Exchange believes that this level of diligence and transparency is called for by the requirements of Section 19(b)(1)

²⁵ 15 U.S.C. 78f(b).

²⁶ 15 U.S.C. 78f(b)(4).

²⁷ 15 U.S.C. 78f(b)(5).

¹⁸ See MIAx Fee Schedule, Section 5(d)ii), note "***"; MIAx Pearl Fee Schedule, Section 5(d), page 20, note "***"; and MIAx Emerald Fee Schedule, Section 5(d)ii), note ■.

¹⁹ See, generally, Chapter VI of the Exchange's Rules.

²⁰ A "Matching Engine" is a part of the MIAx Sapphire electronic system that processes options orders and trades on a symbol-by-symbol basis. Some Matching Engines will process option classes with multiple root symbols, and other Matching Engines may be dedicated to one single option root symbol (for example, options on SPY may be processed by one single Matching Engine that is dedicated only to SPY). A particular root symbol may only be assigned to a single designated Matching Engine. A particular root symbol may not be assigned to multiple Matching Engines. See the Definitions section of the Fee Schedule.

under the Act,²⁸ and Rule 19b–4 thereunder,²⁹ with respect to the types of information exchanges should provide when filing fee changes, and Section 6(b) of the Act,³⁰ which requires, among other things, that exchange fees be reasonable and equitably allocated,³¹ not designed to permit unfair discrimination,³² and that they not impose a burden on competition not necessary or appropriate in furtherance of the purposes of the Act.³³ This rule change proposal addresses those requirements, and the analysis and data in each of the sections that follow are designed to clearly and comprehensively show how they are met.³⁴

As detailed below, the Exchange recently calculated its aggregate annual costs (and approximations for monthly costs) for providing 1Gb and 10Gb ULL connectivity, Full Service MEO Ports, Limited Service MEO Ports, FIX Ports, CTD Ports, and FXD Ports. For physical 1Gb and 10Gb ULL connectivity combined, the Exchange calculated its aggregate annual cost to equal \$6,620,300 (or approximately \$551,692 per month, when rounded to the nearest dollar when dividing the combined annual cost by 12 months). For the various port services, the Exchange calculated the following annual costs: \$605,907 for Full Service MEO Ports (or approximately \$50,491 per month, when rounded to the nearest dollar when dividing the combined annual cost by 12 months); \$600,608 for Limited Service MEO Ports (or approximately \$50,050 per month, when rounded to the nearest dollar when dividing the combined annual cost by 12 months); \$158,148 for FIX Ports (or approximately \$13,178 per month, when rounded to the nearest dollar when dividing the combined annual cost by 12 months); \$109,908 for CTD Ports (or approximately \$9,158 per month, when rounded to the nearest dollar when dividing the combined annual cost by 12 months); and \$36,637 for FXD Ports (or approximately \$3,054 per month, when rounded to the nearest dollar when dividing the combined annual cost by 12 months). In order to cover the aggregate costs of providing connectivity and ports to its users (both Members and non-Members³⁵) going

forward and to make a modest profit for connectivity services, as described below, the Exchange proposes to modify its Fee Schedule to establish the connectivity and port fees described above, subject to certain fee waiver periods. The Exchange does not anticipate that it will make an overall profit on the various port services following the expiration of the Initial Waiver Period, on an annual basis, based on projected subscriber data.

The Exchange's affiliates previously completed a study of their aggregate costs to provide connectivity and port services and produce market data, defined above as its Cost Analysis.³⁶ Personnel began to plan for and develop the Exchange beginning in early 2023, and costs included in this Cost Analysis are related to the development and buildout of the Exchange since that time. During the Exchange's development and buildout that occurred throughout 2023 and continues to today, the Exchange routinely studied its aggregate costs to provide connectivity and port services, which were used to determine the proposed pricing for the provisions of connectivity and port services that are part of the Exchange's Cost Analysis. The Cost Analysis required a detailed analysis of the Exchange's aggregate baseline costs, including a determination and allocation of costs for core services provided by the Exchange—transaction execution, market data, membership services, physical connectivity, and port access (which provide order entry, cancellation and modification functionality, risk functionality, the ability to receive drop copies, and other functionality). The Exchange separately divided its costs between those costs necessary to deliver each of these core services, including infrastructure, software, human resources (*i.e.*, personnel), and certain general and administrative expenses ("cost drivers").

As an initial step, the Exchange determined the total cost for the

Exchange and the affiliated markets for each cost driver as part of its 2024 budget review process. The 2024 budget review is a company-wide process that occurs over the course of many months, includes meetings among senior management, department heads, and the Finance Team. Each department head is required to send a "bottom up" budget to the Finance Team allocating costs at the profit and loss account and vendor levels for the Exchange and its affiliated markets based on a number of factors, including server counts, additional hardware and software utilization, current or anticipated functional or non-functional development projects, capacity needs, end-of-life or end-of-service intervals, number of members, market model (*e.g.*, price time or pro-rata, simple only or simple and complex markets, auction functionality, etc.), which may impact message traffic, individual system architectures that impact platform size,³⁷ storage needs, dedicated infrastructure versus shared infrastructure allocated per platform based on the resources required to support each platform, number of available connections, and employees allocated time. For the 2024 budget process for MIAX Sapphire, only costs and anticipated revenues associated with the electronic exchange were considered. While MIAX Sapphire plans on opening its trading floor in 2025 costs and anticipated revenues from the trading floor were not included as part of any analysis for MIAX Sapphire for 2024.³⁸ All of these factors result in different allocation percentages among the Exchange and its affiliated markets, *i.e.*, the different percentages of the overall cost driver allocated to the Exchange and its affiliated markets will cause the dollar amount of the overall cost allocated among the Exchange and its affiliated markets to also differ. Because the Exchange's parent company currently owns and operates four separate and distinct marketplaces, the Exchange must determine the costs associated with each actual market—as opposed to the Exchange's parent company simply concluding that all costs drivers are the same at each individual marketplace and dividing total cost by five (5) (evenly for each marketplace). Rather, the Exchange's

Service bureaus offer technology-based services to other companies for a fee, including order entry services, and thus, may access ports on behalf of one or more Members. Extranets offer physical connectivity services to Members and non-Members.

³⁶ See Securities Exchange Act Release Nos. 100041 (April 26, 2024), 89 FR 35868 (May 2, 2024) (SR-MIAX–2024–25); 100319 (June 12, 2024), 89 FR 51562 (June 18, 2024) (SR-PEARL–2024–25); 100042 (April 26, 2024), 89 FR 35879 (May 2, 2024) (SR-EMERALD–2024–15). The Exchange frequently updates its Cost Analysis as strategic initiatives change, costs increase or decrease, and market participant needs and trading activity (once live trading begins) changes. The Exchange's most recent Cost Analysis was conducted ahead of this filing.

³⁷ For example, MIAX Sapphire maintains 8 matching engines, MIAX Emerald maintains 12 matching engines, MIAX Pearl Options maintains 12 matching engines, MIAX Pearl Equities maintains 24 matching engines, and MIAX maintains 24 matching engines.

³⁸ Additionally, while MIAX Sapphire received approval as a national securities exchange on July 15, 2024, start-up costs associated with the launch of MIAX Sapphire were not included in the costs used for the 2024 electronic exchange projections.

²⁸ 15 U.S.C. 78s(b)(1).

²⁹ 17 CFR 240.19b–4.

³⁰ 15 U.S.C. 78f(b).

³¹ 15 U.S.C. 78f(b)(4).

³² 15 U.S.C. 78f(b)(5).

³³ 15 U.S.C. 78f(b)(8).

³⁴ See *supra* note 31.

³⁵ Types of market participants that obtain connectivity services from the Exchange but are not Members include service bureaus and extranets.

parent company determines an accurate cost for each marketplace, which results in different allocations and amounts across exchanges for the same cost drivers, due to the unique factors of each marketplace as described above. This allocation methodology also ensures that no cost would be allocated twice or double-counted between the Exchange and its affiliated markets. The Finance Team then consolidates the budget and sends it to senior management, including the Chief Financial Officer and Chief Executive Officer, for review and approval. Next, the budget is presented to the Board of Directors and the Finance and Audit Committees for each exchange for their approval. The above steps encompass the first step of the cost allocation process.

The next step involves determining what portion of the cost allocated to the Exchange pursuant to the above methodology is to be allocated to each core service, *e.g.*, connectivity and ports, market data, and transaction services. The Exchange and its affiliated markets adopted an allocation methodology with thoughtful and consistently applied principles to guide how much of a particular cost amount allocated to the Exchange should be allocated within the Exchange to each core service. This is the final step in the cost allocation process and is applied to each of the cost drivers set forth below. For instance, fixed costs that are not driven by client activity (*e.g.*, message rates), such as data center costs, were allocated more heavily to the provision of 10Gb ULL physical connectivity (57.7% of total expense amount allocated to 10Gb ULL connectivity), with smaller allocations to Full Service MEO Ports (1.6%) and Limited Service MEO Ports (1.6%), and the remainder to the provision of other connectivity, other ports, transaction execution, membership services and market data services (39.1%). This next level of the allocation methodology at the individual exchange level also took into account factors similar to those set forth under the first step of the allocation methodology process described above, to determine the appropriate allocation to connectivity or market data versus

allocations for other services. This allocation methodology was developed through an assessment of costs with senior management intimately familiar with each area of the Exchange's operations. After adopting this allocation methodology, the Exchange then applied an allocation of each cost driver to each core service, resulting in the cost allocations described below. Each of the below cost allocations is unique to the Exchange and represents a percentage of overall cost that was allocated to the Exchange pursuant to the initial allocation described above.

By allocating segmented costs to each core service, the Exchange was able to estimate by core service the potential margin it might earn based on different fee models. The Exchange notes that as a non-listing venue it has five primary sources of revenue that it can potentially use to fund its operations: transaction fees, fees for connectivity and port services, membership fees, regulatory fees, and market data fees. Accordingly, the Exchange must cover its expenses from these five primary sources of revenue. The Exchange also notes that as a general matter each of these sources of revenue is based on services that are interdependent. For instance, the Exchange's system for executing transactions is dependent on physical hardware and connectivity; only Members and parties that they sponsor to participate directly on the Exchange may submit orders to the Exchange; many Members (but not all) consume market data from the Exchange in order to trade on the Exchange; and the Exchange consumes market data from external sources in order to comply with regulatory obligations. Accordingly, given this interdependence, the allocation of costs to each service or revenue source required judgment of the Exchange and was weighted based on estimates of the Exchange that the Exchange believes are reasonable, as set forth below. While there is no standardized and generally accepted methodology for the allocation of an exchange's costs, the Exchange's methodology is the result of an extensive review and analysis and will be consistently applied going forward for any other potential fee proposals. In

the absence of the Commission attempting to specify a methodology for the allocation of exchanges' interdependent costs, the Exchange will continue to be left with its best efforts to attempt to conduct such an allocation in a thoughtful and reasonable manner.

Through the Exchange's extensive updated Cost Analysis, which was again recently further refined, the Exchange analyzed every expense item in the Exchange's general expense ledger to determine whether each such expense relates to the provision of connectivity and port services, and, if such expense did so relate, what portion (or percentage) of such expense actually supports the provision of connectivity and port services, and thus bears a relationship that is, "in nature and closeness," directly related to network connectivity and port services. In turn, the Exchange allocated certain costs more to physical connectivity and others to ports, while certain costs were only allocated to such services at a very low percentage or not at all, using consistent allocation methodologies as described above. Based on this analysis, the Exchange estimates that the aggregate monthly costs for connectivity and ports are as follows: \$532,820 for 10Gb ULL connectivity; \$18,872 for 1Gb connectivity; \$50,491 for Full Service MEO Ports; \$50,050 for Limited Service MEO Ports; \$13,178 for FIX Ports; \$9,158 for CTD Ports; and \$3,054 for FXD Ports (all calculations utilized the number rounded to the nearest dollar when dividing the annual cost for each type of connectivity or port by 12 months), as further detailed below.

Costs Related to Offering Physical 1Gb and 10Gb ULL Connectivity

The following charts detail the individual line-item costs considered by the Exchange to be related to offering physical dedicated 1Gb and 10Gb ULL connectivity as well as the percentage of the Exchange's overall costs that such costs represent for each cost driver (*e.g.*, as set forth below, the Exchange allocated approximately 1.2% of its overall Human Resources cost to offering 1Gb connectivity and 34.5% to offering 10Gb ULL physical connectivity).

1Gb CONNECTIVITY

Cost drivers	Allocated annual cost ^a	Allocated monthly cost ^b	Percent of all
Human Resources	\$125,167	\$10,431	1.2
Connectivity (external fees, cabling, switches, etc.)	522	44	2.0
Internet Services and External Market Data	3,675	306	2.5
Data Center	12,571	1,048	2.0
Hardware and Software Maintenance and Licenses	9,826	819	2.0

1Gb CONNECTIVITY—Continued

Cost drivers	Allocated annual cost ^a	Allocated monthly cost ^b	Percent of all
Depreciation	27,679	2,307	2.3
Allocated Shared Expenses	47,021	3,918	1.7
Total	226,461	18,872	1.5

^a The Annual Cost includes figures rounded to the nearest dollar.

^b The Monthly Cost was determined by dividing the Annual Cost for each line item by twelve (12) months and rounding up or down to the nearest dollar.

10Gb ULL CONNECTIVITY

Cost drivers	Allocated annual cost ^a	Allocated monthly cost ^b	Percent of all
Human Resources	\$3,533,950	\$294,496	34.5
Connectivity (external fees, cabling, switches, etc.)	14,741	1,228	57.7
Internet Services and External Market Data	103,750	8,646	69.8
Data Center	354,917	29,576	57.7
Hardware and Software Maintenance and Licenses	277,415	23,118	55.9
Depreciation	781,473	65,123	63.6
Allocated Shared Expenses	1,327,593	110,633	47
Total	6,393,839	532,820	41.1

^a The Annual Cost includes figures rounded to the nearest dollar.

^b The Monthly Cost was determined by dividing the Annual Cost for each line item by twelve (12) months and rounding up or down to the nearest dollar.

Below are additional details regarding each of the line-item costs considered by the Exchange to be related to offering physical 1Gb and 10Gb ULL connectivity.

Human Resources

The Exchange notes that it and its affiliated markets anticipate that by year-end 2024, there will be 289 employees (excluding employees at non-options/equities exchange subsidiaries of Miami International Holdings, Inc. (“MIH”), the holding company of the Exchange and its affiliated markets), and each department leader has direct knowledge of the time spent by each employee with respect to the various tasks necessary to operate the Exchange. Specifically, twice a year, and as needed with additional new hires and new project initiatives, in consultation with employees as needed, managers and department heads assign a percentage of time to every employee and then allocate that time amongst the Exchange and its affiliated markets to determine each market’s individual Human Resources expense. Then, managers and department heads assign a percentage of each employee’s time allocated to the Exchange into buckets including network connectivity, ports, market data, and other exchange services. This process ensures that every employee is 100% allocated, ensuring there is no double counting between the Exchange and its affiliated markets.

For personnel costs (Human Resources), the Exchange calculated an allocation of employee time for employees whose functions include providing and maintaining physical connectivity and performance thereof (primarily the Exchange’s network infrastructure team, which spends most of their time performing functions necessary to provide physical connectivity). As described more fully above, the Exchange’s parent company allocates costs to the Exchange and its affiliated markets and then a portion of the Human Resources costs allocated to the Exchange is then allocated to connectivity. From that portion allocated to the Exchange that applied to connectivity, the Exchange then allocated weighted averages of 49.1% for 10Gb ULL connectivity and 1.7% for 1Gb connectivity of each employee’s time from the above group.

The Exchange also allocated Human Resources costs to provide physical connectivity to a limited subset of personnel with ancillary functions related to establishing and maintaining such connectivity (such as information security, sales, membership, and finance personnel). The Exchange allocated cost on an employee-by-employee basis (*i.e.*, only including those personnel who support functions related to providing physical connectivity) and then applied a smaller allocation to such employees’ time to 10Gb ULL connectivity (18.4%) and a smaller allocation to 1Gb

connectivity (0.6%). This other group of personnel with a smaller allocation of Human Resources costs also have a direct nexus to 10Gb ULL connectivity, whether it is a sales person selling a connection, finance personnel billing for connectivity or providing budget analysis, or information security ensuring that such connectivity is secure and adequately defended from an outside intrusion.

The estimates of Human Resources cost were therefore determined by consulting with such department leaders, determining which employees are involved in tasks related to providing physical connectivity, and confirming that the proposed allocations were reasonable based on an understanding of the percentage of time such employees devote to those tasks. This includes personnel from the Exchange departments that are predominately involved in providing 1Gb and 10Gb ULL connectivity: Business Systems Development, Trading Systems Development, Systems Operations and Network Monitoring, Network and Data Center Operations, Listings, Trading Operations, and Project Management. Again, the Exchange allocated 49.1% for 10Gb ULL connectivity and 1.7% for 1Gb connectivity of each of their employee’s time assigned to the Exchange for 10Gb ULL and 1Gb connectivity, as stated above. Employees from these departments perform numerous

functions to support 10Gb ULL connectivity, such as the installation, re-location, configuration, and maintenance of 10Gb ULL connections and the hardware they access. This hardware includes servers, routers, switches, firewalls, and monitoring devices. These employees also perform software upgrades, vulnerability assessments, remediation and patch installs, equipment configuration and hardening, as well as performance and capacity management. These employees also engage in research and development analysis for equipment and software supporting 10Gb ULL connectivity and design, and support the development and on-going maintenance of internally-developed applications as well as data capture and analysis, and Member and internal Exchange reports related to network and system performance. The above list of employee functions is not exhaustive of all the functions performed by Exchange employees to support 10Gb ULL and 1Gb connectivity, but illustrates the breadth of functions those employees perform in support of the above cost and time allocations.

Lastly, the Exchange notes that senior level executives' time was only allocated to the 10Gb ULL and 1Gb connectivity related Human Resources costs to the extent that they are involved in overseeing tasks related to providing physical connectivity. The Human Resources cost was calculated using a blended rate of compensation reflecting salary, equity and bonus compensation, benefits, payroll taxes, and 401(k) matching contributions.

Connectivity (External Fees, Cabling, Switches, etc.)

The Connectivity cost driver includes external fees paid to connect to other exchanges and third parties, cabling and switches required to operate the Exchange. The Connectivity cost driver is more narrowly focused on technology used to complete connections to the Exchange and to connect to external markets. The Exchange notes that its connectivity to external markets is required in order to receive market data to run the Exchange's matching engine and basic operations compliant with existing regulations, primarily Regulation NMS.

The Exchange relies on various connectivity providers for connectivity to the entire U.S. options industry, and infrastructure services for critical components of the network that are necessary to provide and maintain its System Networks and access to its System Networks via 1Gb and 10Gb ULL connectivity. Specifically, the

Exchange utilizes connectivity providers to connect to other national securities exchanges and the Options Price Reporting Authority ("OPRA"). The Exchange understands that these service providers provide services to most, if not all, of the other U.S. exchanges and other market participants. Connectivity provided by these service providers is critical to the Exchanges daily operations and performance of its System Networks to which market participants connect to via 1Gb and 10Gb ULL connectivity. Without these services providers, the Exchange would not be able to connect to other national securities exchanges, market data providers or OPRA and, therefore, would not be able to operate and support its System Networks. The Exchange does not employ a separate fee to cover its connectivity provider expense and recoups that expense, in part, by charging for 1Gb and 10Gb ULL connectivity.

Internet Services and External Market Data

The next cost driver consists of internet Services and external market data. Internet services includes third-party service providers that provide the internet, fiber and bandwidth connections between the Exchange's networks, primary and secondary data centers, and office locations in Princeton, New Jersey and Miami, Florida.

External market data includes fees paid to third parties, including other exchanges, to receive market data. The Exchange includes external market data fee costs towards the provisions of physical connectivity because such market data is necessary for certain services related to connectivity, including pre-trade risk checks and checks for other conditions (e.g., repricing of orders to avoid locked or crossed markets and trading collars). Since external market data from other exchanges is consumed at the Exchange's matching engine level, (to which physical connectivity provides access) in order to validate orders before additional orders enter the matching engine or are executed, the Exchange believes it is reasonable to allocate an amount of such costs to 1Gb and 10Gb ULL connectivity.

The Exchange relies on various content service providers for data feeds for the entire U.S. options industry, as well as content for critical components of the network that are necessary to provide and maintain its System Networks and access to its System Networks via 1Gb and 10Gb ULL connectivity. Specifically, the Exchange

utilizes content service providers to receive market data from OPRA, other exchanges and market data providers. The Exchange understands that these service providers provide services to most, if not all, of the other U.S. exchanges and other market participants. Market data provided by these service providers is critical to the Exchanges daily operations and performance of its System Networks to which market participants connect to via 1Gb and 10Gb ULL connectivity. Without these services providers, the Exchange would not be able to receive market data and, therefore, would not be able to operate and support its System Networks. The Exchange does not employ a separate fee to cover its content service provider expense and recoups that expense, in part, by charging for 1Gb and 10Gb ULL connectivity.

Data Center

Data Center costs includes an allocation of the costs the Exchange incurs to provide physical connectivity in the third-party data centers where it maintains its equipment (such as dedicated space, security services, cooling and power). The Exchange notes that it does not own the primary data center or the secondary data center, but instead, leases space in data centers operated by third parties. The Exchange has allocated a high percentage of the total Data Center cost to physical 1Gb and 10Gb ULL connectivity (59.7% combined) because the third-party data centers and the Exchange's physical equipment contained therein is the most direct cost in providing physical access to the Exchange. In other words, for the Exchange to operate in a dedicated space with connectivity by market participants to a physical trading platform, the data centers are a very tangible cost, and in turn, if the Exchange did not maintain such a presence then physical connectivity would be of no value to market participants.

Hardware and Software Maintenance and Licenses

Hardware and Software Licenses includes hardware and software licenses used to operate and monitor physical assets necessary to offer physical connectivity to the Exchange. This software is necessary for the Exchange to operate its options trading platform in order to maintain premium network performance. This hardware includes servers, network switches, cables, optics, protocol data units, and cabinets, to maintain a state-of-the-art technology platform. Accordingly, the Exchange

allocated a high percentage of the total Hardware and Software Maintenance and License cost to physical 1Gb and 10Gb ULL connectivity (57.9% combined) because the hardware and software licenses are the most direct cost in providing physical access to the Exchange's platform.

Depreciation

All physical assets, software, and hardware used to provide 1Gb and 10Gb ULL connectivity, which also includes assets used for testing and monitoring of Exchange infrastructure, were valued at cost, and depreciated or leased over periods ranging from three to five years. Thus, the depreciation cost primarily relates to servers necessary to operate the Exchange, some of which are owned by the Exchange and some of which are leased by the Exchange in order to allow efficient periodic technology refreshes. The Exchange also included in the Depreciation cost driver certain budgeted improvements that the Exchange intends to capitalize and depreciate with respect to 1Gb and 10Gb ULL connectivity in the near-term. As with the other allocated costs in the Exchange's updated Cost Analysis, the Depreciation cost was therefore narrowly tailored to depreciation related to 1Gb and 10Gb ULL connectivity. As noted above, the Exchange allocated 63.6% of its allocated depreciation costs to providing physical 10Gb ULL connectivity and 2.3% of all depreciation costs to providing 1Gb connectivity.

Allocated Shared Expenses

Finally, as with other exchange products and services, a portion of general shared expenses was allocated to overall physical connectivity costs. These general shared costs are integral to exchange operations, including its ability to provide physical connectivity. Costs included in general shared expenses include office space and office expenses (e.g., occupancy and overhead expenses), utilities, recruiting and training, marketing and advertising costs, professional fees for legal, tax and accounting services (including external and internal audit expenses), and telecommunications. Similarly, the cost of paying directors to serve on the Exchange's Board of Directors is also included in the Exchange's general shared expense cost driver.³⁹ These

general shared expenses are incurred by the Exchange's parent company, MIH, as a direct result of operating the Exchange and its affiliated markets.

The Exchange employed a process to determine a reasonable percentage to allocate general shared expenses to 1Gb and 10Gb ULL connectivity pursuant to its multi-layered allocation process. First, general expenses were allocated among the Exchange and affiliated markets as described above. Then, the general shared expense assigned to the Exchange was allocated across core services of the Exchange, including connectivity. Then, these costs were further allocated to sub-categories within the final categories, i.e., 1Gb and 10Gb ULL connectivity as sub-categories of connectivity. In determining the percentage of general shared expenses allocated to connectivity that ultimately apply to 1Gb and 10Gb ULL connectivity, the Exchange looked at the percentage allocations of each of the cost drivers and determined a reasonable allocation percentage. The Exchange also held meetings with senior management, department heads, and the Finance Team to determine the proper amount of the shared general expense to allocate to 1Gb and 10Gb ULL connectivity. The Exchange, therefore, believes it is reasonable to assign allocations, in the range of allocations for other cost drivers, while continuing to ensure that these expenses are only allocated once. Again, the general shared expenses are incurred by the Exchange's parent company as a result of operating the Exchange and its affiliated markets and it is therefore reasonable to allocate a percentage of those expenses to the Exchange and ultimately to specific product offerings such as 1Gb and 10Gb ULL connectivity.

Again, a portion of all shared expenses were allocated to the Exchange (and its affiliated markets) which, in turn, allocated a portion of that overall allocation to all physical connectivity on the Exchange. The Exchange then allocated 47% of the portion allocated to physical connectivity to 10Gb ULL connectivity and 1.7% of the portion allocated to physical connectivity to 1Gb connectivity. The Exchange believes these allocation percentages are reasonable because, while the overall dollar amounts may be higher than other cost drivers, the percentages are based on and in line with the percentage allocations of each of the Exchange's other cost drivers for each provision of connectivity. The percentage allocated

Instead, director costs are included as part of the overall general allocation.

to 10Gb ULL connectivity also reflects its importance to the Exchange's strategy and necessity towards the nature of the Exchange's overall operations, which is to provide a resilient, highly deterministic trading system that relies on faster 10Gb ULL connectivity than the Exchange's competitors to maintain premium performance. This allocation reflects the Exchange's focus on providing and maintaining high performance network connectivity, of which 10Gb ULL connectivity is a main contributor. The Exchange intends to differentiate itself by offering a "premium-product" network experience, as an operator of a high performance, ultra-low latency network with unparalleled system throughput, which system networks can support access to four distinct options markets and multiple competing market makers having affirmative obligations to continuously quote over 1,100,000 distinct trading products (per exchange), and the capacity to handle approximately 8 million quote messages per second. The "premium-product" network experience enables users of 10Gb ULL connections to receive the network monitoring and reporting services for those approximately 1,100,000 distinct trading products. These value add services are part of the Exchange's strategy for offering a high performance trading system, which utilizes 10Gb ULL connectivity.

The Exchange notes that the 47% allocation of general shared expenses for physical 10Gb ULL connectivity is higher than that allocated to general shared expenses for all other types of connectivity and ports. This is based on its allocation methodology that weighted costs attributable to each core service. While physical connectivity has several areas where certain tangible costs are heavily weighted towards providing such service (e.g., Data Center, as described above), other types of connectivity and ports do not require as many broad or indirect resources as other core services.

* * * * *

Approximate Cost per 1Gb and 10Gb ULL Connection per Month

The Exchange divided the total monthly cost for 10Gb ULL connectivity of \$532,820 by the number of physical 10Gb ULL connections the Exchange anticipates maintaining upon expiration of the full length of the waiver period for 10Gb ULL connections at the time the proposed pricing was determined (40), to arrive at a cost of approximately \$13,321 per month (rounded to the

³⁹ The Exchange notes that MEMX allocated a precise amount of 10% of the overall cost for directors to providing physical connectivity. See Securities Exchange Act Release No. 95936 (September 27, 2022), 87 FR 59845 (October 3, 2022) (SR-MEMX-2022-26). The Exchange does not calculate its expenses at that granular a level.

nearest dollar), per physical 10Gb ULL connection.

Similarly, the Exchange divided the total monthly cost for 1Gb connectivity of \$18,872 by the number of physical 1Gb connections the Exchange anticipates maintaining upon expiration of the waiver period at the time the proposed pricing was determined (12), to arrive at a cost of approximately

\$1,573 per month (rounded to the nearest dollar), per physical 1Gb connection.

* * * * *

Costs Related to Offering Full Service MEO Ports

The following chart details the individual line-item costs considered by

the Exchange to be related to offering Full Service MEO Ports as well as the percentage of the Exchange's overall costs such costs represent for such area (e.g., as set forth below, the Exchange allocated approximately 5.1% of its overall Human Resources cost to offering Full Service MEO Ports).

FULL SERVICE MEO PORTS

Cost drivers	Allocated annual cost ^a	Allocated monthly cost ^b	Percent of all
Human Resources	\$517,369	\$43,114	5.1
Connectivity (external fees, cabling, switches, etc.)	160	13	0.6
Internet Services and External Market Data	929	77	0.6
Data Center	9,615	801	1.6
Hardware and Software Maintenance and Licenses	3,106	259	0.6
Depreciation	27,745	2,312	2.3
Allocated Shared Expenses	46,983	3,915	1.7
Total	605,907	50,491	3.9

^a The Annual Cost includes figures rounded to the nearest dollar.

^b The Monthly Cost was determined by dividing the Annual Cost for each line item by twelve (12) months and rounding up or down to the nearest dollar.

Below are additional details regarding each of the line-item costs considered by the Exchange to be related to offering Full Service MEO Ports.

Human Resources

With respect to Full Service MEO Ports, the Exchange calculated Human Resources cost by taking an allocation of employee time for employees whose functions include providing Full Service MEO Ports and maintaining performance thereof (including a broader range of employees such as technical operations personnel, market operations personnel, and software engineering personnel) as well as a limited subset of personnel with ancillary functions related to maintaining such connectivity (such as sales, membership, and finance personnel). Just as described above for connectivity, the estimates of Human Resources cost were again determined by consulting with department leaders, determining which employees are involved in tasks related to providing Full Service MEO Ports and maintaining performance thereof, and confirming that the proposed allocations were reasonable based on an understanding of the percentage of their time such employees devote to tasks related to providing Full Service MEO Ports and maintaining performance thereof. This includes personnel from the following Exchange departments that are predominately involved in providing Full Service MEO Ports: Business Systems Development, Trading Systems

Development, Systems Operations and Network Monitoring, Network and Data Center Operations, Listings, Trading Operations, and Project Management. The Exchange notes that senior level executives were allocated Human Resources costs to the extent they are involved in overseeing tasks specifically related to providing Full Service MEO Ports. Senior level executives were only allocated Human Resources costs to the extent that they are involved in managing personnel responsible for tasks integral to providing Full Service MEO Ports. The Human Resources cost was again calculated using a blended rate of compensation reflecting salary, equity and bonus compensation, benefits, payroll taxes, and 401(k) matching contributions.

Connectivity (External Fees, Cabling, Switches, etc.)

The Connectivity cost driver includes external fees paid to connect to other exchanges and cabling and switches, as described above.

Internet Services and External Market Data

The next cost driver consists of internet services and external market data. Internet services includes third-party service providers that provide the internet, fiber and bandwidth connections between the Exchange's networks, primary and secondary data centers, and office locations in Princeton and Miami. For purposes of Full Service MEO Ports, the Exchange

also includes a portion of its costs related to external market data. External market data includes fees paid to third parties, including other exchanges, to receive and consume market data from other markets. The Exchange includes external market data costs towards the provision of Full Service MEO Ports because such market data is necessary (in addition to physical connectivity) to offer certain services related to such ports, such as validating orders on entry against the NBBO and checking for other conditions (e.g., halted securities).⁴⁰ Thus, since market data from other exchanges is consumed at the Exchange's Full Service MEO Port level in order to validate orders, before additional processing occurs with respect to such orders, the Exchange believes it is reasonable to allocate a small amount of such costs to Full Service MEO Ports.

Data Center

Data Center costs includes an allocation of the costs the Exchange incurs to provide Full Service MEO Ports in the third-party data centers where it maintains its equipment as well as related costs for market data to then enter the Exchange's system via Full Service MEO Ports (the Exchange does not own the primary data center or

⁴⁰ The Exchange notes that MEMX separately allocated 7.5% of its external market data costs to providing physical connectivity. See Securities Exchange Act Release No. 95936 (September 27, 2022), 87 FR 59845 (October 3, 2022) (SR-MEMX-2022-26).

secondary data center, but instead leases space in data centers operated by third parties).

Hardware and Software Maintenance and Licenses

Hardware and Software Licenses includes hardware and software licenses used to monitor the health of the order entry services provided by the Exchange, as described above.

Depreciation

The vast majority of the software the Exchange uses to provide Full Service MEO Ports has been developed in-house and the cost of such development, which takes place over an extended period of time and includes not just development work, but also quality assurance and testing to ensure the software works as intended, is depreciated over time once the software is activated in the production environment. Hardware used to provide Full Service MEO Ports includes equipment used for testing and monitoring of order entry infrastructure and other physical equipment the Exchange purchased and is also depreciated over time.

All hardware and software, which also includes assets used for testing and monitoring of order entry infrastructure, were valued at cost, depreciated or leased over periods ranging from three to five years. Thus, the depreciation cost primarily relates to servers necessary to operate the Exchange, some of which is owned by the Exchange and some of which is leased by the Exchange in order to allow efficient periodic technology refreshes. The Exchange allocated 2.3% of all depreciation costs

to providing Full Service MEO Ports. The Exchange allocated depreciation costs for depreciated software necessary to operate the Exchange to Full Service MEO Ports because such software is related to the provision of Full Service MEO Ports. As with the other allocated costs in the Exchange's updated Cost Analysis, the Depreciation cost driver was therefore narrowly tailored to depreciation related to Full Service MEO Ports.

Allocated Shared Expenses

Finally, a portion of general shared expenses was allocated to overall Full Service MEO Port costs as without these general shared costs the Exchange would not be able to operate in the manner that it does and provide application sessions. The costs included in general shared expenses include general expenses of the Exchange, including office space and office expenses (e.g., occupancy and overhead expenses), utilities, recruiting and training, marketing and advertising costs, professional fees for legal, tax and accounting services (including external and internal audit expenses), and telecommunications costs. The Exchange again notes that the cost of paying directors to serve on its Board of Directors is included in the calculation of Allocated Shared Expenses, and thus a portion of such overall cost amounting to less than 4% of the overall cost for directors was allocated to providing Full Service MEO Ports. The Exchange notes that the 1.7% allocation of general shared expenses for Full Service MEO Ports is lower than that allocated to general shared expenses for physical

connectivity based on its allocation methodology that weighted costs attributable to each Core Service based on an understanding of each area. While Full Service MEO Ports have several areas where certain tangible costs are heavily weighted towards providing such service (e.g., data centers, as described above), 10Gb ULL connectivity requires a broader level of support from Exchange personnel in different areas, which in turn leads to a broader general level of cost to the Exchange.

* * * * *

Approximate Cost per Full Service MEO Port per Month

The Exchange divided the total monthly cost for Full Service MEO Ports of \$50,491 by the number of Full Service MEO Ports the Exchange anticipates maintaining upon expiration of the Initial Waiver Period at the time the proposed pricing was determined (112), to arrive at a cost of approximately \$451 per month (rounded to the nearest dollar), per Full Service MEO Port.

* * * * *

Costs Related to Offering Limited Service MEO Ports

The following chart details the individual line-item costs considered by the Exchange to be related to offering Limited Service MEO Ports as well as the percentage of the Exchange's overall costs such costs represent for such area (e.g., as set forth below, the Exchange allocated approximately 5% of its overall Human Resources cost to offering Limited Service MEO Ports).

LIMITED SERVICE MEO PORTS

Cost drivers	Allocated annual cost ^a	Allocated monthly cost ^b	Percent of all
Human Resources	\$512,844	\$42,737	5
Connectivity (external fees, cabling, switches, etc.)	158	13	0.6
Internet Services and External Market Data	921	77	0.6
Data Center	9,531	794	1.6
Hardware and Software Maintenance and Licenses	3,079	256	0.6
Depreciation	27,503	2,292	2.2
Allocated Shared Expenses	46,572	3,881	1.7
Total	600,608	50,050	3.9

^a The Annual Cost includes figures rounded to the nearest dollar.

^b The Monthly Cost was determined by dividing the Annual Cost for each line item by twelve (12) months and rounding up or down to the nearest dollar.

Below are additional details regarding each of the line-item costs considered by the Exchange to be related to offering Limited Service MEO Ports.

Human Resources

With respect to Limited Service MEO Ports, the Exchange calculated Human Resources cost by taking an allocation of employee time for employees whose functions include providing Limited

Service MEO Ports and maintaining performance thereof (including a broader range of employees such as technical operations personnel, market operations personnel, and software engineering personnel) as well as a

limited subset of personnel with ancillary functions related to maintaining such connectivity (such as sales, membership, and finance personnel). Just as described above for connectivity, the estimates of Human Resources cost were again determined by consulting with department leaders, determining which employees are involved in tasks related to providing Limited Service MEO Ports and maintaining performance thereof, and confirming that the proposed allocations were reasonable based on an understanding of the percentage of their time such employees devote to tasks related to providing Limited Service MEO Ports and maintaining performance thereof. This includes personnel from the following Exchange departments that are predominately involved in providing Limited Service MEO Ports: Business Systems Development, Trading Systems Development, Systems Operations and Network Monitoring, Network and Data Center Operations, Listings, Trading Operations, and Project Management. The Exchange notes that senior level executives were allocated Human Resources costs to the extent they are involved in overseeing tasks specifically related to providing Limited Service MEO Ports. Senior level executives were only allocated Human Resources costs to the extent that they are involved in managing personnel responsible for tasks integral to providing and maintaining Limited Service MEO Ports. The Human Resources cost was again calculated using a blended rate of compensation reflecting salary, equity and bonus compensation, benefits, payroll taxes, and 401(k) matching contributions.

Connectivity (External Fees, Cabling, Switches, etc.)

The Connectivity cost includes external fees paid to connect to other exchanges and cabling and switches, as described above.

Internet Services and External Market Data

The next cost driver consists of internet services and external market data. Internet services includes third-party service providers that provide the internet, fiber and bandwidth connections between the Exchange's networks, primary and secondary data centers, and office locations in Princeton and Miami. For purposes of Limited Service MEO Ports, the Exchange also includes a portion of its costs related to external market data. External market data includes fees paid to third parties, including other

exchanges, to receive and consume market data from other markets. The Exchange includes external market data costs towards the provision of Limited Service MEO Ports because such market data is necessary (in addition to physical connectivity) to offer certain services related to such ports, such as validating orders on entry against the NBBO and checking for other conditions (e.g., halted securities).⁴¹ Thus, since market data from other exchanges is consumed at the Exchange's Limited Service MEO Port level in order to validate orders, before additional processing occurs with respect to such orders, the Exchange believes it is reasonable to allocate a small amount of such costs to Limited Service MEO.

Data Center

Data Center costs includes an allocation of the costs the Exchange incurs to provide Limited Service MEO Ports in the third-party data centers where it maintains its equipment as well as related costs for market data to then enter the Exchange's System via Limited Service MEO Ports (the Exchange does not own the primary data center or the secondary data center, but instead leases space in data centers operated by third parties).

Hardware and Software Maintenance and Licenses

Hardware and Software Licenses includes hardware and software licenses used to monitor the health of the order entry services provided by the Exchange, as described above.

Depreciation

The vast majority of the software the Exchange uses to provide Limited Service MEO Ports has been developed in-house and the cost of such development, which takes place over an extended period of time and includes not just development work, but also quality assurance and testing to ensure the software works as intended, is depreciated over time once the software is activated in the production environment. Hardware used to provide Limited Service MEO Ports includes equipment used for testing and monitoring of order entry infrastructure and other physical equipment the Exchange purchased and is also depreciated over time.

All hardware and software, which also includes assets used for testing and

monitoring of order entry infrastructure, were valued at cost, depreciated or leased over periods ranging from three to five years. Thus, the depreciation cost primarily relates to servers necessary to operate the Exchange, some of which is owned by the Exchange and some of which is leased by the Exchange in order to allow efficient periodic technology refreshes. The Exchange allocated 2.2% of all depreciation costs to providing Limited Service MEO Ports. The Exchange allocated depreciation costs for depreciated software necessary to operate the Exchange because such software is related to the provision of Limited Service MEO Ports. As with the other allocated costs in the Exchange's updated Cost Analysis, the Depreciation cost driver was therefore narrowly tailored to depreciation related to Limited Service MEO Ports.

Allocated Shared Expenses

Finally, a portion of general shared expenses was allocated to overall Limited Service MEO Port costs as without these general shared costs the Exchange would not be able to operate in the manner that it does and provide Limited Service MEO Ports. The costs included in general shared expenses include general expenses of the Exchange, including office space and office expenses (e.g., occupancy and overhead expenses), utilities, recruiting and training, marketing and advertising costs, professional fees for legal, tax and accounting services (including external and internal audit expenses), and telecommunications costs. The Exchange again notes that the cost of paying directors to serve on its Board of Directors is included in the calculation of Allocated Shared Expenses, and thus a portion of such overall cost amounting to less than 4% of the overall cost for directors was allocated to providing Limited Service MEO Ports. The Exchange notes that the 1.7% allocation of general shared expenses for Limited Service MEO Ports is lower than that allocated to general shared expenses for physical connectivity based on its allocation methodology that weighted costs attributable to each Core Service based on an understanding of each area. While Limited Service MEO Ports have several areas where certain tangible costs are heavily weighted towards providing such service (e.g., data center, as described above), Limited Service MEO Ports require a broader level of support from Exchange personnel in different areas, which in turn leads to a

⁴¹ The Exchange notes that MEMX separately allocated 7.5% of its external market data costs to providing physical connectivity. See Securities Exchange Act Release No. 95936 (September 27, 2022), 87 FR 59845 (October 3, 2022) (SR-MEMX-2022-26).

broader general level of cost to the Exchange.

* * * * *

Approximate Cost per Limited Service MEO Port per Month

The Exchange divided the total monthly cost for Limited Service MEO Ports of \$50,050 by the number of Limited Service MEO Ports the Exchange anticipates maintaining upon expiration of the Initial Waiver Period at the time the proposed pricing was

determined (208, for charged ports, without the cap on the number of Limited Service MEO Ports), to arrive at a cost of approximately \$241 per month (rounded to the nearest dollar), per Limited Service MEO Port.

* * * * *

Costs Related to Offering FIX, CTD and FXD Ports

The following charts detail the individual line-item costs considered by the Exchange to be related to offering

FIX, CTD and FXD Ports as well as the percentage of the Exchange's overall costs such costs represent for such area (e.g., as set forth below, the Exchange allocated approximately 1.3%, 0.9%, and 0.3% of its overall Human Resources cost to offering FIX Ports, CTD Ports, and FXD Ports, respectively).

FIX PORTS

Cost drivers	Allocated annual cost ^a	Allocated monthly cost ^b	Percent of all
Human Resources	\$135,037	\$11,253	1.3
Connectivity (external fees, cabling, switches, etc.)	42	4	0.2
Internet Services and External Market Data	243	20	0.2
Data Center	2,510	209	0.4
Hardware and Software Maintenance and Licenses	811	66	0.2
Depreciation	7,242	604	0.6
Allocated Shared Expenses	12,263	1,022	0.4
Total	158,148	13,178	1

^a The Annual Cost includes figures rounded to the nearest dollar.

^b The Monthly Cost was determined by dividing the Annual Cost for each line item by twelve (12) months and rounding up or down to the nearest dollar.

CTD PORTS

Cost drivers	Allocated annual cost ^a	Allocated monthly cost ^b	Percent of all
Human Resources	\$93,848	\$7,821	0.9
Connectivity (external fees, cabling, switches, etc.)	29	2	0.1
Internet Services and External Market Data	169	14	0.1
Data Center	1,744	145	0.3
Hardware and Software Maintenance and Licenses	563	47	0.1
Depreciation	5,033	419	0.4
Allocated Shared Expenses	8,522	710	0.3
Total	109,908	9,158	0.7

^a The Annual Cost includes figures rounded to the nearest dollar.

^b The Monthly Cost was determined by dividing the Annual Cost for each line item by twelve (12) months and rounding up or down to the nearest dollar.

FXD PORTS

Cost drivers	Allocated annual cost ^a	Allocated monthly cost ^b	Percent of all
Human Resources	\$31,283	\$2,607	0.3
Connectivity (external fees, cabling, switches, etc.)	10	1	0.04
Internet Services and External Market Data	56	5	0.04
Data Center	581	48	0.1
Hardware and Software Maintenance and Licenses	188	16	0.04
Depreciation	1,678	140	0.1
Allocated Shared Expenses	2,841	237	0.1
Total	36,637	3,054	0.2

^a The Annual Cost includes figures rounded to the nearest dollar.

^b The Monthly Cost was determined by dividing the Annual Cost for each line item by twelve (12) months and rounding up or down to the nearest dollar.

Below are additional details regarding each of the line-item costs considered by the Exchange to be related to offering FIX, CTD and FXD Ports.

Human Resources

With respect to FIX, CTD and FXD Ports, the Exchange calculated Human Resources cost by taking an allocation of employee time for employees whose functions include providing FIX, CTD and FXD Ports and maintaining performance thereof (including a broader range of employees such as technical operations personnel, market operations personnel, and software engineering personnel) as well as a limited subset of personnel with ancillary functions related to maintaining such connectivity (such as sales, membership, and finance personnel). Just as described above for connectivity, the estimates of Human Resources cost were again determined by consulting with department leaders, determining which employees are involved in tasks related to providing FIX, CTD and FXD Ports and maintaining performance thereof, and confirming that the proposed allocations were reasonable based on an understanding of the percentage of their time such employees devote to tasks related to providing FIX, CTD and FXD Ports and maintaining performance thereof. This includes personnel from the following Exchange departments that are predominately involved in providing FIX, CTD and FXD Ports: Business Systems Development, Trading Systems Development, Systems Operations and Network Monitoring, Network and Data Center Operations, Listings, Trading Operations, and Project Management. The Exchange notes that senior level executives were allocated Human Resources costs to the extent they are involved in overseeing tasks specifically related to providing FIX, CTD and FXD Ports. Senior level executives were only allocated Human Resources costs to the extent that they are involved in managing personnel responsible for tasks integral to providing and maintaining FIX, CTD and FXD Ports. The Human Resources cost was again calculated using a blended rate of compensation reflecting salary, equity and bonus compensation, benefits, payroll taxes, and 401(k) matching contributions.

Lastly, the Exchange notes that the Human Resource allocations for Full Service MEO Ports and Limited Service MEO Ports are greater than the Human Resource allocations for FIX, CTD and FXD Ports. For its Human Resource cost driver, the Exchange allocated 5.1% to Full Service MEO Ports, 5% to Limited

Service MEO Ports, 1.3% to FIX Ports, 0.9% to CTD Ports, and 0.3% to FXD Ports. This is because the MEO interface is a customized binary interface that the Exchange developed in-house and maintains on its own. The FIX interface is the industry standard for simple order entry which requires less development, maintenance, and support than the MEO interface. Likewise, the CTD and FXD interfaces only provide information concerning clearing trade updates and trade execution, respectively, which also require less development, maintenance and support than the MEO interface. The MEO interface is performance oriented and designed to meet the needs of more latency sensitive Members. Due to the in-house development of the MEO interface, the Exchange was required to expend more internal personnel to support the MEO interface than the FIX, CTD or FXD interfaces. Because of the materially higher cost associated with maintaining and supporting MEO Ports (Full Service and Limited Service) versus FIX, CTD and FXD Ports, the Exchange allocates a materially higher percentage of Human Resource expense to MEO Ports versus FIX, CTD and FXD Ports.

Connectivity (external fees, cabling, switches, etc.)

The Connectivity cost includes external fees paid to connect to other exchanges and cabling and switches, as described above.

Internet Services and External Market Data

The next cost driver consists of internet services and external market data. Internet services includes third-party service providers that provide the internet, fiber and bandwidth connections between the Exchange's networks, primary and secondary data centers, and office locations in Princeton and Miami. For purposes of FIX, CTD and FXD Ports, the Exchange also includes a portion of its costs related to external market data. External market data includes fees paid to third parties, including other exchanges, to receive and consume market data from other markets. The Exchange includes external market data costs towards the provision of FIX, CTD and FXD Ports because such market data is necessary (in addition to physical connectivity) to offer certain services related to such ports, such as validating orders on entry against the NBBO and checking for other conditions (e.g., halted securities).⁴² Thus, as market data from

other exchanges is consumed at the port level in order to validate orders before additional processing occurs with respect to such orders, the Exchange believes it is reasonable to allocate a small amount of such costs to FIX, CTD and FXD Ports.

Data Center

Data Center costs includes an allocation of the costs the Exchange incurs to provide physical connectivity in the third-party data centers where it maintains its equipment as well as related costs for market data to then enter the Exchange's System via FIX, CTD and FXD Ports (the Exchange does not own the primary data center or the secondary data center, but instead leases space in data centers operated by third parties).

Hardware and Software Maintenance and Licenses

Hardware and Software Licenses includes hardware and software licenses used to monitor the health of the order entry services provided by the Exchange, as described above.

Depreciation

The vast majority of the software the Exchange uses to provide FIX, CTD and FXD Ports has been developed in-house and the cost of such development, which takes place over an extended period of time and includes not just development work, but also quality assurance and testing to ensure the software works as intended, is depreciated over time once the software is activated in the production environment. Hardware used to provide FIX, CTD and FXD Ports includes equipment used for testing and monitoring of order entry infrastructure and other physical equipment the Exchange purchased and is also depreciated over time.

All hardware and software, which also includes assets used for testing and monitoring of order entry infrastructure, were valued at cost, depreciated or leased over periods ranging from three to five years. Thus, the depreciation cost primarily relates to servers necessary to operate the Exchange, some of which is owned by the Exchange and some of which is leased by the Exchange in order to allow efficient periodic technology refreshes. The Exchange allocated 0.6%, 0.4% and 0.1% of all depreciation costs to providing FIX, CTD and FXD Ports, respectively. The Exchange allocated depreciation costs

providing physical connectivity. See Securities Exchange Act Release No. 95936 (September 27, 2022), 87 FR 59845 (October 3, 2022) (SR-MEMX-2022-26).

⁴² The Exchange notes that MEMX separately allocated 7.5% of its external market data costs to

for depreciated software necessary to operate the Exchange because such software is related to the provision of FIX, CTD and FXD Ports. As with the other allocated costs in the Exchange's updated Cost Analysis, the Depreciation cost driver was therefore narrowly tailored to depreciation related to FIX, CTD and FXD Ports.

Lastly, the Exchange notes that the Depreciation allocations for MEO Ports (Full Service and Limited Service) are greater than the Depreciation allocations for FIX, CTD and FXD Ports. For its Depreciation cost driver, the Exchange allocated 2.3% to Full Service MEO Ports, 2.2% to Limited Service MEO Ports, 0.6% to FIX Ports, 0.4% to CTD Ports, and 0.1% to FXD Ports. As discussed above, this is because the MEO interface is a customized binary interface that the Exchange developed in-house and maintains on its own. The FIX interface is the industry standard for simple order entry which requires less development, maintenance, and support than the MEO interface. Likewise, the CTD and FXD interfaces only provide information concerning clearing trade updates and trade execution, respectively, which also require less development, maintenance and support than the MEO interface. The Exchange maintains more dedicated hardware per port for the MEO interface compared to the FIX, CTD and FXD interfaces. As a result, the MEO interface is supported by more dedicated in-house hardware and software than the FIX, CTD and FXD interfaces that is subject to depreciation. Thus, there is a greater amount of equipment supporting the MEO interface than the FIX, CTD and FXD interfaces, resulting in higher depreciation costs.

Allocated Shared Expenses

Finally, a portion of general shared expenses was allocated to overall FIX, CTD and FXD Port costs as without these general shared costs the Exchange would not be able to operate in the manner that it does and provide FIX, CTD and FXD Ports. The costs included in general shared expenses include general expenses of the Exchange, including office space and office expenses (e.g., occupancy and overhead expenses), utilities, recruiting and training, marketing and advertising costs, professional fees for legal, tax and accounting services (including external and internal audit expenses), and telecommunications costs. The Exchange again notes that the cost of paying directors to serve on its Board of Directors is included in the calculation of Allocated Shared Expenses, and thus

a portion of such overall cost amounting to less than 2% of the overall cost for directors was allocated to providing FIX, CTD and FXD Ports. The Exchange notes that the 0.4%, 0.3% and 0.1% allocations of general shared expenses for FIX, CTD and FXD Ports, respectively, are lower than that allocated to general shared expenses for physical connectivity based on its allocation methodology that weighted costs attributable to each Core Service based on an understanding of each area. While MEO Ports (Full Service and Limited Service) have several areas where certain tangible costs are heavily weighted towards providing such service (e.g., data center, as described above), FIX, CTD and FXD Ports require a broader level of support from Exchange personnel in different areas, which in turn leads to a broader general level of cost to the Exchange.

Lastly, the Exchange notes that the Allocated Shared Expense allocations for MEO Ports (Full Service and Limited Service) are greater than the same allocations for FIX, CTD and FXD Ports. For its Allocated Shared Expense cost driver, the Exchange allocated 1.7% to Full Service MEO Ports, 1.7% to Limited Service MEO Ports, 0.4% to FIX Ports, 0.3% to CTD Ports, and 0.1% to FXD Ports. As discussed above, this is because the MEO interface is a customized binary interface that the Exchange developed in-house and maintains on its own. The FIX interface is the industry standard for simple order entry which requires less development, maintenance, and support than the MEO interface. Likewise, the CTD and FXD interfaces only provide information concerning clearing trade updates and trade execution, respectively, which also require less development, maintenance and support than the MEO interface. The FIX interface is the industry standard for simple order entry which requires less development, maintenance, and support than the MEO interface. The MEO interface is performance oriented and designed to meet the needs of more latency sensitive Members. This required more internal personnel and resources to support than the FIX, CTD and FXD interfaces. Because of the materially higher cost associated with maintaining and supporting MEO Ports versus FIX, CTD and FXD Ports, the Exchange allocates a materially higher percentage of Allocated Shared expense to MEO Ports versus FIX, CTD and FXD Ports, which are less complex, standardized solutions.

Approximate Cost Per FIX, CTD and FXD Port Per Month

The Exchange divided the total monthly cost for FIX Ports of \$13,178 by the number of FIX Ports the Exchange anticipates maintaining upon expiration of the Initial Waiver Period at the time the proposed pricing was determined (25), to arrive at a cost of approximately \$527 per month (rounded to the nearest dollar), per FIX Port.

Similarly, the Exchange divided the total monthly cost for CTD Ports of \$9,158 by the number of CTD Ports the Exchange anticipates maintaining upon expiration of the Initial Waiver Period at the time the proposed pricing was determined (10), to arrive at a cost of approximately \$916 per month (rounded to the nearest dollar), per CTD Port.

Finally, the Exchange divided the total monthly cost for FXD Ports of \$3,054 by the number of FXD Ports the Exchange anticipates maintaining upon expiration of the Initial Waiver Period at the time the proposed pricing was determined (6), to arrive at a cost of approximately \$509 per month (rounded to the nearest dollar), per FXD Port.

* * * * *

Cost Analysis—Additional Discussion

In conducting its Cost Analysis, the Exchange did not allocate any of its expenses in full to any core services (including physical connectivity or ports) and did not double-count any expenses. Instead, as described above, the Exchange allocated applicable cost drivers across its core services and used the same Cost Analysis to form the basis of this proposal and the separate filings the Exchange submitted (or plans to submit) proposing fees for proprietary market data feeds offered by the Exchange, as well as for Purge Ports. For instance, in calculating the Human Resources expenses to be allocated to physical connections based upon the above described methodology, the Exchange has a team of employees dedicated to network infrastructure and with respect to such employees the Exchange allocated network infrastructure personnel with a high percentage of the cost of such personnel (49.1%) given their focus on functions necessary to provide 10Gb ULL physical connections. The salaries of those same personnel were allocated only 6.8% to Full Service MEO Ports and 6.7% to Limited Service MEO Ports and the remaining 37.4% was allocated to 1Gb connectivity, other port services, transaction services, membership services and market data. The Exchange

did not allocate any other Human Resources expense for providing physical connections to any other employee group, outside of a smaller allocation of 18.4% for 10Gb ULL connectivity or 19.7% for the entire network (*i.e.*, 18.4% for 10Gb ULL, 0.7% for Test Bed Connectivity, and 0.6% for 1Gb for a total of 19.7%), of the cost associated with certain specified personnel who work closely with and support network infrastructure personnel. In contrast, the Exchange allocated much smaller percentages of costs (3.1% for Full Service MEO Ports and 0.6% for Limited Service MEO Ports) across a wider range of personnel groups in order to allocate Human Resources costs to providing Full Service MEO Ports and Limited Service MEO Ports (0.2% for FIX Ports, 0.1% for CTD Ports, and 0.04% for FXD Ports). This is because a much wider range of personnel are involved in functions necessary to offer, monitor and maintain Full Service MEO Ports and Limited Service MEO Ports but the tasks necessary to do so are not a primary or full-time function.

In total, the Exchange allocated 35.7% of its personnel costs to providing 10Gb ULL and 1Gb ULL connectivity, 5.1% of its personnel costs to providing Full Service MEO Ports, 5% of its personnel costs to providing Limited Service MEO Ports, 1.3% of its personnel costs to providing FIX Ports, 0.9% of its personnel costs to providing CTD Ports, and 0.3% of its personnel costs to providing FXD Ports, for a total allocation of 48.3% Human Resources expense to provide these specific connectivity and port services. In turn, the Exchange allocated the remaining 51.7% of its Human Resources expense to membership services, transaction services, other port services and market data. Thus, again, the Exchange's allocations of cost across core services were based on real costs of operating the Exchange and were not double-counted across the core services or their associated revenue streams.

As another example, the Exchange allocated depreciation expense to all core services, including physical connections and ports, but in different amounts. The Exchange believes it is reasonable to allocate the identified portion of such expense because such expense includes the actual cost of the computer equipment, such as dedicated servers, computers, laptops, monitors, information security appliances and storage, and network switching infrastructure equipment, including switches and taps that were purchased to operate and support the network. Without this equipment, the Exchange

would not be able to operate the network and provide connectivity and port services to its Members and non-Members and their customers. However, the Exchange did not allocate all of the depreciation and amortization expense toward the cost of providing connectivity services, but instead allocated approximately 65.9% of the Exchange's overall depreciation and amortization expense to connectivity services (63.6% attributed to 10Gb ULL physical connections, 2.3% to 1Gb physical connections, and 5.6% attributed to Full Service MEO Ports, Limited Service MEO Ports, FIX Ports, CTD Ports, and FXD Ports, combined). The Exchange allocated the remaining depreciation and amortization expense (approximately 28.5%) toward the cost of providing transaction services, membership services, other port services, and market data.

The Exchange notes that its revenue estimates are based on projections across all potential revenue streams and will only be realized to the extent such revenue streams actually produce the revenue estimated once the waiver periods expire for each applicable proposed fee. The Exchange does not yet know whether such expectations will be realized. For instance, in order to generate the revenue expected from connectivity, the Exchange will have to be successful in retaining existing clients that wish to maintain physical connectivity and/or ports or in obtaining new clients that will purchase such services. Similarly, the Exchange will have to be successful in retaining a positive net capture on transaction fees in order to realize the anticipated revenue from transaction pricing.

The Exchange notes that personnel began to plan for and develop the Exchange beginning in early 2023, and costs included in this Cost Analysis are related to the development and buildout of the Exchange since that time. During the Exchange's development and buildout that occurred throughout 2023 and continues to today, the Exchange routinely studied its aggregate costs to provide connectivity and port services, which were used to determine the proposed pricing for the provisions of connectivity and port services that are part of the Exchange's Cost Analysis, including projections. It is possible, however, that actual costs may be higher or lower. To the extent the Exchange sees growth in use of connectivity or port services it will receive additional revenue to offset future cost increases. However, if use of connectivity or port services is static or decreases, the Exchange might not realize the revenue that it anticipates or needs in order to

cover applicable costs. Accordingly, the Exchange is committing to conduct a one-year review after implementation of these fees. The Exchange expects that it may propose to adjust fees at that time, to increase fees in the event that revenues fail to cover costs and a reasonable mark-up of such costs. Similarly, the Exchange may propose to decrease fees in the event that revenue materially exceeds our current projections. In addition, the Exchange will periodically conduct a review to inform its decision making on whether a fee change is appropriate (*e.g.*, to monitor for costs increasing/decreasing or subscribers increasing/decreasing, etc. in ways that suggest the then-current fees are becoming dislocated from the prior cost-based analysis) and would propose to increase fees in the event that revenues fail to cover its costs and a reasonable mark-up, or decrease fees in the event that revenue or the mark-up materially exceeds our current projections. In the event that the Exchange determines to propose a fee change, the results of a timely review, including an updated cost estimate, will be included in the rule filing proposing the fee change. More generally, the Exchange believes that it is appropriate for an exchange to refresh and update information about its relevant costs and revenues in seeking any future changes to fees, and the Exchange commits to do so.

Projected Revenue

The proposed fees will allow the Exchange to cover certain costs incurred by the Exchange associated with providing and maintaining necessary hardware and other network infrastructure as well as network monitoring and support services; without such hardware, infrastructure, monitoring and support the Exchange would be unable to provide the connectivity and port services. Much of the cost relates to monitoring and analysis of data and performance of the network via the subscriber's connection(s). The above costs, namely those associated with hardware, software, and human capital, enable the Exchange to measure network performance with nanosecond granularity. These same costs are also associated with time and money spent seeking to continuously improve the network performance, improving the subscriber's experience, based on monitoring and analysis activity. The Exchange routinely works to improve the performance of the network's hardware and software. The costs associated with maintaining and enhancing a state-of-the-art exchange

network is a significant expense for the Exchange, and thus the Exchange believes that it is reasonable and appropriate to help offset those costs by amending fees for connectivity services. Subscribers, particularly those of 10Gb ULL connectivity, expect the Exchange to provide this level of support to connectivity so they continue to receive the performance they expect. This differentiates the Exchange from its competitors. As detailed above, the Exchange has five primary sources of revenue that it can potentially use to fund its operations: transaction fees, fees for connectivity services, membership and regulatory fees, and market data fees. Accordingly, the Exchange must cover its expenses from these five primary sources of revenue.

All revenue projections are based upon an annual return for each of the proposed fees once the relevant waiver periods expire.

The Exchange's Cost Analysis estimates the annual cost to provide 1Gb connectivity services will equal \$226,461. Based on projected 1Gb connectivity services usage, the Exchange would generate annual revenue of approximately \$241,200. The Exchange believes this represents a modest profit of 6.1% when compared to the cost of providing 1Gb connectivity services.

The Exchange's Cost Analysis estimates the annual cost to provide 10Gb ULL connectivity services will equal \$6,393,839. Based on projected 10Gb ULL connectivity services usage, the Exchange would generate annual revenue of approximately \$6,810,000. The Exchange believes this represents a modest profit of 6.1% when compared to the cost of providing 10Gb connectivity services.

The Exchange's Cost Analysis estimates the annual cost to provide Full Service MEO Port services will equal \$605,907. Based on projected Full Service MEO Port service usage, the Exchange would generate annual revenue of approximately \$399,000. The Exchange believes this represents a loss of 51.9% when compared to the cost of providing Full Service MEO Port services.

The Exchange's Cost Analysis estimates the annual cost to provide Limited Service MEO Port services will equal \$600,608. Since launch, taking into account the proposal to remove the cap on the number of Limited Service MEO Ports available and based on projected Limited Service MEO Port service usage, the Exchange would generate annual revenue of approximately \$624,000. The Exchange believes this represents a modest profit

of 3.7% for providing Limited Service MEO Port services.

The Exchange's Cost Analysis estimates the annual cost to provide FIX Port services will equal \$158,148. Based on projected FIX Port service usage, the Exchange would generate annual revenue of approximately \$77,700. The Exchange estimates that its costs to provide FIX Port services will exceed its revenues by 103.5%.

The Exchange's Cost Analysis estimates the annual cost to provide CTD Port services will equal \$109,908. Based on projected CTD Port service usage, the Exchange would generate annual revenue of approximately \$54,000. The Exchange estimates that its costs to provide CTD Port services will exceed its revenues by 103.5%.

The Exchange's Cost Analysis estimates the annual cost to provide FXD Port services will equal \$36,637. Based on projected FXD Port service usage, the Exchange would generate annual revenue of approximately \$18,000. The Exchange estimates that its costs FXD Port services will exceed its revenues by 103.5%.

Based on the above discussion, the Exchange believes that even if the Exchange earns the above revenue or incrementally more or less, the proposed fees are fair and reasonable because they will not result in pricing that deviates from that of other exchanges or a supra-competitive profit, when comparing the total expense of the Exchange associated with providing each of the proposed connectivity and port services versus the total projected revenue of the Exchange associated with connectivity and port services. The Exchange's affiliated options markets recently filed to raise certain connectivity and port fees to the same, or similar, rates as proposed herein and those filings were not suspended by the Commission.⁴³

* * * * *

The Exchange notes that its revenue estimate is based on projections and will only be realized to the extent customer activity produces the revenue estimated. As a competitor in the hyper-

competitive exchange environment, and an exchange focused on driving competition, the Exchange does not yet know whether such projections will be realized. For instance, in order to generate the revenue expected from 10Gb ULL connectivity and Ports, the Exchange will have to be successful in retaining existing clients that wish to utilize 10Gb ULL connectivity and Ports and/or obtaining new clients that will purchase such access. To the extent the Exchange is successful in encouraging new clients to utilize 10Gb ULL connectivity and Ports, the Exchange does not believe it should be penalized for such success. To the extent the Exchange has mispriced and experiences a net loss in connectivity clients or in transaction activity, the Exchange could experience a net reduction in revenue. While the Exchange is supportive of transparency around costs and potential margins (applied across all exchanges), as well as periodic review of revenues and applicable costs (as discussed below), the Exchange does not believe that these estimates should form the sole basis of whether or not a proposed fee is reasonable or can be adopted. Instead, the Exchange believes that the information should be used solely to confirm that an Exchange is not earning—or seeking to earn—supra-competitive profits. The Exchange believes the Cost Analysis and related projections in this filing demonstrate this fact.

The Exchange is owned by a holding company that is the parent company of five exchange markets and, therefore, the Exchange and its affiliated markets must allocate shared costs across all of those markets accordingly, pursuant to the above-described allocation methodology. In contrast, the IEX, which currently operates only one exchange, and MEMX, which just started operating two exchanges, in their recent non-transaction fee filings allocate the entire amount of that same cost to a single exchange. This can result in lower profit margins for the non-transaction fees established by IEX and MEMX because the single allocated cost does not experience the efficiencies and synergies that result from sharing costs across multiple exchanges. The Exchange and its affiliated markets often share a single cost, which results in cost efficiencies that can cause a broader gap between the allocated cost amount and projected revenue, even though the fee levels being proposed are lower or competitive with competing markets (as described above). To the extent that the application of a cost-based standard

⁴³ See Securities Exchange Act Release Nos. 99822 (March 21, 2024), 89 FR 21337 (March 27, 2024) (SR-MIAX-2024-16) (raising monthly 10Gb ULL connectivity fee to \$13,500 per connection and raising fee for Limited Service MEI Ports to \$275 per month per port); 99823 (March 21, 2024), 89 FR 21312 (March 27, 2024) (SR-PEARL-2024-14) (raising monthly 10Gb ULL connectivity fee to \$13,500 per connection and establishing tiered fees for Full Service MEO Ports ranging from \$5,000 to \$12,000 per month); and 99824 (March 21, 2024), 89 FR 21379 (March 27, 2024) (SR-EMERALD-2024-12) (raising monthly 10Gb ULL connectivity fee to \$13,500 per connection and raising fee for Limited Service MEI Ports to \$420 per month per port).

results in Commission Staff making determinations as to the appropriateness of certain profit margins, the Exchange believes that Commission Staff should also consider whether the proposed fee level is comparable to, or competitive with, the same fee charged by competing exchanges and how different cost allocation methodologies (such as across multiple markets) may result in different profit margins for comparable fee levels. Further, if Commission Staff is making determinations as to appropriate profit margins in their approval of exchange fees, the Exchange believes that the Commission should be clear to all market participants as to what they have determined is an appropriate profit margin and should apply such determinations consistently and, in the case of certain legacy exchanges, retroactively, if such standards are to avoid having a discriminatory effect.

Further, as is reflected in the proposal, the Exchange continuously and aggressively works to control its costs as a matter of good business practice. A potential profit margin should not be evaluated solely on its size; that assessment should also consider cost management and whether the ultimate fee reflects the value of the services provided. For example, a profit margin on one exchange should not be deemed excessive where that exchange has been successful in controlling its costs, but not excessive on another exchange where that exchange is charging comparable fees but has a lower profit margin due to higher costs. Doing so could have the perverse effect of not incentivizing cost control where higher costs alone could be used to justify fees increases.

The Proposed Pricing Is Not Unfairly Discriminatory and Provides for the Equitable Allocation of Fees, Dues, and Other Charges

The Exchange believes that the proposed fees for connectivity and ports are reasonable, fair, equitable, and not unfairly discriminatory because they are designed to align fees with services provided and will apply equally to all subscribers.

Connectivity

The Exchange believes that the proposed fees are equitably allocated among anticipated users of the network connectivity and port alternatives, as the Exchange expects that users of 10Gb ULL connections will consume substantially more bandwidth and network resources than users of 1Gb ULL connection. It is the experience of the Exchange's affiliates that this is the

case as 10Gb ULL connection users account for more than 99% of message traffic over the network on those markets, which drives other costs that are linked to capacity utilization, as described above, while the users of the 1Gb ULL connections account for less than 1% of message traffic over the network. In the experience of the Exchange's affiliates, users of the 1Gb connections do not have the same business needs for the high-performance network as 10Gb ULL users.

The Exchange's high-performance network and supporting infrastructure (including employee support), will provide unparalleled system throughput with the network ability to support access to several distinct options markets. To achieve a consistent, premium network performance, the Exchange must build out and maintain a network that has the capacity to handle the message rate requirements of its most heavy network consumers. These billions of messages per day will consume the Exchange's resources and significantly contribute to the overall network connectivity expense for storage and network transport capabilities, just as they do for the Exchange's affiliate markets. The Exchange must then purchase additional storage capacity on an ongoing basis to ensure it has sufficient capacity to store these messages to satisfy its record keeping requirements under the Exchange Act.⁴⁴ Thus, as the number of messages an entity increases, certain other costs incurred by the Exchange that are correlated to, though not directly affected by, connection costs (e.g., storage costs, surveillance costs, service expenses) will likely also increase. Given this anticipated difference in network utilization rate, the Exchange believes that it is reasonable, equitable, and not unfairly discriminatory that the 10Gb ULL users pay for the vast majority of the shared network resources from which all market participants' will benefit.

Full Service MEO Ports

The proposed fees for Full Service MEO Ports are not unfairly discriminatory because they would apply to all Market Makers equally. The Exchange proposes a pricing structure for Full Service MEO Ports that is the same as that used by the Exchange's affiliates, MIAX, MIAX Pearl, and MIAX Emerald, except with lower pricing for

each tier.⁴⁵ In the experience of the Exchange's affiliated markets, Members that are frequently in the highest tier for Full Service MEO/MEI Ports consume the most bandwidth and resources of the network. For example, the Exchange's affiliate, MIAX Pearl, recently noted that Market Makers who reach the highest tier for Full Service MEO Ports accounted for greater than 84% of ADV on MIAX Pearl, while Market Makers that are typically in the lowest Tier for Full Service MEO Ports, accounted for less than 14% of ADV on the Exchange.⁴⁶ Further, as noted by MIAX Pearl, the remaining 1% was accounted for by Market Makers who are frequently in the middle Tier for Full Service MEO Ports.⁴⁷

To achieve a consistent, premium network performance, the Exchange must build out and maintain a network that has the capacity to handle the message rate requirements of its most heavy network consumers during anticipated peak market conditions. The need to support billions of messages per day will consume the Exchange's resources and significantly contribute to the overall network connectivity expense for storage and network transport capabilities. The Exchange may have to purchase additional storage capacity on an ongoing basis to ensure it has sufficient capacity to store these messages as part of its surveillance program and to satisfy its record keeping requirements under the Exchange Act.⁴⁸ Thus, as the number of connections a Market Maker has increases, the related pull on Exchange resources may also increase once the Exchange launches operations. The Exchange sought to design the proposed tiered-pricing structure to set the amount of the fees to relate to the number of ports a firm purchases. The more ports purchased by a Market Maker likely results in greater expenditure of Exchange resources and increased cost to the Exchange.

The Exchange further believes that the proposed fees are reasonable, equitably allocated and not unfairly discriminatory because, for the flat fee in each tier, the Exchange provides each Member two (2) Full Service MEO Ports for each matching engine to which that

⁴⁵ See MIAX Fee Schedule, Section 5(d)(ii), MIAX Pearl Fee Schedule, Section 5(d), and MIAX Emerald Fee Schedule, Section 5(d)(ii).

⁴⁶ See Securities Exchange Act Release No. 99823 (March 21, 2024), 89 FR 21312 (March 27, 2024) (SR-PEARL-2024-14).

⁴⁷ *Id.*

⁴⁸ 17 CFR 240.17a-1 (recordkeeping rule for national securities exchanges, national securities associations, registered clearing agencies and the Municipal Securities Rulemaking Board).

⁴⁴ 17 CFR 240.17a-1 (recordkeeping rule for national securities exchanges, national securities associations, registered clearing agencies and the Municipal Securities Rulemaking Board).

Member is connected. Unlike other options exchanges that provide similar port functionality and charge fees on a per port basis,⁴⁹ the Exchange offers Full Service MEO Ports as a package and provides Market Makers with the option to receive up to two Full Service MEO Ports per matching engine to which it connects. The Exchange currently has eight matching engines, which means Market Makers may receive up to sixteen Full Service MEO Ports for a single monthly fee, that can vary based on certain volume percentages or classes the Market Maker is registered in. Assuming a Market Maker connects to all eight matching engines during the month, and achieves the highest Tier for that month, with two Full Service MEO Ports per matching engine, this would result in a cost of \$375 per Full Service MEO Port (\$6,000 divided by 16).

The Exchange believes its proposal to provide a reduced Full Service MEO Port fee to Market Makers that fall within the 3rd and 4th levels of the proposed fee table is not unfairly discriminatory because this proposed lower monthly fee is designed to provide a lower fixed cost to those Market Makers who are willing to quote the entire Exchange market (or substantial amount of the Exchange market), as objectively measured by either number of classes assigned or national ADV, but who do not otherwise execute a significant amount of volume on the Exchange. The Exchange believes that, by offering lower fixed costs to Market Makers that execute less volume, the Exchange will retain and attract smaller-scale Market Makers, which are an integral component of the option industry marketplace, but have been decreasing in number in recent years, due to industry consolidation and lower market maker profitability. The Exchange believes it is beneficial to incentivize these additional Market Makers to register to make markets on the Exchange to increase liquidity as the Exchange begins operations. Increased liquidity from a diverse set of market participants helps facilitate price discovery and the interaction of orders, which benefits all market participants of the Exchange. Since these smaller-scale

Market Makers may utilize less Exchange capacity due to lower overall volume executed, the Exchange believes it is reasonable, equitably allocated and not unfairly discriminatory to offer such Market Makers a lower fixed cost. The Exchange notes that its affiliated markets, MIAX, MIAX Pearl, and MIAX Emerald, offer a similar reduced fee for their Full Service MEO/MEI Ports for smaller-scale Market Makers.⁵⁰

Limited Service MEO Ports

The proposed fees for Limited Service MEO Ports are not unfairly discriminatory because they would apply to all Market Makers equally. All Market Makers will be eligible to receive four (4) free Limited Service MEO Ports per matching engine and those that elect to purchase more would be subject to the same monthly rate upon the expiration of the Initial Waiver Period, regardless of the number of additional Limited Service MEO Ports they purchase. In the experience of the Exchange's affiliated markets, certain market participants choose to purchase additional Limited Service MEO Ports based on their own particular trading/quoting strategies and feel they need a certain number of connections to the Exchange to execute on those strategies. Other market participants may continue to choose to only utilize the free Limited Service MEO Ports to accommodate their own trading or quoting strategies, or other business models. All market participants elect to receive or purchase the amount of Limited Service MEO Ports they require based on their own business decisions and all market participants would be subject to the same fee structure and flat fee. Every market participant may receive up to four (4) free Limited Service MEO Ports and those that choose to purchase additional Limited Service MEO Ports may elect to do so based on their own business decisions and would continue to be subject to the same monthly fee.

The Exchange believes that its proposed fee for Limited Service MEO Ports is reasonable, equitable, and not unfairly discriminatory because it is designed to align fees with services provided, will apply equally to all Members that are assigned Limited Service MEO Ports (either directly or through a Service Bureau), and will minimize barriers to entry by providing all Members with four free Limited Service MEO Ports from the time the

Exchange launches operations.⁵¹ As a result of the proposed fee structure, a significant majority of Members may not be subject to any fee. In contrast, other exchanges generally charge in excess of \$450 per port without providing any free ports.⁵² Even for Members that choose to maintain more than four Limited Service MEI Ports, the Exchange believes that the cost-based fee proposed herein is low enough that it will not operate to restrain any Member's ability to maintain the number of Limited Service MEO Ports that it determines are consistent with its business objectives. Although the Exchange projects that no Members will utilize more than the four free Limited Service MEO Ports, if there is a small number of Members that do utilize more ports and are subject to the proposed fee of \$250 per port, those Members will still pay considerably less for such ports as compared to the fees that competing exchanges charge.⁵³ Further, the number of assigned Limited Service MEO Ports will continue to be based on decisions by each Member, including the ability to reduce fees by discontinuing unused Limited Service MEO Ports.

The Exchange believes that providing four free Limited Service MEO Ports is reasonable, equitable, and not unfairly discriminatory because it will enable Members to access the Exchange on this basis without having to pay for Limited Service MEO Ports, thereby encouraging

⁵¹ The following rationale to support providing a certain number of Limited Service MEI Ports for free prior to applying a fee is similar to that used by the IEX in a 2020 proposal to do the same as proposed herein. See Securities Exchange Act Release No. 86626 (August 9, 2019), 84 FR 41793 (August 15, 2019) (SR-IEX-2019-07).

⁵² See NASDAQ Pricing Schedule, Options 7, Section 3, Ports and Other Services and NASDAQ Rules, General 8: Connectivity, Section 1. Co-Location Services (similar to the Exchange's MEI Ports, SQF ports are primarily utilized by Market Makers); ISE Pricing Schedule, Options 7, Section 7, Connectivity Fees and ISE Rules, General 8: Connectivity; NYSE American Options Fee Schedule, Section V.A. Port Fees and Section V.B. Co-Location Fees; GEMX Pricing Schedule, Options 7, Section 6, Connectivity Fees and GEMX Rules, General 8: Connectivity.

⁵³ Assuming a Member selects five Limited Service MEO Ports based on their business needs that Member on MIAX Sapphire would be charged only for the fifth Limited Service MEO Port and pay only the \$250 monthly fee, as the first four Limited Service MEO Ports would be free. Meanwhile, a Member that purchases five ports on NYSE Arca Options would pay \$450 per port per month, resulting in a total charge of \$2,250 per month. On Cboe BZX Options, that same member would pay \$750 per port per month, resulting in a total charge of \$3,750 per month for five ports. See NYSE Arca Options Fees and Charges, dated March 1, 2024, available at https://www.nyse.com/publicdocs/nyse/markets/arca-options/NYSE_Arca_Options_Fee_Schedule.pdf and Cboe BZX Options Fee Schedule available at https://www.cboe.com/us/options/membership/fee_schedule/.

⁴⁹ See NASDAQ Pricing Schedule, Options 7, Section 3, Ports and Other Services and NASDAQ Rules, General 8: Connectivity, Section 1. Co-Location Services (similar to the MIAX Pearl Options' MEO Ports, SQF ports are primarily utilized by Market Makers); ISE Pricing Schedule, Options 7, Section 7, Connectivity Fees and ISE Rules, General 8: Connectivity; NYSE American Options Fee Schedule, Section V.A. Port Fees and Section V.B. Co-Location Fees; GEMX Pricing Schedule, Options 7, Section 6, Connectivity Fees and GEMX Rules, General 8: Connectivity.

⁵⁰ See MIAX Fee Schedule, Section 5)d)iii), note “*”; MIAX Pearl Fee Schedule, Section 5)d), page 20, note “***”; and MIAX Emerald Fee Schedule, Section 5)d)iii), note ■.

order flow and liquidity from a diverse set of market participants, facilitating price discovery and the interaction of orders. The Exchange believes that four Limited Service MEO Ports is an appropriate number to provide for free because it aligns with the maximum number of free Limited Service MEO/MEI Ports offered by each of the Exchange's affiliated options markets, and the Exchange believes will align with the amount of such ports that will be maintained by a substantial majority of Members once the Exchange launches operations.

Based on an initial survey of market participants that the Exchange anticipates will utilize Limited Service MEO Ports, the Exchange projects that only a few Members will be subject to any Limited Service MEO Port fees following the expiration of the Initial Waiver Period. In determining the appropriate number of Limited Service MEO Ports to provide for free, the Exchange considered several factors. First, the Exchange believes that, with respect to Limited Service MEO Port usage, Members will prefer at least two Limited Service MEO Ports, for redundancy purposes. Second, from a review of the number of Limited Service MEI Ports currently requested, the median number of ports per Member that will utilize Limited Service MEO Ports upon the launch of the Exchange is approximately eight. Thus, the Exchange believes that having four ports appears to be reasonably sufficient for the majority of Members to access the Exchange. On that basis, the Exchange chose four Limited Service MEO Ports as the maximum number of ports for which it will not charge to access the Exchange. The Exchange notes that some Members may use more Limited Service MEO Ports than other Members (and the four provided for free), which will be driven by the nature and volume of the business they conduct on the Exchange, and the choices they make in segmenting that business across different Limited Service MEO Ports. Allowing for this expansive use of Exchange capacity represents an aggregate cost that the Exchange seeks to recover through charging for ports five and higher.

The proposed fee structure is also designed to encourage Members to be efficient with their Limited Service MEO Port usage, thereby resulting in a corresponding increase in the efficiency that the Exchange would be able to realize in managing its aggregate costs for providing Limited Service MEO Ports. There is no requirement that any Member maintain a specific number of Limited Service MEO Ports and a

Member may choose to maintain as many or as few of such ports as each Member deems appropriate.

The Exchange assessed the impact of the structure and amount of the proposed fee on all Members that the Exchange anticipates will utilize Limited Service MEO Ports. The Exchange believes that the proposed fee is fair and equitably allocated across all Members. As a threshold matter, the fee will not by design apply differently to different types or sizes of Members. Nonetheless, upon launch, the Exchange will be able to assess whether there may be any differences in the amount of the projected fee that correlates to the type and/or size of different Members. This assessment will help determine whether the number of assigned Limited Service MEO Ports, and thus projected fees, correlates closely to a Member's inbound message volume to the Exchange. This is a similar assessment as that performed by the Exchange's affiliates, MIAX and MIAX Emerald, prior to changing their respective Limited Service MEI Port fees recently. Based on the experience of the Exchange's affiliates, as inbound message volume increases per Member, the number of requested and assigned Limited Service MEO Ports increases. As the Exchange has not launched operations at the time of this filing, the Exchange does not have data to show any correlation between a Member's inbound message volume and the number of Limited Service MEO Port assigned to the Member. However, based on the experience of the Exchange's affiliates, MIAX and MIAX Emerald, Members with relatively higher inbound message volume were projected to pay higher fees because they requested more Limited Service MEI Ports for those exchanges.

To achieve consistent, premium network performance, the Exchange must build and maintain a network that has the capacity to handle the message rate requirements of its heaviest network consumers during anticipated peak market conditions. The resultant need to support the anticipated amount of billions of messages per day will consume the Exchange's resources and significantly contribute to the overall network connectivity expense for storage and network transport capabilities. This need will also require the Exchange to purchase additional storage capacity on an ongoing basis to ensure it has sufficient capacity to store these messages as part of its surveillance program and to satisfy its record keeping requirements under the

Exchange Act.⁵⁴ Thus, as the number of connections per Market Maker increases, other costs incurred by the Exchange will likely also increase, e.g., storage costs, surveillance costs, service expenses.

The Exchange further believes that the proposed fees are reasonable, fair and equitable, and non-discriminatory because they will apply to all Members in the same manner and are not targeted at a specific type or category of market participant engaged in any particular trading strategy. All Members will receive four free Limited Service MEO Ports and pay the same proposed fee per Limited Service MEO Port for each additional Limited Service MEO Port. Each Limited Service MEO Port is identical, providing connectivity to the Exchange on identical terms. While the proposed fee will result in a different effective "per unit" rate for different Members after factoring in the four free Limited Service MEO Ports, the Exchange does not believe that this difference is material given the overall low proposed fee per Limited Service MEO Port. Because the first four Limited Service MEO Ports are free of charge, each entity will have a "per unit" rate of less than the proposed fee. Further, the fee is not connected to volume based tiers. All Members will be subject to the same fee schedule, regardless of the volume sent to or executed on the Exchange. The fee also does not depend on any distinctions between Members, customers, broker-dealers, or any other entity. The fee will be assessed solely based on the number of Limited Service MEO Ports an entity selects and not on any other distinction applied by the Exchange. While entities that send relatively more inbound messages to the Exchange may select more Limited Service MEO Ports, thereby resulting in higher fees, that distinction is based on decisions made by each Member and the extent and nature of the Member's business on the Exchange rather than application of the fee by the Exchange. Members can determine how many Limited Service MEO Ports they need to implement their trading strategies effectively. The Exchange proposes to offer additional Limited Service MEO Ports at a low fee to enable all Members to purchase as many Limited Service MEO Ports as their business needs dictate in order to optimize throughput and manage latency across the Exchange.

⁵⁴ 17 CFR 240.17a-1 (recordkeeping rule for national securities exchanges, national securities associations, registered clearing agencies and the Municipal Securities Rulemaking Board).

Notwithstanding that Members with the highest number of Limited Service MEO Ports will pay a greater percentage of the total projected fees than is represented by their Limited Service MEO Port usage, the Exchange does not believe that the proposed fee is unfairly discriminatory. It is not possible to fully synchronize the Exchange's objective to provide four free Limited Service MEO Ports to all Members, thereby minimizing barriers to entry and incentivizing liquidity on the Exchange, with an approach that exactly aligns the projected per Member fee with each Member's number of requested Limited Service MEO Ports. As proposed, the Exchange is providing a reasonable number of Limited Service MEO Ports to each Member without charge. Any variance between projected fees and Limited Service MEO Port usage is attributable to objective differences among Members in terms of the number of Limited Service MEO Ports they determine are appropriate based on their trading on the Exchange. Further, the Exchange believes that the low amount of the proposed fee (which in the aggregate is projected to only partially recover the Exchange's directly-related costs as described herein) mitigates any disparate impact.

Further, the fee will help to encourage Limited Service MEO Port usage in a way that aligns with the Exchange's regulatory obligations. As a national securities exchange, the Exchange is subject to Regulation Systems Compliance and Integrity ("Reg SCI").⁵⁵ Reg SCI Rule 1001(a) requires that the Exchange establish, maintain, and enforce written policies and procedures reasonably designed to ensure (among other things) that its Reg SCI systems have levels of capacity adequate to maintain the Exchange's operational capability and promote the maintenance of fair and orderly markets.⁵⁶ By encouraging Members to be efficient with their Limited Service MEO Ports usage, the proposed fee will support the Exchange's Reg SCI obligations in this regard by ensuring that unused Limited Service MEO Ports are available to be allocated based on individual Members needs and as the Exchange's overall order and trade volumes increase. Additionally, because the Exchange will continue not to charge connectivity testing and certification fees to its disaster recovery facility or where the Exchange requires testing and certification, the proposed fee structure will further support the Exchange's Reg SCI compliance by reducing the

potential impact of a disruption should the Exchange be required to switch to its disaster recovery facility and encouraging Members to engage in any necessary system testing without incurring any port fee costs.⁵⁷

Finally, the Exchange believes that the proposed fee is consistent with Section 11A of the Exchange Act in that it is designed to facilitate the economically efficient execution of securities transactions, fair competition among brokers and dealers, exchange markets and markets other than exchange markets, and the practicability of brokers executing investors' orders in the best market. Specifically, the proposed low, cost-based fee will enable a broad range of the Exchange Members to continue to connect to the Exchange, thereby facilitating the economically efficient execution of securities transactions on the Exchange, fair competition between and among such Members, and the practicability of Members that are brokers executing investors' orders on the Exchange when it is the best market.

FIX, CTD, and FXD Ports

To achieve consistent, premium network performance, the Exchange must build and maintain a network that has the capacity to handle the message rate requirements of its heaviest network consumers during anticipated peak market conditions. The resultant need to support the anticipated amount of billions of messages per day will consume the Exchange's resources and significantly contribute to the overall network connectivity expense for storage and network transport capabilities. This need will also require the Exchange to purchase additional storage capacity on an ongoing basis to ensure it has sufficient capacity to store these messages as part of its surveillance program and to satisfy its record keeping requirements under the Exchange Act.⁵⁸ Thus, as the number of connections per Market Maker increases, other costs incurred by the Exchange will likely also increase, *e.g.*, storage costs, surveillance costs, service expenses.

The Exchange further believes that the proposed fees for FIX, CTD and FXD Ports are reasonable, fair and equitable, and non-discriminatory because they

will apply to all Members in the same manner and are not targeted at a specific type or category of market participant engaged in any particular trading strategy. The fee for each type of port does not depend on any distinctions between Members, customers, broker-dealers, or any other entity. The fee will be assessed solely based on the number of FIX, CTD or FXD Ports an entity selects and not on any other distinction applied by the Exchange.

B. Self-Regulatory Organization's Statement on Burden on Competition

The Exchange does not believe that the proposed rule change will impose any burden on competition that is not necessary or appropriate in furtherance of the purposes of the Act.

Intra-Market Competition

The Exchange believes the proposed fees will not result in any burden on intra-market competition that is not necessary or appropriate in furtherance of the purposes of the Act because the proposed fees will allow the Exchange to recoup its costs with a small profit for providing 1Gb and 10Gb ULL connectivity, while recouping some of its costs for a negative margin for providing Full Service MEO Ports, Limited Service MEO Ports, FIX Ports, CTD Ports and FXD Ports, following expiration of the respective waiver periods for each fee. As described above, the Exchange anticipates operating at a loss for the majority of the above services in order to provide a low-cost alternative to attract order flow and encourage market participants to experience the high determinism and resiliency of the Exchange's trading Systems. To do so, the Exchange chooses to waive the fees for all of the connectivity and port services for a specified time period. This will likely result in the Exchange forgoing revenue it could generate from assessing any fees without a waiver period or higher fees upon expiration of the waiver periods. The Exchange could seek to charge higher fees upon launch, but that could serve to discourage participation on the Exchange. Instead, the Exchange chooses to provide a low-cost exchange alternative to the options industry, which may result in lower initial revenues.

Further, the Exchange does not believe that the proposed fees would place certain market participants at the Exchange at a relative disadvantage compared to other market participants or affect the ability of such market participants to compete. The proposed fees will apply uniformly to all market participants regardless of the number of

⁵⁵ 17 CFR 242.1000–1007.

⁵⁶ 17 CFR 242.1001(a).

⁵⁷ By comparison, some other exchanges charge less to connect to their disaster recovery facilities, but still charge an amount that could both recoup costs and potentially be a source of profits. *See, e.g.*, Nasdaq Stock Market LLC Equity 7, Section 115 (Ports and other Services).

⁵⁸ 17 CFR 240.17a–1 (recordkeeping rule for national securities exchanges, national securities associations, registered clearing agencies and the Municipal Securities Rulemaking Board).

1Gb or 10Gb ULL connections they choose to purchase. The proposed fees do not favor certain categories of market participants in a manner that would impose an undue burden on competition.

The Exchange does not believe that the proposed rule change would place certain market participants at the Exchange at a relative disadvantage compared to other market participants or affect the ability of such market participants to compete. In particular, Exchange personnel has been informally discussing potential fees for connectivity services with a diverse group of market participants that are likely to connect to the Exchange for launch (including large and small firms, firms with large connectivity service footprints and small connectivity service footprints, as well as extranets and service bureaus) for several months leading up to that time. The Exchange does not believe the proposed fees for connectivity services would negatively impact the ability of Members, non-Members (extranets or service bureaus), third-parties that purchase the Exchange's connectivity and resell it, and customers of those resellers to compete with other market participants or that they are placed at a disadvantage.

The Exchange does anticipate, however, that some market participants may reduce or discontinue use of connectivity services provided directly by the Exchange once the relevant waiver periods expire. The Exchange's affiliates have experienced similar reductions in use by their members for similar non-transaction fee increases. For example, one MIAx Pearl Options Market Maker terminated their MIAx Pearl Options membership on January 1, 2023 as a direct result of the similar proposed fee changes by MIAx Pearl Options.⁵⁹

The Exchange does not believe that the proposed fees for connectivity services place certain market participants at a relative disadvantage to other market participants because the

proposed connectivity pricing is associated with relative usage of the Exchange by each market participant and does not impose a barrier to entry to smaller participants. The Exchange believes its proposed pricing is reasonable and, when coupled with the availability of third-party providers that also offer connectivity solutions, that participation on the Exchange is affordable for all market participants, including smaller trading firms. As described above, the connectivity services purchased by market participants typically increase based on their additional message traffic and/or the complexity of their operations. The market participants that utilize more connectivity services typically utilize the most bandwidth, and those are the participants that consume the most resources from the network. Accordingly, the proposed fees for connectivity services do not favor certain categories of market participants in a manner that would impose a burden on competition; rather, the allocation of the proposed connectivity fees reflects the network resources consumed by the various size of market participants and the costs to the Exchange of providing such connectivity services.

The Exchange does not believe its proposed fees for Limited Service MEO Ports will place certain market participants at a relative disadvantage to other market participants. All market participants would be eligible to receive four (4) free Limited Service MEO Ports and those that elect to purchase more would be subject to the same flat fee regardless of the number of additional Limited Service MEO Ports they purchase. All firms purchase the amount of Limited Service MEO Ports they require based on their own business decisions and similarly situated firms are subject to the same fees.

Inter-Market Competition

The Exchange also does not believe that the proposed rule change and price increase will result in any burden on inter-market competition that is not necessary or appropriate in furtherance of the purposes of the Act. As this is a fee increase, arguably if set too high, this fee would make it easier for other exchanges to compete with the Exchange. Only if this were a substantial fee decrease could this be considered a form of predatory pricing. In contrast, the Exchange believes that, without this fee increase, we are potentially at a competitive disadvantage to certain other exchanges that have in place higher fees for similar

services. As we have noted, the Exchange believes that connectivity fees can be used to foster more competitive transaction pricing and additional infrastructure investment and there are other options markets of which market participants may connect to trade options at higher rates than the Exchange's. Accordingly, the Exchange does not believe its proposed fee changes impose any burden on competition that is not necessary or appropriate in furtherance of the purposes of the Act.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

Written comments were neither solicited nor received.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

The foregoing rule change has become effective pursuant to Section 19(b)(3)(A)(ii) of the Act,⁶⁰ and Rule 19b-4(f)(2)⁶¹ thereunder. At any time within 60 days of the filing of the proposed rule change, the Commission summarily may temporarily suspend such rule change if it appears to the Commission that such action is necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of the Act. If the Commission takes such action, the Commission shall institute proceedings to determine whether the proposed rule should be approved or disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views, and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-SAPPHIRE-2024-32 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

⁶⁰ 15 U.S.C. 78s(b)(3)(A)(ii).

⁶¹ 17 CFR 240.19b-4(f)(2).

⁵⁹ The Exchange acknowledges that IEX included in its proposal to adopt market data fees after offering market data for free an analysis of what its projected revenue would be if all of its existing customers continued to subscribe versus what its projected revenue would be if a limited number of customers subscribed due to the new fees. See Securities Exchange Act Release No. 94630 (April 7, 2022), 87 FR 21945 (April 13, 2022) (SR-IEX-2022-02). MEMX did not include a similar analysis in its recent non-transaction fee proposal. See *supra* note 41. The Exchange does not believe a similar analysis would be useful here because it is amending existing fees, not proposing to charge a new fee where existing subscribers may terminate connections because they are no longer enjoying the service at no cost.

All submissions should refer to file number SR–SAPPHIRE–2024–32. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission’s internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission’s Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR–SAPPHIRE–2024–32 and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁶²

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2024–25056 Filed 10–28–24; 8:45 am]

BILLING CODE 8011–01–P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–101412; File No. SR–OCC–2024–011]

Self-Regulatory Organizations; The Options Clearing Corporation; Notice of Designation of Longer Period for Commission Action on Proposed Rule Change, as Modified by Partial Amendment No. 1, by the Options Clearing Corporation Concerning Its Stock Loan Programs

October 23, 2024.

On August 22, 2024, The Options Clearing Corporation (“OCC”) filed with the Securities and Exchange Commission (“Commission”) the proposed rule change SR–OCC–2024–011 pursuant to Section 19(b) of the Securities Exchange Act of 1934 (“Exchange Act”) ¹ and Rule 19b–4 ² thereunder to address limitations in the structure of OCC’s Stock Loan/Hedge (“Hedge”) Program and Market Loan Program (together, the “Stock Loan Programs”) by creating the framework for a single, enhanced program designed to support current and future needs. The proposed rule change, as modified by Partial Amendment No. 1 (hereafter “Proposed Rule Change”), was published for public comment in the **Federal Register** on September 10, 2024.³ The Commission has not received comments regarding the Proposed Rule Change.

Section 19(b)(2)(i) of the Exchange Act ⁴ provides that, within 45 days of the publication of notice of the filing of a proposed rule change, the Commission shall either approve the proposed rule change, disapprove the proposed rule change, or institute proceedings to determine whether the proposed rule change should be disapproved unless the Commission extends the period within which it must act as provided in Section 19(b)(2)(ii) of the Exchange Act.⁵ Section 19(b)(2)(ii) of the Exchange Act allows the Commission to designate a longer period for review (up to 90 days from the publication of notice of the filing of a proposed rule change) if the Commission finds such longer period to be appropriate and publishes its reasons for so finding, or as to which the self-regulatory organization consents.⁶

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b–4.

³ Securities Exchange Act Release No. 100930 (Sept. 4, 2024), 89 FR 73466 (Sept. 10, 2024) (File No. SR–OCC–2024–011).

⁴ 15 U.S.C. 78s(b)(2)(i).

⁵ 15 U.S.C. 78s(b)(2)(ii).

⁶ *Id.*

The 45th day after publication of the Notice of Filing is October 25, 2024. In order to provide the Commission with sufficient time to consider the Proposed Rule Change, the Commission finds that it is appropriate to designate a longer period within which to take action on the Proposed Rule Change, and therefore is extending this 45-day time period.

Accordingly, the Commission, pursuant to Section 19(b)(2) of the Exchange Act,⁷ designates December 9, 2024, as the date by which the Commission shall either approve, disapprove, or institute proceedings to determine whether to disapprove the Proposed Rule Change.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁸

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2024–25051 Filed 10–28–24; 8:45 am]

BILLING CODE 8011–01–P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–101416; File No. SR–CboeEDGA–2024–037]

Self-Regulatory Organizations; Cboe EDGA Exchange, Inc.; Notice of Filing of a Proposed Rule Change With Respect to Amendments to the Seventh Amended and Restated Bylaws (the “CGM Bylaws”) of Its Parent Corporation, Cboe Global Markets, Inc. (“Cboe” or “Corporation”)

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (the “Act”),¹ and Rule 19b–4 thereunder,² notice is hereby given that on October 11, 2024, Cboe EDGA Exchange, Inc. (the “Exchange” or “EDGA”) filed with the Securities and Exchange Commission (“Commission”) the proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization’s Statement of the Terms of Substance of the Proposed Rule Change

Cboe EDGA Exchange, Inc. (the “Exchange” or “EDGA”) is filing with the Securities and Exchange

⁷ 15 U.S.C. 78s(b)(2).

⁸ 17 CFR 200.30–3(a)(12).

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b–4.

⁶² 17 CFR 200.30–3(a)(12).

Commission (the “Commission”) a proposed rule change with respect to amendments to the Seventh Amended and Restated Bylaws (the “CGM Bylaws”) of its parent corporation, Cboe Global Markets, Inc. (“Cboe” or “Corporation”). The text of the proposed rule change is provided in Exhibit 5.

The text of the proposed rule change is also available on the Exchange’s website (http://markets.cboe.com/us/equities/regulation/rule_filings/edga/), at the Exchange’s Office of the Secretary, and at the Commission’s Public Reference Room.

II. Self-Regulatory Organization’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the Exchange included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

A. Self-Regulatory Organization’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

At Cboe’s annual meeting held on May 16, 2024, Cboe’s stockholders considered two advisory proposals that would provide Cboe stockholders with the right to call a special meeting of the stockholders provided that a certain threshold percentage of stockholders propose to call such a meeting. The two proposals were submitted separately. One of the proposals was submitted by an individual stockholder (“Stockholder Proposal”). The other proposal was submitted by Cboe Management (“Management Proposal”). The Stockholder Proposal, which did not pass but received 45% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 10% of Cboe’s voting power to call a special meeting of the stockholders. The Management Proposal, which passed with 65% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 25% of Cboe’s voting power to call a special meeting of the stockholders.

The Nominating & Governance Committee of the CGM Board reviewed the voting results of the Stockholder

Proposal and the Management Proposal and discussed the stockholder voting standards and rights contemplated by the CGM Bylaws. Following this review, the Nominating & Governance Committee recommended to the CGM Board, and the CGM Board approved, certain changes to the CGM Bylaws to implement the Management Proposal. The CGM Board also approved amending the CGM Bylaws to improve the governance processes of Cboe, to make certain provisions more consistent with Delaware General Corporation Law (“DGCL”), and to make clarifying and cleanup changes to the CGM Bylaws. The proposed rule change amends the CGM Bylaws to implement the changes approved by the CGM Board.

Proposed Changes to Article 2—Stockholders

Current Section 2.3 (Special Meeting) of the CGM Bylaws provides that only the Chair of the Board, the Chief Executive Officer or the CGM Board may call a special meeting of the stockholders. To respond to feedback from its stockholders, as discussed above, Cboe proposes to delete portions of this provision and add language that will provide Cboe stockholders with the right to call special stockholder meetings (a “Stockholder Requested Special Meeting”) after following particular procedures.

In defining the procedural requirements, Cboe’s goals are to ensure timely notice of a meeting request and to gather sufficient information about the proposing stockholder(s) and the proposed business itself. Among other things, this information will help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to adequately assess proposed business submitted by stockholders. Additionally, Cboe notes that the proposed terms are common among public companies that have adopted a right for stockholders to call special meetings. The proposed changes to the CGM Bylaws to effect the stockholder special meeting right are set forth below.

Revisions to Section 2.3(a)

First, the proposed changes to Section 2.3(a) provide that a Stockholder Requested Special Meeting may be called: (i) at any time by the CGM Board pursuant to a resolution adopted by the affirmative vote of a majority of the total number of CGM directors then in office; or (ii) by Cboe’s Corporate Secretary following the receipt of a written request in proper form for a special meeting (a “Special Meeting Request”) by one or more stockholders. In order to call a special meeting, the stockholders must hold, in the aggregate, at least 25% of Cboe’s outstanding shares of common stock entitled to vote on matters brought before the special meeting (the “Requisite Percentage”).

The proposed changes to Section 2.3(a) also clarify that the Chair of the Board, the Chief Executive Officer or the President of Cboe may not individually call a special meeting of the stockholders. This change was made to vest authority within Cboe to call a special meeting in the Board. Without the proposed change, the Chair of the Board, Chief Executive Officer and the President could each call a special meeting of the stockholders without CGM Board approval. The proposed change to Section 2.3(a) simplifies this requirement to confirm that, within Cboe, only the CGM Board may call for a special meeting of the stockholders.

Proposed Section 2.3(b) and Section 2.3(c)

Proposed Section 2.3(b) and Section 2.3(c)

Proposed Section 2.3(b) and Section 2.3(c) set forth the procedures a stockholder must follow in order to submit a written request in proper form to call a Stockholder Requested Special Meeting. Stockholders must first submit a request to Cboe’s Corporate Secretary to define a date on which the Requisite Percentage will be determined (the “Record Date”). A stockholder must sign any request to set a Record Date and also provide a reasonably brief description of the purpose or purposes of the special meeting of the stockholders. A stockholder is also required in the request to set a Record Date to disclose certain information regarding themselves and any individuals or entities such stockholder may be associated with (a “Stockholder Associated Person(s)”), as well as such information concerning any nominees to the CGM Board (“Stockholder Nominee(s)”) if such stockholder is so proposing. The information that a stockholder must disclose regarding Stockholder Associated Persons and Stockholder Nominees is contained in Section 2.11 of the CGM Bylaws and incorporated by reference in this Section 2.3(b). The information required to be provided in the request to set a Record Date provides Cboe with notice that a stockholder is seeking to bring business before the stockholders and assists with the logistical aspects of determining which stockholders will be counted for purposes of determining whether the Requisite Percentage is met.

Proposed Section 2.3(d) and Section 2.3(e)

Proposed Section 2.3(d) and Section 2.3(e) include detailed information on the requirements for a Special Meeting Request to have been properly delivered, subject to certain carve-outs for stockholders who submit their request in response to a solicitation for public consent by the Corporation made pursuant to Section 14 of the Exchange Act. Specifically, a Special Meeting Request must:

- be delivered within 60 days following the Record Date;
- be signed by each stockholder making up the Requisite Percentage;
- contain a reasonably brief description of the purpose of the special meeting;
- include details of each stockholder holding the Requisite Percentage, including:
 - The stockholder's name;
 - The stockholder's address;
 - information concerning the stockholder submitting the Special Meeting Request and any Stockholder Associated Persons;
 - information concerning any Stockholder Nominees; and
 - documentary evidence that the shares included in the Requisite Percentage are owned by such stockholder;
- include an acknowledgment that any reduction in the number of shares owned by such stockholders as of the date of such Special Meeting Request and through the meeting date will constitute a revocation of such Special Meeting Request with respect to such reduction;
- relate to an item of business that is a proper subject for stockholder action under applicable law;
- not include an item of business that did not appear on the request to set a Record Date;
- not be delivered during the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting and ending on the date of the next annual meeting; and
- otherwise comply with applicable law.

In defining the requirements for a Special Meeting Request, Cboe's goal is to gather sufficient information about the stockholder seeking to request a special meeting and the proposed business for both itself and its stockholders and to help ensure the efficient use of corporate resources by restricting a stockholder from raising items that could reasonably be addressed at an annual meeting of the

stockholders, as in the requirement that a Special Meeting Request not be delivered in the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting. Overall, this information is designed to help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to assess the proposed business or Stockholder Nominee adequately.

Proposed Section 2.3(f)

Proposed Section 2.3(f) provides that the CGM Board may cancel a special meeting in its discretion if the percentage of stock held by the stockholders requesting a special meeting falls below the Requisite Percentage at any point after sixty (60) days from the first date on which a valid Special Meeting Request is delivered to Cboe. This provides the CGM Board with discretion to reevaluate the Special Meeting Request in the event the Special Meeting Request is revoked by stockholders holding a sufficient percentage of the stock of the Corporation.

Proposed Section 2.3(g)

Proposed Section 2.3(g) provides that within ten (10) days following the date on which the Secretary has received valid Special Meeting Requests, the CGM Board shall fix the record date and meeting date, time and location for the Stockholder Requested Special Meeting, provided that the date of any such Stockholder Requested Special Meeting shall not be more than ninety (90) days after the date on which a valid Special Meeting Request is received by Cboe. The CGM Board may submit its own proposal or proposals for consideration at any Stockholder Requested Special Meeting. Ninety (90) days allows the Corporation reasonable time to assess the items proposed in the Special Meeting Request while also not imposing a potentially burdensome delay on the stockholders.

Proposed Section 2.3(h)

Proposed Section 2.3(h) provides that multiple Special Meeting Requests may be considered together if (i) each Special Meeting Request identifies the same or substantially the same purpose or purposes of the Stockholder Requested Special Meeting and the same or substantially the same items of business proposed to be brought before the Stockholder Requested Special Meeting, and (ii) such Special Meeting Requests have been dated and delivered to the Corporate Secretary within sixty (60)

days of the delivery to the Corporate Secretary of the earliest dated Special Meeting Request relating to such item(s) of business. This proposed section helps to ensure the efficient use of corporate resources by preventing multiple stockholders from raising items that should reasonably be consolidated. The conditions under which the Corporation may combine multiple Special Meeting Requests are sufficiently limited to require that each unique item is addressed separately.

Revisions to Section 2.9

Section 2.9 of the CGM Bylaws governs proxy representation. It is proposed that language be added to clarify that any stockholder directly or indirectly soliciting proxies from other stockholders of the Corporation may use any proxy card color other than white, which shall be reserved for exclusive use by the CGM Board.

Revisions to Section 2.11

Section 2.11 of the CGM Bylaws, which are the "advance notice bylaws",³ requires stockholders to notify Cboe, during a specified period in advance of an annual meeting or special meeting called by the CGM Board, of their intention to nominate one or more persons for election to the CGM Board or to present a business proposal for consideration by the stockholders at the meeting and provide certain information regarding such request. When designing the proposed procedural requirements for stockholders to call a special meeting, as outlined above, Cboe evaluated the existing procedural requirements for stockholders to bring business before an annual meeting or to nominate director candidates at an annual meeting or special meeting. Cboe has determined that the advance notice bylaws may be enhanced to help achieve the core objectives of fulsome disclosure and accurate explanations from stockholders bringing business or potential nominees before a stockholder meeting. While advance notice bylaws are beneficial in providing a company and its stockholders with information regarding stockholders, and their Stockholder Associated Persons, seeking to bring business or potential nominees before a stockholder meeting, therefore permitting orderly meetings and

³ "Advance notice bylaws" allow stockholder(s) to bring business before an annual or special meeting of stockholders, but set forth procedural requirements to help ensure that companies and boards have sufficient information about the proposal and the proposing stockholder(s), as well as adequate time to consider the proposal, by requiring the proposing stockholder(s) to give advance notice of the intention to bring the proposal before the annual or special meeting.

election contests, and assisting the board's information gathering and disclosure functions, the Delaware Supreme Court in *Kellner v. AIM ImmunoTech Inc.*⁴ has recently provided some guidance on circumstances where such requests may be overbroad or request information not sufficiently connected to the legitimate information gathering function these provisions serve. Therefore, as further detailed below, Cboe has determined that it would be beneficial to refine certain of the provisions in the CGM Bylaws to increase the clarity of the requests for information from stockholders seeking to bring business before a meeting.

First, Section 2.11(a)(iii)(C) of the CGM Bylaws currently defines the information required to be disclosed regarding a stockholder providing notice of nominations or other business, any Stockholder Associated Person(s) and any Stockholder Nominee(s). Cboe proposes certain amendments to this section to (i) clarify the information a stockholder is required to disclose relating to arrangements between the stockholder providing notice or any Stockholder Associated Person and any other stockholder with regard to the stockholder meeting and (ii) eliminate disclosures on performance related fees to which such stockholder or Stockholder Associated Person may be entitled as a result of any increase or decrease in the stock of Cboe, and the prospectus or similar document of the stockholder providing notice or any Stockholder Associated Person. Cboe believes that, while these provisions as currently written provide valuable information to the Corporation and its stockholders in assessing the proposed business or Stockholder Nominee, these requirements should be sufficiently specific so as not to potentially dissuade stockholders from bringing business before a stockholder meeting and should otherwise comply with Delaware law. The proposed changes narrow the information required to be disclosed such that Cboe is able to help ensure the objectives of the provisions are met without burdening stockholders with potentially overbroad requests for information.

Section 2.11(a)(iii)(D) of the CGM Bylaws currently sets forth certain representations that must be made by a stockholder seeking to bring business or a Stockholder Nominee before a stockholder meeting regarding whether such stockholder is part of a group which intends to deliver or solicit

proxies from stockholders in support of such proposed business. Cboe proposes changes to update this section in order to be more consistent with the universal proxy rules provided for in Rule 14a–19 of the Exchange Act by explicitly stating that any stockholder providing notice that they intend to solicit proxies in support of a proposed nominee must do so in accordance with Rule 14a–19 of the Exchange Act. Cboe also proposes to clarify that the representation must confirm whether the stockholder intends or is part of a group which intends to engage in a solicitation (within the meaning of Rule 14a–1(1) of the Exchange Act) with respect to the nomination of any proposed nominee or proposed business to be considered at the meeting.

Section 2.11(a)(iii)(F) of the CGM Bylaws currently requires that a Stockholder Nominee furnish any information that Cboe may determine is required for Cboe to determine the qualifications of such Stockholder Nominee to serve as a director of the Corporation. Cboe proposes to add language clarifying that the information Cboe may require must be consistent with the parameters set forth in Cboe's Corporate Governance Guidelines or the CGM Board's past practice in evaluating potential director nominees.

Proposed Section 2.11(c)(ii) of the CGM Bylaws requires the stockholder providing notice to notify the Secretary of any inaccuracy or change in any information submitted pursuant to Section 2.11 within two (2) business days of becoming aware of such inaccuracy or change. Cboe proposes to modify this requirement by narrowing the scope of circumstances in which a stockholder is required to provide notice of any inaccuracy or change of information that they have previously provided to material inaccuracies or changes.

Proposed Section 2.11(c)(iii) of the CGM Bylaws provides that any stockholder or Stockholder Associated Person providing notice with respect to any Stockholder Nominee is required to do so in a manner consistent with the requirements for universal proxy rules pursuant to Rule 14a–19 of the Exchange Act. Namely, the nomination of a Stockholder Nominee shall be disregarded if, among other things, there is no longer an intent to solicit proxies in support of a Stockholder Nominee or there is a failure to comply with the applicable requirements of Rule 14a–19. Upon request by the Corporation, if any stockholder providing notice or any Stockholder Associated Person provides notice pursuant to Rule 14a–19(b) under the Exchange Act, such stockholder

providing notice shall deliver to the Corporate Secretary, no later than five (5) business days prior to the applicable meeting date, then reasonable evidence that the requirements of Rule 14a–19(a)(3) under the Exchange Act have been satisfied.

Currently Section 2.11(c)(vi) of the CGM Bylaws defines "Stockholder Associated Person" to mean, among other things, (i) any person who is a member of a "group" (used in Rule 13d–5 under the Exchange Act) with, or otherwise acting in concert with, any stockholder providing notice, (ii) any person that is directly or indirectly controlled by, or under common control with, such stockholder or such Stockholder Associated Person, or (iii) any person directly or indirectly controlling any such stockholder or any Stockholder Associated Person. The proposed rule change reflects recent developments in Delaware law to add specificity to the definition and limit which individuals may be determined to be a Stockholder Associated Person and makes other clarifying changes. Specifically, the proposed rule change adds the qualifier that a Stockholder Associated Person must be known by the stockholder to be acting in concert with such stockholder, removes from the definition any person directly or indirectly controlled by, or under common control with such stockholder and replaces it with any affiliate or associate of such stockholder providing notice, and deletes the reference in the definition to any person directly or indirectly controlling any such stockholder or Stockholder Associated Person. The proposed rule change also adds any Stockholder Nominee to the definition of Stockholder Associated Person.

Revisions to Other Sections of the Bylaws

Cboe also proposes to make changes to Section 2.11 to reflect recent developments in Delaware law and to provide clarifications and prevent confusion. Cboe proposes to add a note to Section 2.11(a)(ii) that any proposed business for a stockholder meeting must be a proper matter for stockholder action. Cboe also proposes to amend Section 2.11(a)(iii)(B) to state that a Stockholder Nominee's written consent must be included in Cboe's proxy statement before they may be brought before a meeting. Previously, Section 2.11(a)(iii)(B) had stated that the Stockholder Nominee's written consent must be included in a proxy statement, but had not specifically defined it as Cboe's proxy statement. Cboe also proposes to amend the same section to

⁴ *Kellner v. AIM ImmunoTech Inc.*, C.A. 2023–0879–LWW (Del. Ch. Jan. 5, 2024)

state that a Stockholder Nominee will not enter into any commitment to vote in a certain manner if nominated to the CGM Board. Previously, this section had simply stated that a Stockholder Nominee may not enter into any commitment to vote in a certain manner with respect to certain matters at any company, without defining Cboe specifically. Cboe also proposes to amend the same section to require that a Stockholder Nominee not omit facts that are necessary to ensure statements made are not misleading in any material respect. Previously, the Stockholder Nominee's responsibility to not omit facts that are necessary to ensure statements are not misleading was not subject to materiality.

Cboe also proposes to make changes to Section 3.10 of the CGM Bylaws to provide that the Lead Director of Cboe may call a special meeting of the CGM Board. Section 3.10 currently permits, among other things, the Chair of the Board or the Chief Executive Officer to call a special meeting of the CGM Board. Revising this section to allow the Lead Director to call a special meeting of the CGM Board addresses a potential scenario in which the Chair of the Board and the Chief Executive Officer positions are jointly held by one individual and a special meeting of the CGM Board is not able to be called by individual independent directors.

2. Statutory Basis

The Exchange believes the proposed rule change is consistent with the Act and the rules and regulations thereunder applicable to the Exchange and, in particular, the requirements of Section 6(b) of the Act.⁵ Specifically, the Exchange believes the proposed rule change is consistent with the Section 6(b)(5)⁶ requirements that the rules of an exchange be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.

In light of an advisory vote by the stockholders of Cboe, Cboe is proposing changes to its Bylaws to implement a right for stockholders to call a special meeting of the stockholders at a 25% threshold. The Exchange believes that

this filing furthers the objectives of Section 6(b)(5) of the Act because the proposed rule change would be consistent with and facilitate a governance and regulatory structure that is designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to, and perfect the mechanism of a free and open market and a national market system and, in general, to protect investors and the public interest. Particularly, the Exchange believes that, by permitting stockholders of Cboe to bring business or Stockholder Nominees before a special meeting, the proposed rule change strengthens the corporate governance of the Exchange's ultimate parent company, which is beneficial to both investors and the public interest.

Additionally, the procedural requirements are designed to help protect investors by stating clearly and explicitly the procedures stockholders must follow in order to bring business or Stockholder Nominees before a special meeting. The informational requirements are designed to enhance investor protection by helping to ensure among other things, that the Corporation and its stockholders have full and accurate information about nominating stockholders and Stockholder Nominees and that such stockholders and nominees comply with applicable laws, regulations and other requirements.

The changes that the Exchange is proposing with regard to so-called "advance notice bylaws" in light of the recent developments in Delaware law are designed to help provide additional clarity to stockholders wishing to bring business before a stockholder meeting or propose a Stockholder Nominee. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) by simplifying the requirements and clarifying the information that must be disclosed by stockholders. This furthers the interests of investors and the public by removing potential impediments to raising business or proposing Stockholder Nominees that may otherwise restrict a stockholder's ability to participate in the corporate governance of the Corporation.

Finally, the remaining changes to existing provisions of the CGM Bylaws are clarifying in nature, and they enhance investor protection and the public interest by preventing confusion with respect to the operation of the Bylaw provisions.

B. Self-Regulatory Organization's Statement on Burden on Competition

Because the proposed rule change relates to the governance of the Corporation and not to the operations of the Exchange, the Exchange does not believe that the proposed rule change will impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. The proposed rule change is not designed to address any competitive issue or have any impact on competition; rather, adoption of a stockholder special meeting provision, updating "advance notice bylaws," and other bylaws updates by the Corporation are intended to enhance corporate governance and accountability to stockholders.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

The Exchange neither solicited nor received comments on the proposed rule change.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the Exchange consents, the Commission will:

- A. by order approve or disapprove such proposed rule change, or
- B. institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-CboeEDGA-2024-037 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange

⁵ 15 U.S.C. 78f(b).

⁶ 15 U.S.C. 78f(b)(5).

Commission, 100 F Street NE, Washington, DC 20549–1090.

All submissions should refer to file number SR–CboeEDGA–2024–037. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR–CboeEDGA–2024–037 and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁷

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2024–25054 Filed 10–28–24; 8:45 am]

BILLING CODE 8011–01–P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–101419; File No. SR–CboeBZX–2024–087]

Self-Regulatory Organizations; Cboe BZX Exchange, Inc.; Notice of Filing of a Proposed Rule Change With Respect to Amendments to the Seventh Amended and Restated Bylaws (the “CGM Bylaws”) of Its Parent Corporation, Cboe Global Markets, Inc. (“Cboe” or “Corporation”)

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (the “Act”),¹ and Rule 19b–4 thereunder,² notice is hereby given that on October 11, 2024, Cboe BZX Exchange, Inc. (the “Exchange” or “BZX”) filed with the Securities and Exchange Commission (“Commission”) the proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization's Statement of the Terms of Substance of the Proposed Rule Change

Cboe BZX Exchange, Inc. (the “Exchange” or “BZX”) is filing with the Securities and Exchange Commission (the “Commission”) a proposed rule change with respect to amendments to the Seventh Amended and Restated Bylaws (the “CGM Bylaws”) of its parent corporation, Cboe Global Markets, Inc. (“Cboe” or “Corporation”). The text of the proposed rule change is provided in Exhibit 5.

The text of the proposed rule change is also available on the Exchange's website (http://markets.cboe.com/us/equities/regulation/rule_filings/bzx/), at the Exchange's Office of the Secretary, and at the Commission's Public Reference Room.

II. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the Exchange included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of

the most significant aspects of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

At Cboe's annual meeting held on May 16, 2024, Cboe's stockholders considered two advisory proposals that would provide Cboe stockholders with the right to call a special meeting of the stockholders provided that a certain threshold percentage of stockholders propose to call such a meeting. The two proposals were submitted separately. One of the proposals was submitted by an individual stockholder (“Stockholder Proposal”). The other proposal was submitted by Cboe Management (“Management Proposal”). The Stockholder Proposal, which did not pass but received 45% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 10% of Cboe's voting power to call a special meeting of the stockholders. The Management Proposal, which passed with 65% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 25% of Cboe's voting power to call a special meeting of the stockholders.

The Nominating & Governance Committee of the CGM Board reviewed the voting results of the Stockholder Proposal and the Management Proposal and discussed the stockholder voting standards and rights contemplated by the CGM Bylaws. Following this review, the Nominating & Governance Committee recommended to the CGM Board, and the CGM Board approved, certain changes to the CGM Bylaws to implement the Management Proposal. The CGM Board also approved amending the CGM Bylaws to improve the governance processes of Cboe, to make certain provisions more consistent with Delaware General Corporation Law (“DGCL”), and to make clarifying and cleanup changes to the CGM Bylaws. The proposed rule change amends the CGM Bylaws to implement the changes approved by the CGM Board.

Proposed Changes to Article 2—Stockholders

Current Section 2.3 (Special Meeting) of the CGM Bylaws provides that only the Chair of the Board, the Chief Executive Officer or the CGM Board may call a special meeting of the stockholders. To respond to feedback from its stockholders, as discussed above, Cboe proposes to delete portions of this provision and add language that

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b–4.

⁷ 17 CFR 200.30–3(a)(12).

will provide Cboe stockholders with the right to call special stockholder meetings (a "Stockholder Requested Special Meeting") after following particular procedures.

In defining the procedural requirements, Cboe's goals are to ensure timely notice of a meeting request and to gather sufficient information about the proposing stockholder(s) and the proposed business itself. Among other things, this information will help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to adequately assess proposed business submitted by stockholders. Additionally, Cboe notes that the proposed terms are common among public companies that have adopted a right for stockholders to call special meetings. The proposed changes to the CGM Bylaws to effect the stockholder special meeting right are set forth below.

Revisions to Section 2.3(a)

First, the proposed changes to Section 2.3(a) provide that a Stockholder Requested Special Meeting may be called: (i) at any time by the CGM Board pursuant to a resolution adopted by the affirmative vote of a majority of the total number of CGM directors then in office; or (ii) by Cboe's Corporate Secretary following the receipt of a written request in proper form for a special meeting (a "Special Meeting Request") by one or more stockholders. In order to call a special meeting, the stockholders must hold, in the aggregate, at least 25% of Cboe's outstanding shares of common stock entitled to vote on matters brought before the special meeting (the "Requisite Percentage").

The proposed changes to Section 2.3(a) also clarify that the Chair of the Board, the Chief Executive Officer or the President of Cboe may not individually call a special meeting of the stockholders. This change was made to vest authority within Cboe to call a special meeting in the Board. Without the proposed change, the Chair of the Board, Chief Executive Officer and the President could each call a special meeting of the stockholders without CGM Board approval. The proposed change to Section 2.3(a) simplifies this requirement to confirm that, within Cboe, only the CGM Board may call for a special meeting of the stockholders.

Proposed Section 2.3(b) and Section 2.3(c)

Proposed Section 2.3(b) and Section 2.3(c) set forth the procedures a stockholder must follow in order to submit a written request in proper form

to call a Stockholder Requested Special Meeting. Stockholders must first submit a request to Cboe's Corporate Secretary to define a date on which the Requisite Percentage will be determined (the "Record Date"). A stockholder must sign any request to set a Record Date and also provide a reasonably brief description of the purpose or purposes of the special meeting of the stockholders. A stockholder is also required in the request to set a Record Date to disclose certain information regarding themselves and any individuals or entities such stockholder may be associated with (a "Stockholder Associated Person(s)"), as well as such information concerning any nominees to the CGM Board ("Stockholder Nominee(s)") if such stockholder is so proposing. The information that a stockholder must disclose regarding Stockholder Associated Persons and Stockholder Nominees is contained in Section 2.11 of the CGM Bylaws and incorporated by reference in this Section 2.3(b). The information required to be provided in the request to set a Record Date provides Cboe with notice that a stockholder is seeking to bring business before the stockholders and assists with the logistical aspects of determining which stockholders will be counted for purposes of determining whether the Requisite Percentage is met.

Proposed Section 2.3(d) and Section 2.3(e)

Proposed Section 2.3(d) and Section 2.3(e) include detailed information on the requirements for a Special Meeting Request to have been properly delivered, subject to certain carve-outs for stockholders who submit their request in response to a solicitation for public consent by the Corporation made pursuant to Section 14 of the Exchange Act. Specifically, a Special Meeting Request must:

- be delivered within 60 days following the Record Date;
- be signed by each stockholder making up the Requisite Percentage;
- contain a reasonably brief description of the purpose of the special meeting;
- include details of each stockholder holding the Requisite Percentage, including:
 - The stockholder's name;
 - The stockholder's address;
 - information concerning the stockholder submitting the Special Meeting Request and any Stockholder Associated Persons;
 - information concerning any Stockholder Nominees; and
 - documentary evidence that the shares included in the Requisite

Percentage are owned by such stockholder;

- include an acknowledgment that any reduction in the number of shares owned by such stockholders as of the date of such Special Meeting Request and through the meeting date will constitute a revocation of such Special Meeting Request with respect to such reduction;
- relate to an item of business that is a proper subject for stockholder action under applicable law;
- not include an item of business that did not appear on the request to set a Record Date;
- not be delivered during the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting and ending on the date of the next annual meeting; and
- otherwise comply with applicable law.

In defining the requirements for a Special Meeting Request, Cboe's goal is to gather sufficient information about the stockholder seeking to request a special meeting and the proposed business for both itself and its stockholders and to help ensure the efficient use of corporate resources by restricting a stockholder from raising items that could reasonably be addressed at an annual meeting of the stockholders, as in the requirement that a Special Meeting Request not be delivered in the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting. Overall, this information is designed to help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to assess the proposed business or Stockholder Nominee adequately.

Proposed Section 2.3(f)

Proposed Section 2.3(f) provides that the CGM Board may cancel a special meeting in its discretion if the percentage of stock held by the stockholders requesting a special meeting falls below the Requisite Percentage at any point after sixty (60) days from the first date on which a valid Special Meeting Request is delivered to Cboe. This provides the CGM Board with discretion to reevaluate the Special Meeting Request in the event the Special Meeting Request is revoked by stockholders holding a sufficient percentage of the stock of the Corporation.

Proposed Section 2.3(g)

Proposed Section 2.3(g) provides that within ten (10) days following the date on which the Secretary has received valid Special Meeting Requests, the CGM Board shall fix the record date and meeting date, time and location for the Stockholder Requested Special Meeting, provided that the date of any such Stockholder Requested Special Meeting shall not be more than ninety (90) days after the date on which a valid Special Meeting Request is received by Cboe. The CGM Board may submit its own proposal or proposals for consideration at any Stockholder Requested Special Meeting. Ninety (90) days allows the Corporation reasonable time to assess the items proposed in the Special Meeting Request while also not imposing a potentially burdensome delay on the stockholders.

Proposed Section 2.3(h)

Proposed Section 2.3(h) provides that multiple Special Meeting Requests may be considered together if (i) each Special Meeting Request identifies the same or substantially the same purpose or purposes of the Stockholder Requested Special Meeting and the same or substantially the same items of business proposed to be brought before the Stockholder Requested Special Meeting, and (ii) such Special Meeting Requests have been dated and delivered to the Corporate Secretary within sixty (60) days of the delivery to the Corporate Secretary of the earliest dated Special Meeting Request relating to such item(s) of business. This proposed section helps to ensure the efficient use of corporate resources by preventing multiple stockholders from raising items that should reasonably be consolidated. The conditions under which the Corporation may combine multiple Special Meeting Requests are sufficiently limited to require that each unique item is addressed separately.

Revisions to Section 2.9

Section 2.9 of the CGM Bylaws governs proxy representation. It is proposed that language be added to clarify that any stockholder directly or indirectly soliciting proxies from other stockholders of the Corporation may use any proxy card color other than white, which shall be reserved for exclusive use by the CGM Board.

Revisions to Section 2.11

Section 2.11 of the CGM Bylaws, which are the “advance notice bylaws”,³ requires stockholders to

notify Cboe, during a specified period in advance of an annual meeting or special meeting called by the CGM Board, of their intention to nominate one or more persons for election to the CGM Board or to present a business proposal for consideration by the stockholders at the meeting and provide certain information regarding such request. When designing the proposed procedural requirements for stockholders to call a special meeting, as outlined above, Cboe evaluated the existing procedural requirements for stockholders to bring business before an annual meeting or to nominate director candidates at an annual meeting or special meeting. Cboe has determined that the advance notice bylaws may be enhanced to help achieve the core objectives of fulsome disclosure and accurate explanations from stockholders bringing business or potential nominees before a stockholder meeting. While advance notice bylaws are beneficial in providing a company and its stockholders with information regarding stockholders, and their Stockholder Associated Persons, seeking to bring business or potential nominees before a stockholder meeting, therefore permitting orderly meetings and election contests, and assisting the board’s information gathering and disclosure functions, the Delaware Supreme Court in *Kellner v. AIM ImmunoTech Inc.*⁴ has recently provided some guidance on circumstances where such requests may be overbroad or request information not sufficiently connected to the legitimate information gathering function these provisions serve. Therefore, as further detailed below, Cboe has determined that it would be beneficial to refine certain of the provisions in the CGM Bylaws to increase the clarity of the requests for information from stockholders seeking to bring business before a meeting.

First, Section 2.11(a)(iii)(C) of the CGM Bylaws currently defines the information required to be disclosed regarding a stockholder providing notice of nominations or other business, any Stockholder Associated Person(s) and any Stockholder Nominee(s). Cboe proposes certain amendments to this section to (i) clarify the information a stockholder is required to disclose

meeting of stockholders, but set forth procedural requirements to help ensure that companies and boards have sufficient information about the proposal and the proposing stockholder(s), as well as adequate time to consider the proposal, by requiring the proposing stockholder(s) to give advance notice of the intention to bring the proposal before the annual or special meeting.

⁴ *Kellner v. AIM ImmunoTech Inc.*, C. A. 2023–0879–LWW (Del. Ch. Jan. 5, 2024).

relating to arrangements between the stockholder providing notice or any Stockholder Associated Person and any other stockholder with regard to the stockholder meeting and (ii) eliminate disclosures on performance related fees to which such stockholder or Stockholder Associated Person may be entitled as a result of any increase or decrease in the stock of Cboe, and the prospectus or similar document of the stockholder providing notice or any Stockholder Associated Person. Cboe believes that, while these provisions as currently written provide valuable information to the Corporation and its stockholders in assessing the proposed business or Stockholder Nominee, these requirements should be sufficiently specific so as not to potentially dissuade stockholders from bringing business before a stockholder meeting and should otherwise comply with Delaware law. The proposed changes narrow the information required to be disclosed such that Cboe is able to help ensure the objectives of the provisions are met without burdening stockholders with potentially overbroad requests for information.

Section 2.11(a)(iii)(D) of the CGM Bylaws currently sets forth certain representations that must be made by a stockholder seeking to bring business or a Stockholder Nominee before a stockholder meeting regarding whether such stockholder is part of a group which intends to deliver or solicit proxies from stockholders in support of such proposed business. Cboe proposes changes to update this section in order to be more consistent with the universal proxy rules provided for in Rule 14a–19 of the Exchange Act by explicitly stating that any stockholder providing notice that they intend to solicit proxies in support of a proposed nominee must do so in accordance with Rule 14a–19 of the Exchange Act. Cboe also proposes to clarify that the representation must confirm whether the stockholder intends or is part of a group which intends to engage in a solicitation (within the meaning of Rule 14a–1(1) of the Exchange Act) with respect to the nomination of any proposed nominee or proposed business to be considered at the meeting.

Section 2.11(a)(iii)(F) of the CGM Bylaws currently requires that a Stockholder Nominee furnish any information that Cboe may determine is required for Cboe to determine the qualifications of such Stockholder Nominee to serve as a director of the Corporation. Cboe proposes to add language clarifying that the information Cboe may require must be consistent with the parameters set forth in Cboe’s

³ “Advance notice bylaws” allow stockholder(s) to bring business before an annual or special

Corporate Governance Guidelines or the CGM Board's past practice in evaluating potential director nominees.

Proposed Section 2.11(c)(ii) of the CGM Bylaws requires the stockholder providing notice to notify the Secretary of any inaccuracy or change in any information submitted pursuant to Section 2.11 within two (2) business days of becoming aware of such inaccuracy or change. Cboe proposes to modify this requirement by narrowing the scope of circumstances in which a stockholder is required to provide notice of any inaccuracy or change of information that they have previously provided to material inaccuracies or changes.

Proposed Section 2.11(c)(iii) of the CGM Bylaws provides that any stockholder or Stockholder Associated Person providing notice with respect to any Stockholder Nominee is required to do so in a manner consistent with the requirements for universal proxy rules pursuant to Rule 14a–19 of the Exchange Act. Namely, the nomination of a Stockholder Nominee shall be disregarded if, among other things, there is no longer an intent to solicit proxies in support of a Stockholder Nominee or there is a failure to comply with the applicable requirements of Rule 14a–19. Upon request by the Corporation, if any stockholder providing notice or any Stockholder Associated Person provides notice pursuant to Rule 14a–19(b) under the Exchange Act, such stockholder providing notice shall deliver to the Corporate Secretary, no later than five (5) business days prior to the applicable meeting date, then reasonable evidence that the requirements of Rule 14a–19(a)(3) under the Exchange Act have been satisfied.

Currently Section 2.11(c)(vi) of the CGM Bylaws defines “Stockholder Associated Person” to mean, among other things, (i) any person who is a member of a “group” (used in Rule 13d–5 under the Exchange Act) with, or otherwise acting in concert with, any stockholder providing notice, (ii) any person that is directly or indirectly controlled by, or under common control with, such stockholder or such Stockholder Associated Person, or (iii) any person directly or indirectly controlling any such stockholder or any Stockholder Associated Person. The proposed rule change reflects recent developments in Delaware law to add specificity to the definition and limit which individuals may be determined to be a Stockholder Associated Person and makes other clarifying changes. Specifically, the proposed rule change adds the qualifier that a Stockholder Associated Person must be known by

the stockholder to be acting in concert with such stockholder, removes from the definition any person directly or indirectly controlled by, or under common control with such stockholder and replaces it with any affiliate or associate of such stockholder providing notice, and deletes the reference in the definition to any person directly or indirectly controlling any such stockholder or Stockholder Associated Person. The proposed rule change also adds any Stockholder Nominee to the definition of Stockholder Associated Person.

Revisions to Other Sections of the Bylaws

Cboe also proposes to make changes to Section 2.11 to reflect recent developments in Delaware law and to provide clarifications and prevent confusion. Cboe proposes to add a note to Section 2.11(a)(ii) that any proposed business for a stockholder meeting must be a proper matter for stockholder action. Cboe also proposes to amend Section 2.11(a)(iii)(B) to state that a Stockholder Nominee's written consent must be included in Cboe's proxy statement before they may be brought before a meeting. Previously, Section 2.11(a)(iii)(B) had stated that the Stockholder Nominee's written consent must be included in a proxy statement, but had not specifically defined it as Cboe's proxy statement. Cboe also proposes to amend the same section to state that a Stockholder Nominee will not enter into any commitment to vote in a certain manner if nominated to the CGM Board. Previously, this section had simply stated that a Stockholder Nominee may not enter into any commitment to vote in a certain manner with respect to certain matters at any company, without defining Cboe specifically. Cboe also proposes to amend the same section to require that a Stockholder Nominee not omit facts that are necessary to ensure statements made are not misleading in any material respect. Previously, the Stockholder Nominee's responsibility to not omit facts that are necessary to ensure statements are not misleading was not subject to materiality.

Cboe also proposes to make changes to Section 3.10 of the CGM Bylaws to provide that the Lead Director of Cboe may call a special meeting of the CGM Board. Section 3.10 currently permits, among other things, the Chair of the Board or the Chief Executive Officer to call a special meeting of the CGM Board. Revising this section to allow the Lead Director to call a special meeting of the CGM Board addresses a potential scenario in which the Chair of the Board

and the Chief Executive Officer positions are jointly held by one individual and a special meeting of the CGM Board is not able to be called by individual independent directors.

2. Statutory Basis

The Exchange believes the proposed rule change is consistent with the Act and the rules and regulations thereunder applicable to the Exchange and, in particular, the requirements of Section 6(b) of the Act.⁵ Specifically, the Exchange believes the proposed rule change is consistent with the Section 6(b)(5)⁶ requirements that the rules of an exchange be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.

In light of an advisory vote by the stockholders of Cboe, Cboe is proposing changes to its Bylaws to implement a right for stockholders to call a special meeting of the stockholders at a 25% threshold. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) of the Act because the proposed rule change would be consistent with and facilitate a governance and regulatory structure that is designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to, and perfect the mechanism of a free and open market and a national market system and, in general, to protect investors and the public interest. Particularly, the Exchange believes that, by permitting stockholders of Cboe to bring business or Stockholder Nominees before a special meeting, the proposed rule change strengthens the corporate governance of the Exchange's ultimate parent company, which is beneficial to both investors and the public interest.

Additionally, the procedural requirements are designed to help protect investors by stating clearly and explicitly the procedures stockholders must follow in order to bring business

⁵ 15 U.S.C. 78f(b).

⁶ 15 U.S.C. 78f(b)(5).

or Stockholder Nominees before a special meeting. The informational requirements are designed to enhance investor protection by helping to ensure among other things, that the Corporation and its stockholders have full and accurate information about nominating stockholders and Stockholder Nominees and that such stockholders and nominees comply with applicable laws, regulations and other requirements.

The changes that the Exchange is proposing with regard to so-called “advance notice bylaws” in light of the recent developments in Delaware law are designed to help provide additional clarity to stockholders wishing to bring business before a stockholder meeting or propose a Stockholder Nominee. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) by simplifying the requirements and clarifying the information that must be disclosed by stockholders. This furthers the interests of investors and the public by removing potential impediments to raising business or proposing Stockholder Nominees that may otherwise restrict a stockholder’s ability to participate in the corporate governance of the Corporation.

Finally, the remaining changes to existing provisions of the CGM Bylaws are clarifying in nature, and they enhance investor protection and the public interest by preventing confusion with respect to the operation of the Bylaw provisions.

B. Self-Regulatory Organization’s Statement on Burden on Competition

Because the proposed rule change relates to the governance of the Corporation and not to the operations of the Exchange, the Exchange does not believe that the proposed rule change will impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. The proposed rule change is not designed to address any competitive issue or have any impact on competition; rather, adoption of a stockholder special meeting provision, updating “advance notice bylaws,” and other bylaws updates by the Corporation are intended to enhance corporate governance and accountability to stockholders.

C. Self-Regulatory Organization’s Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

The Exchange neither solicited nor received comments on the proposed rule change.

III. Date of Effectiveness of the Proposed Rule Change and Timing of Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the Exchange consents, the Commission will:

- A. by order approve or disapprove such proposed rule change, or
- B. institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission’s internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-CboeBZX-2024-087 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.
- All submissions should refer to file number SR-CboeBZX-2024-087. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission’s internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission’s Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and

copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR-CboeBZX-2024-087 and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁷

Sherry R. Haywood,

Assistant Secretary.

[FR Doc. 2024-25057 Filed 10-28-24; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-101410; File No. SR-NYSEARCA-2024-85]

Self-Regulatory Organizations; NYSE Arca, Inc.; Notice of Filing and Immediate Effectiveness of Proposed Rule Change To Amend the NYSE Arca Equities Fees and Charges

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (“Act”),¹ and Rule 19b-4 thereunder,² notice is hereby given that on October 10, 2024, NYSE Arca, Inc. (“NYSE Arca” or the “Exchange”) filed with the Securities and Exchange Commission (“SEC” or “Commission”) the proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization’s Statement of the Terms of Substance of the Proposed Rule Change

The Exchange proposes to amend the NYSE Arca Equities Fees and Charges (“Fee Schedule”) to (1) increase the credits payable under certain Mid-Point Liquidity (“MPL”) Order pricing tiers, and (2) adopt a lower fee for certain Retail Orders that remove liquidity in securities with a per share price below \$1.00. The proposed rule change is available on the Exchange’s website at www.nyse.com, at the principal office of the Exchange, and at the Commission’s Public Reference Room.

⁷ 17 CFR 200.30-3(a)(12).

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

II. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the self-regulatory organization included statements concerning the purpose of, and basis for, the proposed rule change and discussed any comments it received on the proposed rule change. The text of those statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of the most significant parts of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

The Exchange proposes to amend the Fee Schedule to (1) increase the credits payable under certain MPL Order³ pricing tiers, and (2) adopt a lower fee for certain Retail Orders⁴ that remove liquidity in securities with a per share price below \$1.00 ("Sub-Dollar Securities"), as described below.

The Exchange proposes to implement the fee changes effective October 10, 2024.⁵

Background

The Exchange operates in a highly competitive market. The Commission has repeatedly expressed its preference for competition over regulatory intervention in determining prices, products, and services in the securities markets. In Regulation NMS, the Commission highlighted the importance of market forces in determining prices and SRO revenues and, also, recognized that current regulation of the market system "has been remarkably successful in promoting market competition in its broader forms that are most important to investors and listed companies."⁶

While Regulation NMS has enhanced competition, it has also fostered a "fragmented" market structure where trading in a single stock can occur across multiple trading centers. When multiple trading centers compete for order flow in the same stock, the Commission has recognized that "such competition can lead to the fragmentation of order flow in that stock."⁷ Indeed, equity trading is currently dispersed across 16 exchanges,⁸ numerous alternative trading systems,⁹ and broker-dealer internalizers and wholesalers, all competing for order flow. Based on publicly available information, no single exchange currently has more than 20% market share.¹⁰ Therefore, no exchange possesses significant pricing power in the execution of equity order flow. More specifically, the Exchange currently has less than 12% market share of executed volume of equities trading.¹¹

The Exchange believes that the ever-shifting market share among the exchanges from month to month demonstrates that market participants can move order flow, or discontinue or reduce use of certain categories of products. While it is not possible to know a firm's reason for shifting order flow, the Exchange believes that one such reason is because of fee changes at any of the registered exchanges or non-exchange venues to which the firm routes order flow. Accordingly, competitive forces compel the Exchange to use exchange transaction fees and credits because market participants can readily trade on competing venues if they deem pricing levels at those other venues to be more favorable.

Proposed Rule Change

MPL Orders

In response to this competitive environment, the Exchange has already established multiple levels of credits for MPL Orders that allow ETP Holders to passively interact with trading interest on the Exchange and offer potential

price improvement to incoming marketable orders submitted to the Exchange.¹² In order to provide an incentive for ETP Holders to provide such liquidity, the credits increase based on increased levels of volume directed to the Exchange. The MPL Order pricing tiers are intended to incentivize ETP Holders to earn increased credits by sending greater amounts of liquidity-providing MPL Orders in Tapes A, B and C securities to the Exchange.

As noted above, the Exchange currently provides multiple levels of credits, ranging from \$0.0015 per share to \$0.0030 per share, to ETP Holders that send MPL Orders that provide liquidity to the Exchange. For the current MPL Order pricing tier, the amount of the per share credit is based on an ETP Holder's ADV of provided liquidity in MPL Orders for Tape A, Tape B and Tape C Securities combined ("MPL Adding ADV").

Under current MPL Tier 8, for ETP Holders that have MPL Adding ADV during a billing month of at least 1.5 million shares, the Exchange currently provides a credit of \$0.0015 per share in Tape A, Tape B and Tape C securities. Under current MPL Tier 7, for ETP Holders with MPL Adding ADV during a billing month of at least 2 million shares, the Exchange currently provides a credit of \$0.0020 per share in Tape A, Tape B and Tape C securities. Under current MPL Tier 6, the Exchange provides a credit of \$0.0025 per share in Tape A, Tape B and Tape C securities to ETP Holders that have MPL Adding ADV during a billing month of at least 3 million shares. ETP Holders can alternatively qualify for the MPL Tier 6 credit if they have MPL Adding ADV during the billing month of at least 1 million shares and have MPL Adding ADV, as a percent of Adding ADV, of at least 50%. Under current MPL Tier 5, the Exchange provides a credit of \$0.0026 per share in Tape A, Tape B and Tape C securities to ETP Holders that have MPL Adding ADV during a billing month of at least 5 million shares. ETP Holders can alternatively qualify for the MPL Tier 5 credit if they have MPL Adding ADV during the billing month of at least 2 million shares and have MPL Adding ADV, as a percent of Adding ADV, of at least 50%. Under MPL Tier 4, for ETP Holders with MPL Adding ADV during a billing month of at least 13 million shares, the Exchange currently provides a credit of \$0.0027 per share in Tape A, Tape B

³ A MPL Order is a limit order that is not displayed and does not route, with a working price at the lower (higher) of the midpoint of the Protected Best Bid/Offer or its limit price. See NYSE Arca Rule 7.31-E(d)(3).

⁴ Rule 7.31-E(i)(4)(A) provides that an "order designated with a "retail" modifier is an agency order or a riskless principal order that meets the criteria of FINRA Rule 5320.03 that originates from a natural person and is submitted to the Exchange by an ETP Holder, provided that no change is made to the terms of the order with respect to price or side of market and the order does not originate from a trading algorithm or any other computerized methodology."

⁵ The Exchange originally filed to amend the Fee Schedule on October 1, 2024 (SR-NYSEARCA-2024-82). SR-NYSEARCA-2024-82 was subsequently withdrawn and replaced by this filing.

⁶ See Securities Exchange Act Release No. 51808 (June 9, 2005), 70 FR 37496, 37499 (June 29, 2005)

(File No. S7-10-04) (Final Rule) ("Regulation NMS").

⁷ See Securities Exchange Act Release No. 61358, 75 FR 3594, 3597 (January 21, 2010) (File No. S7-02-10) (Concept Release on Equity Market Structure).

⁸ See Choe U.S. Equities Market Volume Summary, available at https://markets.cboe.com/us/equities/market_share.

⁹ See FINRA ATS Transparency Data, available at <https://otctransparency.finra.org/otctransparency/AtsIssueData>. A list of alternative trading systems registered with the Commission is available at <https://www.sec.gov/foia/docs/atstlist.htm>.

¹⁰ See Choe Global Markets U.S. Equities Market Volume Summary, available at http://markets.cboe.com/us/equities/market_share/.

¹¹ See *id.*

¹² See, e.g., Securities Exchange Act Release No. 54511 (September 26, 2006), 71 FR 58460, 58461 (October 3, 2006) (SR-PCX-2005-53).

and Tape C securities. Under MPL Tier 3, for ETP Holders with MPL Adding ADV during a billing month of at least 15 million shares, the Exchange currently provides a credit of \$0.0028 per share in Tape A, Tape B and Tape C securities. Under MPL Tier 2, for ETP Holders with MPL Adding ADV during a billing month of at least 25 million shares, the Exchange currently provides a credit of \$0.0029 per share in Tape A, Tape B and Tape C securities. Finally, under MPL Tier 1, for ETP Holders with MPL Adding ADV during a billing month of at least 30 million shares, the Exchange currently provides a credit of \$0.0030 per share in Tape A, Tape B and Tape C securities.¹³

The Exchange now proposes to increase the credits payable for MPL Tier 1, MPL Tier 2, MPL Tier 3 and MPL Tier 4, as follows:

- Increase the credit payable for MPL Tier 1, from \$0.0030 per share to \$0.0033 per share in Tape A, Tape B and Tape C securities, without any change to the volume requirement to qualify for the proposed higher MPL Tier 1 credit;
- Increase the credit payable for MPL Tier 2, from \$0.0029 per share to \$0.0032 per share in Tape A, Tape B and Tape C securities, without any change to the volume requirement to qualify for the proposed higher MPL Tier 2 credit;

- Increase the credit payable for MPL Tier 3, from \$0.0028 per share to \$0.0031 per share in Tape A, Tape B and Tape C securities, without any change to the volume requirement to qualify for the proposed higher MPL Tier 3 credit; and

- Increase the credit payable for MPL Tier 4, from \$0.0027 per share to \$0.0029 per share in Tape A, Tape B and Tape C securities, without any change to the volume requirement to qualify for the proposed higher MPL Tier 4 credit.

With this proposed change, the MPL Order Tiers pricing tier would appear as follows:

MPL order tiers

Tier	Minimum requirement		Credit for MPL adding	
	MPL adding ADV	MPL adding ADV as percent of adding ADV	Tape A	Tape B and Tape C
MPL Tier 1	30 Million		(\$0.0033)	(\$0.0033)
MPL Tier 2	25 Million		(0.0032)	(0.0032)
MPL Tier 3	15 Million		(0.0031)	(0.0031)
MPL Tier 4	13 Million		(0.0029)	(0.0029)
MPL Tier 5	5 Million or		(0.0026)	(0.0026)
	2 Million	50		
MPL Tier 6	3 Million or		(0.0025)	(0.0025)
	1 Million	50		
MPL Tier 7	2 Million		(0.0020)	(0.0020)
MPL Tier 8	1.5 Million		(0.0015)	(0.0015)

The goal of the proposed rule change is to incentivize ETP Holders to increase the number of MPL Orders they post on the Exchange's Book, which would provide additional price improvement opportunities for incoming orders, and thus qualify for the proposed higher per share credits. MPL Orders allow for additional opportunities for passive interaction with trading interest on the Exchange and are designed to offer potential price improvement to incoming marketable orders submitted to the Exchange. The Exchange believes that by correlating the level of the credit to the level of MPL Adding ADV, the Exchange's fee structure would incentivize ETP Holders to submit more liquidity-providing MPL Orders to the Exchange, thereby increasing the potential for price improvement to incoming marketable orders submitted to the Exchange.

The Exchange believes adopting increased credits payable under the MPL Tiers 1, 2, 3 and 4 would provide an incentive for ETP Holders to send increased order flow to qualify for these

tiers. As noted above, the Exchange operates in a competitive environment, particularly as it relates to attracting MPL Orders that are posted on the Exchange's Book. Since the Exchange is not amending the volume requirement to qualify for MPL Tiers 1, 2, 3 and 4, the Exchange believes that the proposed higher credits would incentivize ETP Holders to route a greater number of liquidity-providing orders to the Exchange to qualify for the proposed higher credits.

The Exchange does not know how much order flow ETP Holders choose to route to other exchanges or to off-exchange venues. Without having a view of ETP Holders' activity on other markets and off-exchange venues, the Exchange has no way of knowing whether the proposed fee change would result in any ETP Holder sending more of its liquidity-providing orders to the Exchange to qualify for the proposed higher credits. The Exchange cannot predict with certainty how many ETP Holders would avail themselves of this opportunity, but additional liquidity-

providing orders would benefit all market participants because it would provide greater execution opportunities on the Exchange. The Exchange believes the proposed higher credits would provide an incentive for ETP Holders to submit additional MPL Orders to the Exchange to qualify for such credits.

Sub-Dollar Retail Day Remove Tier

As described below, the Exchange proposes to adopt a new pricing tier that would provide ETP Holders the ability to pay a lower fee for Retail Orders in Sub-Dollar Securities with a time-in-force of Day that remove liquidity from the Exchange. Currently, the Exchange charges a fee equal to 0.3% of the total dollar value for all orders in Sub-Dollar Securities that remove liquidity.¹⁴

Specifically, the Exchange proposes to adopt a new pricing tier titled Sub-Dollar Retail Day Remove Tier under Section VIII. Tier Rates—Round Lots and Odd Lots (Per Share Price Below \$1.00). As proposed, ETP Holders that, during the billing month, have Retail Orders in Sub-Dollar Securities with a

¹³ The Exchange charges a fee of \$0.0030 per share for MPL Orders in Tape A, Tape B and Tape C Securities that remove liquidity from the Exchange that are not designated as "Retail

Orders." MPL Orders removing liquidity from the Exchange that are designated as Retail Orders are subject to a fee of \$0.0010 per share. *See* Fee Schedule.

¹⁴ *See* Fee Schedule, Section III. Standard Rates—Transactions (applicable when Tier Rates do not apply).

time-in-force of Day equal to 0.20% of CADV¹⁵ in Sub-Dollar Securities that remove liquidity would be charged a fee of 0.20% of total dollar value. ETP Holders that meet the proposed volume requirement would qualify to pay the proposed lower fee for Retail Orders in Sub-Dollar Securities with a time-in-force of Day that remove liquidity.

The purpose of the proposed rule change is to encourage greater participation from ETP Holders and promote liquidity in Retail Orders. The Exchange believes that the proposed rule change to adopt a volume requirement to qualify for the proposed fee reduction would incentivize ETP Holders to direct a greater number of Retail Orders in Sub-Dollar Securities to the Exchange that remove liquidity. As described above, ETP Holders have a choice of where to send their Retail Orders in Sub-Dollar Securities that remove liquidity. The Exchange believes that the proposed rule change to reduce fees paid by ETP Holders for Retail Orders in Sub-Dollar Securities could lead to more ETP Holders choosing to route such orders for execution to the Exchange rather than to a competing exchange.

While the Exchange proposes to adopt a volume threshold for the proposed new pricing tier, the Exchange believes ETP Holders will be able to meet the proposed requirement given the increased trading in Sub-Dollar Securities in recent months. ETP Holders that trade in Sub-Dollar Securities would benefit by paying a lower fee for Retail Orders with a time-in-force of Day if they choose to send such orders to the Exchange. Based on their current trading profile on the Exchange, a number of ETP Holders would currently qualify for the proposed lower fee. However, without having a view of ETP Holders' activity on other markets and off-exchange venues, the Exchange has no way of knowing whether this proposed rule change would result in other ETP Holders directing orders to the Exchange in order to qualify for the proposed lower fee. The Exchange cannot predict with certainty how many ETP Holders would avail themselves of this opportunity, but increased activity of Retail Orders in Sub-Dollar Securities

would benefit all market participants because it would provide greater execution opportunities on the Exchange.

The proposed changes are not otherwise intended to address any other issues, and the Exchange is not aware of any significant problems that market participants would have in complying with the proposed changes.

2. Statutory Basis

The Exchange believes that the proposed rule change is consistent with Section 6(b) of the Act,¹⁶ in general, and furthers the objectives of Sections 6(b)(4) and (5) of the Act,¹⁷ in particular, because it provides for the equitable allocation of reasonable dues, fees, and other charges among its members, issuers and other persons using its facilities and does not unfairly discriminate between customers, issuers, brokers or dealers.

The Proposed Fee Change Is Reasonable

As discussed above, the Exchange operates in a highly fragmented and competitive market. The Commission has repeatedly expressed its preference for competition over regulatory intervention in determining prices, products, and services in the securities markets. Specifically, in Regulation NMS, the Commission highlighted the importance of market forces in determining prices and SRO revenues and, also, recognized that current regulation of the market system "has been remarkably successful in promoting market competition in its broader forms that are most important to investors and listed companies."¹⁸

As the Commission itself recognized, the market for trading services in NMS stocks has become "more fragmented and competitive."¹⁹ Indeed, equity trading is currently dispersed across 16 exchanges,²⁰ numerous alternative trading systems,²¹ and broker-dealer internalizers and wholesalers, all competing for order flow. Based on publicly-available information, no

single exchange currently has more than 20% market share (whether including or excluding auction volume).²² The Exchange believes that the ever-shifting market share among the exchanges from month to month demonstrates that market participants can shift order flow, or discontinue or reduce use of certain categories of products, in response to fee changes. Accordingly, the Exchange's fees are reasonably constrained by competitive alternatives and market participants can readily trade on competing venues if they deem pricing levels at those other venues to be more favorable.

MPL Orders

The Exchange believes the proposed changes to MPL Tiers 1, 2, 3 and 4 are reasonable because the increased credits payable under these tiers would provide an incentive for ETP Holders to route greater amounts of liquidity-providing orders to the Exchange. As noted above, the Exchange operates in a highly competitive environment, particularly for attracting order flow that provides liquidity on an exchange. The Exchange believes it is reasonable to provide the higher credits under MPL Tiers 1, 2, 3, and 4 for orders that provide liquidity if an ETP Holder meets the qualification for such pricing tiers.

The Exchange believes the proposed increased credits are reasonable as they would provide an additional incentive for ETP Holders to qualify for these new tiers and direct their order flow to the Exchange and provide meaningful added levels of liquidity, thereby contributing to the depth, market quality, and price improvement on the Exchange.

On the backdrop of the competitive environment in which the Exchange currently operates, the proposed rule change is a reasonable attempt by the Exchange to increase its liquidity and improve its market share relative to its competitors.

Sub-Dollar Retail Day Remove Tier

The Exchange believes it is reasonable to adopt the proposed Sub-Dollar Retail Day Remove pricing tier because the Exchange believes the proposed lower fee under the proposed pricing tier would encourage greater participation from ETP Holders, which could result in increased execution of Retail Orders in Sub-Dollar Securities. In this regard, an ETP Holder that does not qualify for the proposed lower fees would continue to pay the current fee applicable to Retail

¹⁵ Pursuant to Section I. of the Fee Schedule, the term "CADV" means, unless otherwise stated, the United States consolidated average daily volume of transactions reported to a securities information processor ("SIP"). Transactions that are not reported to a SIP are not included in the CADV. If CADV is preceded by a reference to a Tape or to Sub-Dollar, then CADV would refer to all consolidated average daily volume of transactions reported to a SIP for all securities in that Tape or to all Sub-Dollar securities.

¹⁶ 15 U.S.C. 78f(b).

¹⁷ 15 U.S.C. 78f(b)(4) and (5).

¹⁸ See Regulation NMS, *supra* note 6, 70 FR at 37499.

¹⁹ See Securities Exchange Act Release No. 51808, 84 FR 5202, 5253 (February 20, 2019) (File No. S7-05-18) (Final Rule).

²⁰ See Cboe U.S. Equities Market Volume Summary, available at https://markets.cboe.com/us/equities/market_share. See generally <https://www.sec.gov/fast-answers/divisionsmarketregmrexchangesshtml.html>.

²¹ See FINRA ATS Transparency Data, available at <https://otctransparency.finra.org/otctransparency/AtsIssueData>. A list of alternative trading systems registered with the Commission is available at <https://www.sec.gov/foia/docs/atstlist.htm>.

²² See Cboe Global Markets U.S. Equities Market Volume Summary, available at http://markets.cboe.com/us/equities/market_share/.

Orders in Sub-Dollar Securities that remove liquidity. The proposed new pricing tier would create an added financial incentive for ETP Holders to bring additional retail flow to a public market. The proposed new pricing tier is also reasonable because it would reduce the costs of ETP Holders that represent retail flow and potentially also reduce costs to their customers.

The Exchange believes that it is reasonable that only Retail Orders in Sub-Dollar Securities with a time-in-force designation of Day that remove liquidity would count toward qualifying for the Sub-Dollar Retail Day Remove Tier. The Exchange notes that it currently offers lower fees for Retail Orders with a time-in-force of Day that remove liquidity in securities with a per share price of \$1.00 or above under Retail Tiers 1, 2, and 3 and under Retail Step-Up Tier.²³ The Exchange believes that the proposed volume requirement to qualify for the proposed lower fee is reasonable because it is within a range that the Exchange believes would continue to incentivize ETP Holders to submit Retail Orders in Sub-Dollar Securities to the Exchange to qualify for the proposed lower fee.

The Proposed Fee Change is an Equitable Allocation of Credits and Fees MPL Orders

The Exchange believes that the adoption of increased credits under MPL Tiers 1, 2, 3 and 4 is equitable because the magnitude of the additional credit is not unreasonably high in comparison to the credit paid with respect to other pricing tiers on the Exchange, and in comparison to the credits paid by other exchanges for orders that provide midpoint liquidity. For example, ETP Holders currently receive credits in Tape A, Tape B and Tape C securities that range between \$0.0010 per share and \$0.0038 per share under Standard and Tiered rates. With respect to credits paid by the Exchange's competitors, the Nasdaq Stock Market LLC provides a credit of \$0.0028 per share to add non-displayed midpoint liquidity in Tape A, Tape B and Tape C Securities on that market for firms that add midpoint liquidity that represents 0.30% TCV or more.²⁴ NYSE American LLC, an affiliate of the Exchange, also currently provides a credit of \$0.0030 per share to add MPL liquidity on that market for members

that add greater than 3.5 million shares.²⁵

The Exchange believes the proposed rule change would improve market quality for all market participants on the Exchange and, as a consequence, attract more liquidity to the Exchange thereby improving market-wide quality. ETP Holders that currently qualify for credits associated with MPL Orders will continue to receive credits when they provide liquidity to the Exchange. The Exchange believes that recalibrating the credits for providing liquidity will continue to attract order flow and liquidity to the Exchange, thereby providing additional price improvement opportunities on the Exchange and benefiting investors generally. As to those market participants that do not presently qualify for the credits associated with MPL Orders, the proposal will not adversely impact their existing pricing or their ability to qualify for other credits provided by the Exchange.

Sub-Dollar Retail Day Remove Tier

The Exchange believes that the proposed adoption of the Sub-Dollar Retail Day Remove pricing tier is equitable. The proposed new pricing tier is intended to provide ETP Holders an incentive to send a greater number of Retail Orders in Sub-Dollar Securities to the Exchange in order to pay a lower fee for such orders when removing liquidity from the Exchange, thereby increasing the number of orders that are executed on the Exchange, promoting price discovery and transparency and enhancing order execution opportunities and improving overall liquidity on a public exchange. The Exchange also believes that the proposed change is equitable because the proposed new pricing tier would apply to all similarly situated ETP Holders that remove liquidity. As previously noted, the Exchange operates in a competitive environment, particularly as it relates to attracting Retail Orders to the Exchange.

The Exchange believes that a number of ETP Holders could qualify for the proposed lower fee based on their current trading profile on the Exchange if they choose to direct more of their order flow to the Exchange. However, without having a view of an ETP Holder's activity on other exchanges and off-exchange venues, the Exchange has no way of knowing whether this proposed rule change would result in

any ETP Holder directing Retail Orders to the Exchange in order to qualify for the proposed lower fee. The Exchange believes the proposed rule change would improve market quality for all market participants on the Exchange and, as a consequence, attract more Retail Orders to the Exchange, thereby improving market-wide quality and price discovery.

The Exchange also believes the proposed Sub-Dollar Retail Day Remove Tier is equitable and not unfairly discriminatory because it is available to all ETP Holders on an equal basis. The Exchange does not believe that it is unfairly discriminatory to offer lower fees to ETP Holders as these participants would be subject to meeting prescribed volume requirements. The Exchange believes that the proposed rule change is also equitable and not unfairly discriminatory because maintaining or increasing the proportion of Retail Orders in exchange-listed securities that are executed on a registered national securities exchange (rather than relying on certain available off-exchange execution methods) would contribute to investors' confidence in the fairness of their transactions and would benefit all investors by deepening the Exchange's liquidity pool, supporting the quality of price discovery, promoting market transparency and improving investor protection.

The Proposed Fee Change Is Not Unfairly Discriminatory MPL Orders

The Exchange believes that the adoption of increased credits under MPL Tiers 1, 2, 3 and 4 is not unfairly discriminatory. Moreover, the proposed higher credits neither targets nor will it have a disparate impact on any particular category of market participant. The Exchange believes it is not unfairly discriminatory to provide the increased per share credits under MPL Tiers 1, 2, 3, and 4 as each such credit would be provided on an equal basis to all ETP Holders that add liquidity by meeting the volume requirement of MPL Tiers 1, 2, 3, and 4. The Exchange believes the proposed increased per share credits would incentivize ETP Holders to send more of their MPL Orders to the Exchange to qualify for such credits. The proposed higher credits would apply equally to all ETP Holders as each would be required to provide liquidity in MPL Orders for Tape A, Tape B and Tape C Securities combined during the billing month regardless of whether an ETP Holder currently meets the requirement of another pricing tier.

²³ See Fee Schedule, Retail Tiers under Section VII. Tier Rates—Round Lots and Odd Lots (Per Share Price \$1.00 or Above).

²⁴ See Rebate to Add Non-Displayed Midpoint Liquidity, at <http://nasdaqtrader.com/Trader.aspx?id=PriceListTrading2>.

²⁵ See Standard Rates under I. Transaction Fees (other than for Transactions by an eDMM in Securities Assigned to an eDMM), at https://www.nyse.com/publicdocs/nyse/markets/nyse-american/NYSE_America_Equities_Price_List.pdf.

Sub-Dollar Retail Day Remove Tier

The Exchange believes that the adoption of the proposed Sub-Dollar Retail Day Remove pricing tier is not unfairly discriminatory. The Exchange also believes that the proposal to adopt a volume requirement to qualify for the proposed fee reduction is not unfairly discriminatory. In the prevailing competitive environment, ETP Holders are free to disfavor the Exchange's pricing if they view the proposed fee as excessive. Moreover, the proposal neither targets nor will it have a disparate impact on any particular category of market participant. The Exchange believes that the proposed rule change will incentivize ETP Holders to direct a greater number of Retail Orders to a public exchange to qualify for the proposed reduced fee for removing liquidity, thereby promoting price discovery and transparency and enhancing order execution opportunities for ETP Holders. The proposal does not permit unfair discrimination because the proposed volume requirement for removing liquidity would be applied to all similarly situated ETP Holders, who would all be eligible to pay a reduced fee on an equal basis. Accordingly, no ETP Holder already operating on the Exchange would be disadvantaged by this allocation of fees. The Exchange believes it is not unfairly discriminatory to provide lower fees for removing liquidity as the proposed fee would be provided on an equal basis to all ETP Holders that remove liquidity by meeting the proposed volume requirement. Further, the Exchange believes the proposed reduced fee would provide an incentive for ETP Holders to execute more of their Retail Orders on the Exchange.

Finally, the submission of orders to the Exchange is optional for ETP Holders in that they could choose whether to submit orders to the Exchange and, if they do, the extent of its activity in this regard. The Exchange believes that it is subject to significant competitive forces, as described below in the Exchange's statement regarding the burden on competition.

For the foregoing reasons, the Exchange believes that the proposal is consistent with the Act.

B. Self-Regulatory Organization's Statement on Burden on Competition

In accordance with Section 6(b)(8) of the Act,²⁶ the Exchange believes that the proposed rule change would not impose any burden on competition that is not

necessary or appropriate in furtherance of the purposes of the Act. Instead, as discussed above, the Exchange believes that the proposed changes would encourage the submission of additional liquidity to a public exchange, thereby promoting market depth, price discovery and transparency and enhancing order execution opportunities for ETP Holders. As a result, the Exchange believes that the proposed change furthers the Commission's goal in adopting Regulation NMS of fostering integrated competition among orders, which promotes "more efficient pricing of individual stocks for all types of orders, large and small."²⁷

Intramarket Competition. The proposed changes are designed to attract additional order flow to the Exchange. The Exchange believes that the adoption of higher credits under MPL Tiers 1, 2, 3 and 4, would continue to incentivize market participants to direct more orders to the Exchange, and in particular, liquidity-providing MPL Orders. Greater liquidity benefits all market participants on the Exchange by providing more trading opportunities. The proposed changes to the MPL Order pricing tiers should incentivize ETP Holders to send liquidity-providing orders to the Exchange, thereby contributing to robust levels of liquidity, which would benefit all market participants on the Exchange. The proposed higher credits would be available to all similarly-situated market participants, and, as such, the proposed changes would not impose a disparate burden on competition among market participants on the Exchange. The proposed rule change is also designed to attract Retail Orders in Sub-Dollar Securities to the Exchange. The Exchange believes that the proposed change would incentivize market participants to direct retail order flow to a public market. Greater overall order flow, trading opportunities, and pricing transparency would benefit all market participants on the Exchange by enhancing market quality and would continue to encourage ETP Holders to send their orders to the Exchange, thereby contributing towards a robust and well-balanced market ecosystem. The proposed fee reduction would be available to all similarly situated market participants, and, as such, the proposed change would not impose a disparate burden on competition among market participants on the Exchange. Additionally, the proposed change would apply to all ETP Holders equally

in that all ETP Holders would have a reasonable opportunity to meet the volume requirement to qualify for the proposed fee reduction and would pay a lower fee for removing liquidity if such criteria is met.

Intermarket Competition. The Exchange operates in a highly competitive market in which market participants can readily choose to send their orders to other exchange and off-exchange venues if they deem fee levels at those other venues to be more favorable. As noted above, the Exchange's market share of intraday trading (*i.e.*, excluding auctions) is currently less than 12%. In such an environment, the Exchange must continually review, and consider adjusting its fees and rebates to remain competitive with other exchanges and with off-exchange venues. Because competitors are free to modify their own fees and credits in response, the Exchange does not believe its proposed fee change can impose any burden on intermarket competition.

The Exchange believes that the proposed changes could promote competition between the Exchange and other execution venues, including those that currently offer similar order types and comparable transaction pricing, by encouraging additional orders to be sent to the Exchange for execution.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

No written comments were solicited or received with respect to the proposed rule change.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Pursuant to Section 19(b)(3)(A)(ii) of the Act,²⁸ and Rule 19b-4(f)(2) thereunder²⁹ the Exchange has designated this proposal as establishing or changing a due, fee, or other charge imposed on any person, whether or not the person is a member of the self-regulatory organization, which renders the proposed rule change effective upon filing. At any time within 60 days of the filing of the proposed rule change, the Commission summarily may temporarily suspend such rule change if it appears to the Commission that such action is necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of the Act.

²⁶ 15 U.S.C. 78f(b)(8).

²⁷ See Regulation NMS, *supra* note 6, 70 FR 37498-99.

²⁸ 15 U.S.C. 78s(b)(3)(A)(ii).

²⁹ 17 CFR 240.19b-4.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views, and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-NYSEARCA-2024-85 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

All submissions should refer to file number SR-NYSEARCA-2024-85. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549 on official business days between the hours of 10:00 a.m. and 3:00 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR-NYSEARCA-2024-85, and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.³⁰

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2024-25049 Filed 10-28-24; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-101421; File No. SR-C2-2024-016]

Self-Regulatory Organizations; Cboe C2 Exchange, Inc.; Notice of Filing of a Proposed Rule Change With Respect to Amendments to the Seventh Amended and Restated Bylaws (the "CGM Bylaws") of its Parent Corporation, Cboe Global Markets, Inc. ("Cboe" or "Corporation")

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (the "Act"),¹ and Rule 19b-4 thereunder,² notice is hereby given that on October 11, 2024, Cboe C2 Exchange, Inc. (the "Exchange" or "C2") filed with the Securities and Exchange Commission ("Commission") the proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization's Statement of the Terms of Substance of the Proposed Rule Change

Cboe C2 Exchange, Inc. (the "Exchange" or "C2") is filing with the Securities and Exchange Commission (the "Commission") a proposed rule change with respect to amendments to the Seventh Amended and Restated Bylaws (the "CGM Bylaws") of its parent corporation, Cboe Global Markets, Inc. ("Cboe" or "Corporation"). The text of the proposed rule change is provided in Exhibit 5.

The text of the proposed rule change is also available on the Exchange's website (http://markets.cboe.com/us/options/regulation/rule_filings/ctwo/), at the Exchange's Office of the Secretary, and at the Commission's Public Reference Room.

³⁰ 17 CFR 200.30-3(a)(12).

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

II. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the Exchange included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

At Cboe's annual meeting held on May 16, 2024, Cboe's stockholders considered two advisory proposals that would provide Cboe stockholders with the right to call a special meeting of the stockholders provided that a certain threshold percentage of stockholders propose to call such a meeting. The two proposals were submitted separately. One of the proposals was submitted by an individual stockholder ("Stockholder Proposal"). The other proposal was submitted by Cboe Management ("Management Proposal"). The Stockholder Proposal, which did not pass but received 45% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 10% of Cboe's voting power to call a special meeting of the stockholders. The Management Proposal, which passed with 65% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 25% of Cboe's voting power to call a special meeting of the stockholders.

The Nominating & Governance Committee of the CGM Board reviewed the voting results of the Stockholder Proposal and the Management Proposal and discussed the stockholder voting standards and rights contemplated by the CGM Bylaws. Following this review, the Nominating & Governance Committee recommended to the CGM Board, and the CGM Board approved, certain changes to the CGM Bylaws to implement the Management Proposal. The CGM Board also approved amending the CGM Bylaws to improve the governance processes of Cboe, to make certain provisions more consistent with Delaware General Corporation Law ("DGCL"), and to make clarifying and cleanup changes to the CGM Bylaws. The proposed rule change amends the

CGM Bylaws to implement the changes approved by the CGM Board.

Proposed Changes to Article 2— Stockholders

Current Section 2.3 (Special Meeting) of the CGM Bylaws provides that only the Chair of the Board, the Chief Executive Officer or the CGM Board may call a special meeting of the stockholders. To respond to feedback from its stockholders, as discussed above, Cboe proposes to delete portions of this provision and add language that will provide Cboe stockholders with the right to call special stockholder meetings (a “Stockholder Requested Special Meeting”) after following particular procedures.

In defining the procedural requirements, Cboe’s goals are to ensure timely notice of a meeting request and to gather sufficient information about the proposing stockholder(s) and the proposed business itself. Among other things, this information will help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to adequately assess proposed business submitted by stockholders. Additionally, Cboe notes that the proposed terms are common among public companies that have adopted a right for stockholders to call special meetings. The proposed changes to the CGM Bylaws to effect the stockholder special meeting right are set forth below.

Revisions to Section 2.3(a)

First, the proposed changes to Section 2.3(a) provide that a Stockholder Requested Special Meeting may be called: (i) at any time by the CGM Board pursuant to a resolution adopted by the affirmative vote of a majority of the total number of CGM directors then in office; or (ii) by Cboe’s Corporate Secretary following the receipt of a written request in proper form for a special meeting (a “Special Meeting Request”) by one or more stockholders. In order to call a special meeting, the stockholders must hold, in the aggregate, at least 25% of Cboe’s outstanding shares of common stock entitled to vote on matters brought before the special meeting (the “Requisite Percentage”).

The proposed changes to Section 2.3(a) also clarify that the Chair of the Board, the Chief Executive Officer or the President of Cboe may not individually call a special meeting of the stockholders. This change was made to vest authority within Cboe to call a special meeting in the Board. Without the proposed change, the Chair of the Board, Chief Executive Officer and the

President could each call a special meeting of the stockholders without CGM Board approval. The proposed change to Section 2.3(a) simplifies this requirement to confirm that, within Cboe, only the CGM Board may call for a special meeting of the stockholders.

Proposed Section 2.3(b) and Section 2.3(c)

Proposed Section 2.3(b) and Section 2.3(c) set forth the procedures a stockholder must follow in order to submit a written request in proper form to call a Stockholder Requested Special Meeting. Stockholders must first submit a request to Cboe’s Corporate Secretary to define a date on which the Requisite Percentage will be determined (the “Record Date”). A stockholder must sign any request to set a Record Date and also provide a reasonably brief description of the purpose or purposes of the special meeting of the stockholders. A stockholder is also required in the request to set a Record Date to disclose certain information regarding themselves and any individuals or entities such stockholder may be associated with (a “Stockholder Associated Person(s)”), as well as such information concerning any nominees to the CGM Board (“Stockholder Nominee(s)”) if such stockholder is so proposing. The information that a stockholder must disclose regarding Stockholder Associated Persons and Stockholder Nominees is contained in Section 2.11 of the CGM Bylaws and incorporated by reference in this Section 2.3(b). The information required to be provided in the request to set a Record Date provides Cboe with notice that a stockholder is seeking to bring business before the stockholders and assists with the logistical aspects of determining which stockholders will be counted for purposes of determining whether the Requisite Percentage is met.

Proposed Section 2.3(d) and Section 2.3(e)

Proposed Section 2.3(d) and Section 2.3(e) include detailed information on the requirements for a Special Meeting Request to have been properly delivered, subject to certain carve-outs for stockholders who submit their request in response to a solicitation for public consent by the Corporation made pursuant to Section 14 of the Exchange Act. Specifically, a Special Meeting Request must:

- be delivered within 60 days following the Record Date;
- be signed by each stockholder making up the Requisite Percentage;

- contain a reasonably brief description of the purpose of the special meeting;

- include details of each stockholder holding the Requisite Percentage, including:

- The stockholder’s name;
- The stockholder’s address;
- information concerning the stockholder submitting the Special Meeting Request and any Stockholder Associated Persons;
- information concerning any Stockholder Nominees; and
- documentary evidence that the shares included in the Requisite Percentage are owned by such stockholder;

- include an acknowledgment that any reduction in the number of shares owned by such stockholders as of the date of such Special Meeting Request and through the meeting date will constitute a revocation of such Special Meeting Request with respect to such reduction;

- relate to an item of business that is a proper subject for stockholder action under applicable law;

- not include an item of business that did not appear on the request to set a Record Date;

- not be delivered during the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting and ending on the date of the next annual meeting; and

- otherwise comply with applicable law.

In defining the requirements for a Special Meeting Request, Cboe’s goal is to gather sufficient information about the stockholder seeking to request a special meeting and the proposed business for both itself and its stockholders and to help ensure the efficient use of corporate resources by restricting a stockholder from raising items that could reasonably be addressed at an annual meeting of the stockholders, as in the requirement that a Special Meeting Request not be delivered in the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting. Overall, this information is designed to help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to assess the proposed business or Stockholder Nominee adequately.

Proposed Section 2.3(f)

Proposed Section 2.3(f) provides that the CGM Board may cancel a special meeting in its discretion if the

percentage of stock held by the stockholders requesting a special meeting falls below the Requisite Percentage at any point after sixty (60) days from the first date on which a valid Special Meeting Request is delivered to Cboe. This provides the CGM Board with discretion to reevaluate the Special Meeting Request in the event the Special Meeting Request is revoked by stockholders holding a sufficient percentage of the stock of the Corporation.

Proposed Section 2.3(g)

Proposed Section 2.3(g) provides that within ten (10) days following the date on which the Secretary has received valid Special Meeting Requests, the CGM Board shall fix the record date and meeting date, time and location for the Stockholder Requested Special Meeting, provided that the date of any such Stockholder Requested Special Meeting shall not be more than ninety (90) days after the date on which a valid Special Meeting Request is received by Cboe. The CGM Board may submit its own proposal or proposals for consideration at any Stockholder Requested Special Meeting. Ninety (90) days allows the Corporation reasonable time to assess the items proposed in the Special Meeting Request while also not imposing a potentially burdensome delay on the stockholders.

Proposed Section 2.3(h)

Proposed Section 2.3(h) provides that multiple Special Meeting Requests may be considered together if (i) each Special Meeting Request identifies the same or substantially the same purpose or purposes of the Stockholder Requested Special Meeting and the same or substantially the same items of business proposed to be brought before the Stockholder Requested Special Meeting, and (ii) such Special Meeting Requests have been dated and delivered to the Corporate Secretary within sixty (60) days of the delivery to the Corporate Secretary of the earliest dated Special Meeting Request relating to such item(s) of business. This proposed section helps to ensure the efficient use of corporate resources by preventing multiple stockholders from raising items that should reasonably be consolidated. The conditions under which the Corporation may combine multiple Special Meeting Requests are sufficiently limited to require that each unique item is addressed separately.

Revisions to Section 2.9

Section 2.9 of the CGM Bylaws governs proxy representation. It is proposed that language be added to

clarify that any stockholder directly or indirectly soliciting proxies from other stockholders of the Corporation may use any proxy card color other than white, which shall be reserved for exclusive use by the CGM Board.

Revisions to Section 2.11

Section 2.11 of the CGM Bylaws, which are the “advance notice bylaws,”³ requires stockholders to notify Cboe, during a specified period in advance of an annual meeting or special meeting called by the CGM Board, of their intention to nominate one or more persons for election to the CGM Board or to present a business proposal for consideration by the stockholders at the meeting and provide certain information regarding such request. When designing the proposed procedural requirements for stockholders to call a special meeting, as outlined above, Cboe evaluated the existing procedural requirements for stockholders to bring business before an annual meeting or to nominate director candidates at an annual meeting or special meeting. Cboe has determined that the advance notice bylaws may be enhanced to help achieve the core objectives of fulsome disclosure and accurate explanations from stockholders bringing business or potential nominees before a stockholder meeting. While advance notice bylaws are beneficial in providing a company and its stockholders with information regarding stockholders, and their Stockholder Associated Persons, seeking to bring business or potential nominees before a stockholder meeting, therefore permitting orderly meetings and election contests, and assisting the board’s information gathering and disclosure functions, the Delaware Supreme Court in *Kellner v. AIM ImmunoTech Inc.*⁴ has recently provided some guidance on circumstances where such requests may be overbroad or request information not sufficiently connected to the legitimate information gathering function these provisions serve. Therefore, as further detailed below, Cboe has determined that it would be beneficial to refine certain of the provisions in the CGM Bylaws to increase the clarity of the requests for information from

³ “Advance notice bylaws” allow stockholder(s) to bring business before an annual or special meeting of stockholders, but set forth procedural requirements to help ensure that companies and boards have sufficient information about the proposal and the proposing stockholder(s), as well as adequate time to consider the proposal, by requiring the proposing stockholder(s) to give advance notice of the intention to bring the proposal before the annual or special meeting.

⁴ *Kellner v. AIM ImmunoTech Inc.*, C. A. 2023–0879–LWW (Del. Ch. Jan. 5, 2024).

stockholders seeking to bring business before a meeting.

First, Section 2.11(a)(iii)(C) of the CGM Bylaws currently defines the information required to be disclosed regarding a stockholder providing notice of nominations or other business, any Stockholder Associated Person(s) and any Stockholder Nominee(s). Cboe proposes certain amendments to this section to (i) clarify the information a stockholder is required to disclose relating to arrangements between the stockholder providing notice or any Stockholder Associated Person and any other stockholder with regard to the stockholder meeting and (ii) eliminate disclosures on performance related fees to which such stockholder or Stockholder Associated Person may be entitled as a result of any increase or decrease in the stock of Cboe, and the prospectus or similar document of the stockholder providing notice or any Stockholder Associated Person. Cboe believes that, while these provisions as currently written provide valuable information to the Corporation and its stockholders in assessing the proposed business or Stockholder Nominee, these requirements should be sufficiently specific so as not to potentially dissuade stockholders from bringing business before a stockholder meeting and should otherwise comply with Delaware law. The proposed changes narrow the information required to be disclosed such that Cboe is able to help ensure the objectives of the provisions are met without burdening stockholders with potentially overbroad requests for information.

Section 2.11(a)(iii)(D) of the CGM Bylaws currently sets forth certain representations that must be made by a stockholder seeking to bring business or a Stockholder Nominee before a stockholder meeting regarding whether such stockholder is part of a group which intends to deliver or solicit proxies from stockholders in support of such proposed business. Cboe proposes changes to update this section in order to be more consistent with the universal proxy rules provided for in Rule 14a–19 of the Exchange Act by explicitly stating that any stockholder providing notice that they intend to solicit proxies in support of a proposed nominee must do so in accordance with Rule 14a–19 of the Exchange Act. Cboe also proposes to clarify that the representation must confirm whether the stockholder intends or is part of a group which intends to engage in a solicitation (within the meaning of Rule 14a–1(1) of the Exchange Act) with respect to the nomination of any proposed nominee or

proposed business to be considered at the meeting.

Section 2.11(a)(iii)(F) of the CGM Bylaws currently requires that a Stockholder Nominee furnish any information that Cboe may determine is required for Cboe to determine the qualifications of such Stockholder Nominee to serve as a director of the Corporation. Cboe proposes to add language clarifying that the information Cboe may require must be consistent with the parameters set forth in Cboe's Corporate Governance Guidelines or the CGM Board's past practice in evaluating potential director nominees.

Proposed Section 2.11(c)(ii) of the CGM Bylaws requires the stockholder providing notice to notify the Secretary of any inaccuracy or change in any information submitted pursuant to Section 2.11 within two (2) business days of becoming aware of such inaccuracy or change. Cboe proposes to modify this requirement by narrowing the scope of circumstances in which a stockholder is required to provide notice of any inaccuracy or change of information that they have previously provided to material inaccuracies or changes.

Proposed Section 2.11(c)(iii) of the CGM Bylaws provides that any stockholder or Stockholder Associated Person providing notice with respect to any Stockholder Nominee is required to do so in a manner consistent with the requirements for universal proxy rules pursuant to Rule 14a–19 of the Exchange Act. Namely, the nomination of a Stockholder Nominee shall be disregarded if, among other things, there is no longer an intent to solicit proxies in support of a Stockholder Nominee or there is a failure to comply with the applicable requirements of Rule 14a–19. Upon request by the Corporation, if any stockholder providing notice or any Stockholder Associated Person provides notice pursuant to Rule 14a–19(b) under the Exchange Act, such stockholder providing notice shall deliver to the Corporate Secretary, no later than five (5) business days prior to the applicable meeting date, then reasonable evidence that the requirements of Rule 14a–19(a)(3) under the Exchange Act have been satisfied.

Currently Section 2.11(c)(vi) of the CGM Bylaws defines "Stockholder Associated Person" to mean, among other things, (i) any person who is a member of a "group" (used in Rule 13d–5 under the Exchange Act) with, or otherwise acting in concert with, any stockholder providing notice, (ii) any person that is directly or indirectly controlled by, or under common control with, such stockholder or such

Stockholder Associated Person, or (iii) any person directly or indirectly controlling any such stockholder or any Stockholder Associated Person. The proposed rule change reflects recent developments in Delaware law to add specificity to the definition and limit which individuals may be determined to be a Stockholder Associated Person and makes other clarifying changes. Specifically, the proposed rule change adds the qualifier that a Stockholder Associated Person must be known by the stockholder to be acting in concert with such stockholder, removes from the definition any person directly or indirectly controlled by, or under common control with such stockholder and replaces it with any affiliate or associate of such stockholder providing notice, and deletes the reference in the definition to any person directly or indirectly controlling any such stockholder or Stockholder Associated Person. The proposed rule change also adds any Stockholder Nominee to the definition of Stockholder Associated Person.

Revisions to Other Sections of the Bylaws

Cboe also proposes to make changes to Section 2.11 to reflect recent developments in Delaware law and to provide clarifications and prevent confusion. Cboe proposes to add a note to Section 2.11(a)(ii) that any proposed business for a stockholder meeting must be a proper matter for stockholder action. Cboe also proposes to amend Section 2.11(a)(iii)(B) to state that a Stockholder Nominee's written consent must be included in Cboe's proxy statement before they may be brought before a meeting. Previously, Section 2.11(a)(iii)(B) had stated that the Stockholder Nominee's written consent must be included in a proxy statement, but had not specifically defined it as Cboe's proxy statement. Cboe also proposes to amend the same section to state that a Stockholder Nominee will not enter into any commitment to vote in a certain manner if nominated to the CGM Board. Previously, this section had simply stated that a Stockholder Nominee may not enter into any commitment to vote in a certain manner with respect to certain matters at any company, without defining Cboe specifically. Cboe also proposes to amend the same section to require that a Stockholder Nominee not omit facts that are necessary to ensure statements made are not misleading in any material respect. Previously, the Stockholder Nominee's responsibility to not omit facts that are necessary to ensure

statements are not misleading was not subject to materiality.

Cboe also proposes to make changes to Section 3.10 of the CGM Bylaws to provide that the Lead Director of Cboe may call a special meeting of the CGM Board. Section 3.10 currently permits, among other things, the Chair of the Board or the Chief Executive Officer to call a special meeting of the CGM Board. Revising this section to allow the Lead Director to call a special meeting of the CGM Board addresses a potential scenario in which the Chair of the Board and the Chief Executive Officer positions are jointly held by one individual and a special meeting of the CGM Board is not able to be called by individual independent directors.

2. Statutory Basis

The Exchange believes the proposed rule change is consistent with the Act and the rules and regulations thereunder applicable to the Exchange and, in particular, the requirements of Section 6(b) of the Act.⁵ Specifically, the Exchange believes the proposed rule change is consistent with the Section 6(b)(5)⁶ requirements that the rules of an exchange be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.

In light of an advisory vote by the stockholders of Cboe, Cboe is proposing changes to its Bylaws to implement a right for stockholders to call a special meeting of the stockholders at a 25% threshold. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) of the Act because the proposed rule change would be consistent with and facilitate a governance and regulatory structure that is designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to, and perfect the mechanism of a free and open market and a national market system and, in general, to protect investors and the

⁵ 15 U.S.C. 78f(b).

⁶ 15 U.S.C. 78f(b)(5).

public interest. Particularly, the Exchange believes that, by permitting stockholders of Cboe to bring business or Stockholder Nominees before a special meeting, the proposed rule change strengthens the corporate governance of the Exchange's ultimate parent company, which is beneficial to both investors and the public interest.

Additionally, the procedural requirements are designed to help protect investors by stating clearly and explicitly the procedures stockholders must follow in order to bring business or Stockholder Nominees before a special meeting. The informational requirements are designed to enhance investor protection by helping to ensure among other things, that the Corporation and its stockholders have full and accurate information about nominating stockholders and Stockholder Nominees and that such stockholders and nominees comply with applicable laws, regulations and other requirements.

The changes that the Exchange is proposing with regard to so-called "advance notice bylaws" in light of the recent developments in Delaware law are designed to help provide additional clarity to stockholders wishing to bring business before a stockholder meeting or propose a Stockholder Nominee. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) by simplifying the requirements and clarifying the information that must be disclosed by stockholders. This furthers the interests of investors and the public by removing potential impediments to raising business or proposing Stockholder Nominees that may otherwise restrict a stockholder's ability to participate in the corporate governance of the Corporation.

Finally, the remaining changes to existing provisions of the CGM Bylaws are clarifying in nature, and they enhance investor protection and the public interest by preventing confusion with respect to the operation of the Bylaw provisions.

B. Self-Regulatory Organization's Statement on Burden on Competition

Because the proposed rule change relates to the governance of the Corporation and not to the operations of the Exchange, the Exchange does not believe that the proposed rule change will impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. The proposed rule change is not designed to address any competitive issue or have any impact on competition; rather, adoption of a stockholder special meeting provision, updating "advance notice bylaws," and

other bylaws updates by the Corporation are intended to enhance corporate governance and accountability to stockholders.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

The Exchange neither solicited nor received comments on the proposed rule change.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the Exchange consents, the Commission will:

- A. by order approve or disapprove such proposed rule change, or
- B. institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-C2-2024-016 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.
- All submissions should refer to file number SR-C2-2024-016. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the

proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR-C2-2024-016 and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁷

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2024-25059 Filed 10-28-24; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-101417; File No. SR-CboeEDGX-2024-059]

Self-Regulatory Organizations; Cboe EDGX Exchange, Inc.; Notice of Filing of a Proposed Rule Change With Respect to Amendments to the Seventh Amended and Restated Bylaws (the "CGM Bylaws") of Its Parent Corporation, Cboe Global Markets, Inc. ("Cboe" or "Corporation")

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (the "Act"),¹ and Rule 19b-4 thereunder,² notice is hereby given that on October 11, 2024, Cboe EDGX Exchange, Inc. (the "Exchange" or "EDGX") filed with the Securities and Exchange Commission ("Commission") the proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

⁷ 17 CFR 200.30-3(a)(12).

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

I. Self-Regulatory Organization's Statement of the Terms of Substance of the Proposed Rule Change

Cboe EDGX Exchange, Inc. (the "Exchange" or "EDGX") is filing with the Securities and Exchange Commission (the "Commission") a proposed rule change with respect to amendments to the Seventh Amended and Restated Bylaws (the "CGM Bylaws") of its parent corporation, Cboe Global Markets, Inc. ("Cboe" or "Corporation"). The text of the proposed rule change is provided in Exhibit 5.

The text of the proposed rule change is also available on the Exchange's website (http://markets.cboe.com/us/options/regulation/rule_filings/edgx/), at the Exchange's Office of the Secretary, and at the Commission's Public Reference Room.

II. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the Exchange included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

At Cboe's annual meeting held on May 16, 2024, Cboe's stockholders considered two advisory proposals that would provide Cboe stockholders with the right to call a special meeting of the stockholders provided that a certain threshold percentage of stockholders propose to call such a meeting. The two proposals were submitted separately. One of the proposals was submitted by an individual stockholder ("Stockholder Proposal"). The other proposal was submitted by Cboe Management ("Management Proposal"). The Stockholder Proposal, which did not pass but received 45% of the votes cast, requested that the CGM Board take steps to enable stockholders having at least 10% of Cboe's voting power to call a special meeting of the stockholders. The Management Proposal, which passed with 65% of the votes cast, requested that the CGM Board take steps to enable

stockholders having at least 25% of Cboe's voting power to call a special meeting of the stockholders.

The Nominating & Governance Committee of the CGM Board reviewed the voting results of the Stockholder Proposal and the Management Proposal and discussed the stockholder voting standards and rights contemplated by the CGM Bylaws. Following this review, the Nominating & Governance Committee recommended to the CGM Board, and the CGM Board approved, certain changes to the CGM Bylaws to implement the Management Proposal. The CGM Board also approved amending the CGM Bylaws to improve the governance processes of Cboe, to make certain provisions more consistent with Delaware General Corporation Law ("DGCL"), and to make clarifying and cleanup changes to the CGM Bylaws. The proposed rule change amends the CGM Bylaws to implement the changes approved by the CGM Board.

Proposed Changes to Article 2—Stockholders

Current Section 2.3 (Special Meeting) of the CGM Bylaws provides that only the Chair of the Board, the Chief Executive Officer or the CGM Board may call a special meeting of the stockholders. To respond to feedback from its stockholders, as discussed above, Cboe proposes to delete portions of this provision and add language that will provide Cboe stockholders with the right to call special stockholder meetings (a "Stockholder Requested Special Meeting") after following particular procedures.

In defining the procedural requirements, Cboe's goals are to ensure timely notice of a meeting request and to gather sufficient information about the proposing stockholder(s) and the proposed business itself. Among other things, this information will help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to adequately assess proposed business submitted by stockholders. Additionally, Cboe notes that the proposed terms are common among public companies that have adopted a right for stockholders to call special meetings. The proposed changes to the CGM Bylaws to effect the stockholder special meeting right are set forth below.

Revisions to Section 2.3(a)

First, the proposed changes to Section 2.3(a) provide that a Stockholder Requested Special Meeting may be called: (i) at any time by the CGM Board pursuant to a resolution adopted by the

affirmative vote of a majority of the total number of CGM directors then in office; or (ii) by Cboe's Corporate Secretary following the receipt of a written request in proper form for a special meeting (a "Special Meeting Request") by one or more stockholders. In order to call a special meeting, the stockholders must hold, in the aggregate, at least 25% of Cboe's outstanding shares of common stock entitled to vote on matters brought before the special meeting (the "Requisite Percentage").

The proposed changes to Section 2.3(a) also clarify that the Chair of the Board, the Chief Executive Officer or the President of Cboe may not individually call a special meeting of the stockholders. This change was made to vest authority within Cboe to call a special meeting in the Board. Without the proposed change, the Chair of the Board, Chief Executive Officer and the President could each call a special meeting of the stockholders without CGM Board approval. The proposed change to Section 2.3(a) simplifies this requirement to confirm that, within Cboe, only the CGM Board may call for a special meeting of the stockholders.

Proposed Section 2.3(b) and Section 2.3(c)

Proposed Section 2.3(b) and Section 2.3(c) set forth the procedures a stockholder must follow in order to submit a written request in proper form to call a Stockholder Requested Special Meeting. Stockholders must first submit a request to Cboe's Corporate Secretary to define a date on which the Requisite Percentage will be determined (the "Record Date"). A stockholder must sign any request to set a Record Date and also provide a reasonably brief description of the purpose or purposes of the special meeting of the stockholders. A stockholder is also required in the request to set a Record Date to disclose certain information regarding themselves and any individuals or entities such stockholder may be associated with (a "Stockholder Associated Person(s)"), as well as such information concerning any nominees to the CGM Board ("Stockholder Nominee(s)") if such stockholder is so proposing. The information that a stockholder must disclose regarding Stockholder Associated Persons and Stockholder Nominees is contained in Section 2.11 of the CGM Bylaws and incorporated by reference in this Section 2.3(b). The information required to be provided in the request to set a Record Date provides Cboe with notice that a stockholder is seeking to bring business before the stockholders and assists with the logistical aspects of

determining which stockholders will be counted for purposes of determining whether the Requisite Percentage is met.

Proposed Section 2.3(d) and Section 2.3(e)

Proposed Section 2.3(d) and Section 2.3(e) include detailed information on the requirements for a Special Meeting Request to have been properly delivered, subject to certain carve-outs for stockholders who submit their request in response to a solicitation for public consent by the Corporation made pursuant to Section 14 of the Exchange Act. Specifically, a Special Meeting Request must:

- be delivered within 60 days following the Record Date;
- be signed by each stockholder making up the Requisite Percentage;
- contain a reasonably brief description of the purpose of the special meeting;
- include details of each stockholder holding the Requisite Percentage, including:
 - The stockholder's name;
 - The stockholder's address;
 - information concerning the stockholder submitting the Special Meeting Request and any Stockholder Associated Persons;
 - information concerning any Stockholder Nominees; and
 - documentary evidence that the shares included in the Requisite Percentage are owned by such stockholder;
- include an acknowledgment that any reduction in the number of shares owned by such stockholders as of the date of such Special Meeting Request and through the meeting date will constitute a revocation of such Special Meeting Request with respect to such reduction;
- relate to an item of business that is a proper subject for stockholder action under applicable law;
- not include an item of business that did not appear on the request to set a Record Date;
- not be delivered during the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting and ending on the date of the next annual meeting; and
- otherwise comply with applicable law.

In defining the requirements for a Special Meeting Request, Cboe's goal is to gather sufficient information about the stockholder seeking to request a special meeting and the proposed business for both itself and its stockholders and to help ensure the efficient use of corporate resources by

restricting a stockholder from raising items that could reasonably be addressed at an annual meeting of the stockholders, as in the requirement that a Special Meeting Request not be delivered in the period commencing 90 days prior to the one-year anniversary of the immediately preceding annual meeting. Overall, this information is designed to help ensure that Cboe is able to comply with its disclosure and other requirements under applicable law and that Cboe, the CGM Board and its stockholders are able to assess the proposed business or Stockholder Nominee adequately.

Proposed Section 2.3(f)

Proposed Section 2.3(f) provides that the CGM Board may cancel a special meeting in its discretion if the percentage of stock held by the stockholders requesting a special meeting falls below the Requisite Percentage at any point after sixty (60) days from the first date on which a valid Special Meeting Request is delivered to Cboe. This provides the CGM Board with discretion to reevaluate the Special Meeting Request in the event the Special Meeting Request is revoked by stockholders holding a sufficient percentage of the stock of the Corporation.

Proposed Section 2.3(g)

Proposed Section 2.3(g) provides that within ten (10) days following the date on which the Secretary has received valid Special Meeting Requests, the CGM Board shall fix the record date and meeting date, time and location for the Stockholder Requested Special Meeting, provided that the date of any such Stockholder Requested Special Meeting shall not be more than ninety (90) days after the date on which a valid Special Meeting Request is received by Cboe. The CGM Board may submit its own proposal or proposals for consideration at any Stockholder Requested Special Meeting. Ninety (90) days allows the Corporation reasonable time to assess the items proposed in the Special Meeting Request while also not imposing a potentially burdensome delay on the stockholders.

Proposed Section 2.3(h)

Proposed Section 2.3(h) provides that multiple Special Meeting Requests may be considered together if (i) each Special Meeting Request identifies the same or substantially the same purpose or purposes of the Stockholder Requested Special Meeting and the same or substantially the same items of business proposed to be brought before the Stockholder Requested Special Meeting,

and (ii) such Special Meeting Requests have been dated and delivered to the Corporate Secretary within sixty (60) days of the delivery to the Corporate Secretary of the earliest dated Special Meeting Request relating to such item(s) of business. This proposed section helps to ensure the efficient use of corporate resources by preventing multiple stockholders from raising items that should reasonably be consolidated. The conditions under which the Corporation may combine multiple Special Meeting Requests are sufficiently limited to require that each unique item is addressed separately.

Revisions to Section 2.9

Section 2.9 of the CGM Bylaws governs proxy representation. It is proposed that language be added to clarify that any stockholder directly or indirectly soliciting proxies from other stockholders of the Corporation may use any proxy card color other than white, which shall be reserved for exclusive use by the CGM Board.

Revisions to Section 2.11

Section 2.11 of the CGM Bylaws, which are the "advance notice bylaws",³ requires stockholders to notify Cboe, during a specified period in advance of an annual meeting or special meeting called by the CGM Board, of their intention to nominate one or more persons for election to the CGM Board or to present a business proposal for consideration by the stockholders at the meeting and provide certain information regarding such request. When designing the proposed procedural requirements for stockholders to call a special meeting, as outlined above, Cboe evaluated the existing procedural requirements for stockholders to bring business before an annual meeting or to nominate director candidates at an annual meeting or special meeting. Cboe has determined that the advance notice bylaws may be enhanced to help achieve the core objectives of fulsome disclosure and accurate explanations from stockholders bringing business or potential nominees before a stockholder meeting. While advance notice bylaws are beneficial in providing a company and its stockholders with information regarding stockholders, and their Stockholder Associated Persons, seeking

³ "Advance notice bylaws" allow stockholder(s) to bring business before an annual or special meeting of stockholders, but set forth procedural requirements to help ensure that companies and boards have sufficient information about the proposal and the proposing stockholder(s), as well as adequate time to consider the proposal, by requiring the proposing stockholder(s) to give advance notice of the intention to bring the proposal before the annual or special meeting.

to bring business or potential nominees before a stockholder meeting, therefore permitting orderly meetings and election contests, and assisting the board's information gathering and disclosure functions, the Delaware Supreme Court in *Kellner v. AIM ImmunoTech Inc.*⁴ has recently provided some guidance on circumstances where such requests may be overbroad or request information not sufficiently connected to the legitimate information gathering function these provisions serve. Therefore, as further detailed below, Cboe has determined that it would be beneficial to refine certain of the provisions in the CGM Bylaws to increase the clarity of the requests for information from stockholders seeking to bring business before a meeting.

First, Section 2.11(a)(iii)(C) of the CGM Bylaws currently defines the information required to be disclosed regarding a stockholder providing notice of nominations or other business, any Stockholder Associated Person(s) and any Stockholder Nominee(s). Cboe proposes certain amendments to this section to (i) clarify the information a stockholder is required to disclose relating to arrangements between the stockholder providing notice or any Stockholder Associated Person and any other stockholder with regard to the stockholder meeting and (ii) eliminate disclosures on performance related fees to which such stockholder or Stockholder Associated Person may be entitled as a result of any increase or decrease in the stock of Cboe, and the prospectus or similar document of the stockholder providing notice or any Stockholder Associated Person. Cboe believes that, while these provisions as currently written provide valuable information to the Corporation and its stockholders in assessing the proposed business or Stockholder Nominee, these requirements should be sufficiently specific so as not to potentially dissuade stockholders from bringing business before a stockholder meeting and should otherwise comply with Delaware law. The proposed changes narrow the information required to be disclosed such that Cboe is able to help ensure the objectives of the provisions are met without burdening stockholders with potentially overbroad requests for information.

Section 2.11(a)(iii)(D) of the CGM Bylaws currently sets forth certain representations that must be made by a stockholder seeking to bring business or a Stockholder Nominee before a

stockholder meeting regarding whether such stockholder is part of a group which intends to deliver or solicit proxies from stockholders in support of such proposed business. Cboe proposes changes to update this section in order to be more consistent with the universal proxy rules provided for in Rule 14a-19 of the Exchange Act by explicitly stating that any stockholder providing notice that they intend to solicit proxies in support of a proposed nominee must do so in accordance with Rule 14a-19 of the Exchange Act. Cboe also proposes to clarify that the representation must confirm whether the stockholder intends or is part of a group which intends to engage in a solicitation (within the meaning of Rule 14a-1(1) of the Exchange Act) with respect to the nomination of any proposed nominee or proposed business to be considered at the meeting.

Section 2.11(a)(iii)(F) of the CGM Bylaws currently requires that a Stockholder Nominee furnish any information that Cboe may determine is required for Cboe to determine the qualifications of such Stockholder Nominee to serve as a director of the Corporation. Cboe proposes to add language clarifying that the information Cboe may require must be consistent with the parameters set forth in Cboe's Corporate Governance Guidelines or the CGM Board's past practice in evaluating potential director nominees.

Proposed Section 2.11(c)(ii) of the CGM Bylaws requires the stockholder providing notice to notify the Secretary of any inaccuracy or change in any information submitted pursuant to Section 2.11 within two (2) business days of becoming aware of such inaccuracy or change. Cboe proposes to modify this requirement by narrowing the scope of circumstances in which a stockholder is required to provide notice of any inaccuracy or change of information that they have previously provided to material inaccuracies or changes.

Proposed Section 2.11(c)(iii) of the CGM Bylaws provides that any stockholder or Stockholder Associated Person providing notice with respect to any Stockholder Nominee is required to do so in a manner consistent with the requirements for universal proxy rules pursuant to Rule 14a-19 of the Exchange Act. Namely, the nomination of a Stockholder Nominee shall be disregarded if, among other things, there is no longer an intent to solicit proxies in support of a Stockholder Nominee or there is a failure to comply with the applicable requirements of Rule 14a-19. Upon request by the Corporation, if any stockholder providing notice or any

Stockholder Associated Person provides notice pursuant to Rule 14a-19(b) under the Exchange Act, such stockholder providing notice shall deliver to the Corporate Secretary, no later than five (5) business days prior to the applicable meeting date, then reasonable evidence that the requirements of Rule 14a-19(a)(3) under the Exchange Act have been satisfied.

Currently Section 2.11(c)(vi) of the CGM Bylaws defines "Stockholder Associated Person" to mean, among other things, (i) any person who is a member of a "group" (used in Rule 13d-5 under the Exchange Act) with, or otherwise acting in concert with, any stockholder providing notice, (ii) any person that is directly or indirectly controlled by, or under common control with, such stockholder or such Stockholder Associated Person, or (iii) any person directly or indirectly controlling any such stockholder or any Stockholder Associated Person. The proposed rule change reflects recent developments in Delaware law to add specificity to the definition and limit which individuals may be determined to be a Stockholder Associated Person and makes other clarifying changes. Specifically, the proposed rule change adds the qualifier that a Stockholder Associated Person must be known by the stockholder to be acting in concert with such stockholder, removes from the definition any person directly or indirectly controlled by, or under common control with such stockholder and replaces it with any affiliate or associate of such stockholder providing notice, and deletes the reference in the definition to any person directly or indirectly controlling any such stockholder or Stockholder Associated Person. The proposed rule change also adds any Stockholder Nominee to the definition of Stockholder Associated Person.

Revisions to Other Sections of the Bylaws

Cboe also proposes to make changes to Section 2.11 to reflect recent developments in Delaware law and to provide clarifications and prevent confusion. Cboe proposes to add a note to Section 2.11(a)(ii) that any proposed business for a stockholder meeting must be a proper matter for stockholder action. Cboe also proposes to amend Section 2.11(a)(iii)(B) to state that a Stockholder Nominee's written consent must be included in Cboe's proxy statement before they may be brought before a meeting. Previously, Section 2.11(a)(iii)(B) had stated that the Stockholder Nominee's written consent must be included in a proxy statement,

⁴ *Kellner v. AIM ImmunoTech Inc.*, C.A. 2023-0879-LWW (Del. Ch. Jan. 5, 2024).

but had not specifically defined it as Cboe's proxy statement. Cboe also proposes to amend the same section to state that a Stockholder Nominee will not enter into any commitment to vote in a certain manner if nominated to the CGM Board. Previously, this section had simply stated that a Stockholder Nominee may not enter into any commitment to vote in a certain manner with respect to certain matters at any company, without defining Cboe specifically. Cboe also proposes to amend the same section to require that a Stockholder Nominee not omit facts that are necessary to ensure statements made are not misleading in any material respect. Previously, the Stockholder Nominee's responsibility to not omit facts that are necessary to ensure statements are not misleading was not subject to materiality.

Cboe also proposes to make changes to Section 3.10 of the CGM Bylaws to provide that the Lead Director of Cboe may call a special meeting of the CGM Board. Section 3.10 currently permits, among other things, the Chair of the Board or the Chief Executive Officer to call a special meeting of the CGM Board. Revising this section to allow the Lead Director to call a special meeting of the CGM Board addresses a potential scenario in which the Chair of the Board and the Chief Executive Officer positions are jointly held by one individual and a special meeting of the CGM Board is not able to be called by individual independent directors.

2. Statutory Basis

The Exchange believes the proposed rule change is consistent with the Act and the rules and regulations thereunder applicable to the Exchange and, in particular, the requirements of Section 6(b) of the Act.⁵ Specifically, the Exchange believes the proposed rule change is consistent with the Section 6(b)(5)⁶ requirements that the rules of an exchange be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.

In light of an advisory vote by the stockholders of Cboe, Cboe is proposing changes to its Bylaws to implement a

right for stockholders to call a special meeting of the stockholders at a 25% threshold. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) of the Act because the proposed rule change would be consistent with and facilitate a governance and regulatory structure that is designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to, and perfect the mechanism of a free and open market and a national market system and, in general, to protect investors and the public interest. Particularly, the Exchange believes that, by permitting stockholders of Cboe to bring business or Stockholder Nominees before a special meeting, the proposed rule change strengthens the corporate governance of the Exchange's ultimate parent company, which is beneficial to both investors and the public interest.

Additionally, the procedural requirements are designed to help protect investors by stating clearly and explicitly the procedures stockholders must follow in order to bring business or Stockholder Nominees before a special meeting. The informational requirements are designed to enhance investor protection by helping to ensure among other things, that the Corporation and its stockholders have full and accurate information about nominating stockholders and Stockholder Nominees and that such stockholders and nominees comply with applicable laws, regulations and other requirements.

The changes that the Exchange is proposing with regard to so-called "advance notice bylaws" in light of the recent developments in Delaware law are designed to help provide additional clarity to stockholders wishing to bring business before a stockholder meeting or propose a Stockholder Nominee. The Exchange believes that this filing furthers the objectives of Section 6(b)(5) by simplifying the requirements and clarifying the information that must be disclosed by stockholders. This furthers the interests of investors and the public by removing potential impediments to raising business or proposing Stockholder Nominees that may otherwise restrict a stockholder's ability to participate in the corporate governance of the Corporation.

Finally, the remaining changes to existing provisions of the CGM Bylaws are clarifying in nature, and they enhance investor protection and the

public interest by preventing confusion with respect to the operation of the Bylaw provisions.

B. Self-Regulatory Organization's Statement on Burden on Competition

Because the proposed rule change relates to the governance of the Corporation and not to the operations of the Exchange, the Exchange does not believe that the proposed rule change will impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. The proposed rule change is not designed to address any competitive issue or have any impact on competition; rather, adoption of a stockholder special meeting provision, updating "advance notice bylaws," and other bylaws updates by the Corporation are intended to enhance corporate governance and accountability to stockholders.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

The Exchange neither solicited nor received comments on the proposed rule change.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the Exchange consents, the Commission will:

- A. by order approve or disapprove such proposed rule change, or
- B. institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR-CboeEDGX-2024-059 on the subject line.

⁵ 15 U.S.C. 78f(b).

⁶ 15 U.S.C. 78f(b)(5).

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

All submissions should refer to file number SR-CboeEDGX-2024-059. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR-CboeEDGX-2024-059 and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁷

Sherry R. Haywood,

Assistant Secretary.

[FR Doc. 2024-25055 Filed 10-28-24; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-101408; File No. SR-NYSE-2024-65]

Self-Regulatory Organizations; New York Stock Exchange LLC; Notice of Filing and Immediate Effectiveness of Proposed Rule Change To Amend Its Price List

October 23, 2024.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act"),¹ and Rule 19b-4 thereunder,² notice is hereby given that on October 10, 2024, New York Stock Exchange LLC ("NYSE" or the "Exchange") filed with the Securities and Exchange Commission ("SEC" or "Commission") the proposed rule change as described in Items I, II, and III below, which Items have been prepared by the Exchange. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization's Statement of the Terms of Substance of the Proposed Rule Change

The Exchange proposes to amend its Price List to modify two adding tiers for Midpoint Passive Liquidity ("MPL") Orders that add liquidity to the Exchange. The proposed rule change is available on the Exchange's website at www.nyse.com, at the principal office of the Exchange, and at the Commission's Public Reference Room.

II. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the self-regulatory organization included statements concerning the purpose of, and basis for, the proposed rule change and discussed any comments it received on the proposed rule change. The text of those statements may be examined at the places specified in Item IV below. The Exchange has prepared summaries, set forth in sections A, B, and C below, of the most significant parts of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

The Exchange proposes to amend its Price List to modify two adding tiers for

MPL Orders that add liquidity to the Exchange.

The proposed changes respond to the current competitive environment where order flow providers have a choice of where to direct liquidity-providing orders by offering further incentives for member organizations to send additional displayed liquidity to the Exchange.

The Exchange proposes to implement the fee changes effective October 10, 2024.³

Background

Current Market and Competitive Environment

The Exchange operates in a highly competitive market. The Commission has repeatedly expressed its preference for competition over regulatory intervention in determining prices, products, and services in the securities markets. In Regulation NMS, the Commission highlighted the importance of market forces in determining prices and SRO revenues and, also, recognized that current regulation of the market system "has been remarkably successful in promoting market competition in its broader forms that are most important to investors and listed companies."⁴

While Regulation NMS has enhanced competition, it has also fostered a "fragmented" market structure where trading in a single stock can occur across multiple trading centers. When multiple trading centers compete for order flow in the same stock, the Commission has recognized that "such competition can lead to the fragmentation of order flow in that stock."⁵ Indeed, cash equity trading is currently dispersed across 16 exchanges,⁶ numerous alternative trading systems,⁷ and broker-dealer internalizers and wholesalers, all competing for order flow. Based on publicly-available information, no

³ The Exchange originally filed to amend the Fee Schedule on October 1, 2024 (SR-NYSE-2024-62). SR-NYSE-2024-62 was subsequently withdrawn and replaced by this filing.

⁴ See Securities Exchange Act Release No. 51808 (June 9, 2005), 70 FR 37496, 37499 (June 29, 2005) (File No. S7-10-04) (Final Rule) ("Regulation NMS").

⁵ See Securities Exchange Act Release No. 61358, 75 FR 3594, 3597 (January 21, 2010) (File No. S7-02-10) (Concept Release on Equity Market Structure).

⁶ See Cboe U.S. Equities Market Volume Summary, available at https://markets.cboe.com/us/equities/market_share. See generally <https://www.sec.gov/fast-answers/divisionsmarketregmrexchangesshtml.html>.

⁷ See FINRA ATS Transparency Data, available at <https://otctransparency.finra.org/otctransparency/AtsIssueData>. A list of alternative trading systems registered with the Commission is available at <https://www.sec.gov/foia/docs/atlist.htm>.

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

⁷ 17 CFR 200.30-3(a)(12).

single exchange currently has more than 20% market share.⁸ Therefore, no exchange possesses significant pricing power in the execution of cash equity order flow. More specifically, the Exchange's share of executed volume of equity trades in Tapes A, B and C securities is less than 12%.⁹

The Exchange believes that the ever-shifting market share among the exchanges from month to month demonstrates that market participants can move order flow, or discontinue or reduce use of certain categories of products. While it is not possible to know a firm's reason for shifting order flow, the Exchange believes that one such reason is because of fee changes at any of the registered exchanges or non-exchange venues to which the firm routes order flow. Accordingly, competitive forces compel the Exchange to use exchange transaction fees and credits because market participants can readily trade on competing venues if they deem pricing levels at those other venues to be more favorable.

In response to this competitive environment, the Exchange has established incentives for member organizations who submit orders that provide liquidity on the Exchange in MPL Orders. The proposed fee change is designed to enhance incentives to member organizations to submit additional such liquidity to the Exchange.

Proposed Rule Change

An MPL Order is defined in Rule 7.31 as a Limit Order that is not displayed and does not route, with a working price at the midpoint of the PBBO.¹⁰

Currently, the Exchange offers tiered credits, among others, of \$0.0029 and \$0.0030, respectively, for member organizations that have an average daily trading volume ("ADV") that adds liquidity to the Exchange during the billing month ("Adding ADV") in MPL Orders of at least 25 million shares and 30 million shares, respectively, excluding any liquidity added by a Designated Market Maker ("DMM").

The Exchange proposes to modify these adding tier credits for MPL Orders, as follows.

First, the Exchange would raise the \$0.0029 credit to \$0.0030. The Exchange would also lower the ADV requirement from 25 million shares to 20 million shares. As proposed, the tier would offer a \$0.0030 credit for member

organizations that have an Adding ADV in MPL Orders of 20 million shares, excluding any liquidity added by a DMM.

Second, the Exchange would raise the other tiered credit of \$0.0030 to \$0.0031. The Exchange would also lower the ADV requirement from 30 million shares to 25 million shares. As proposed, this tier would offer a \$0.0031 credit for member organizations that have an Adding ADV in MPL Orders of at least 25 million shares, excluding any liquidity added by a DMM.

In both instances, the Exchange believes that modifying the amount of the credit and the minimum share requirement would incentivize member organizations to trade on the Exchange in MPL Orders. Specifically, the Exchange believes that increasing the credits and lowering volume requirements would enable more member organizations with high volumes of Adding ADV in MPL Orders to qualify for the respective tiers, especially in high volume months.

The purpose of the proposed change is to provide additional incentives for member organizations to qualify for higher credits for MPL Orders that add liquidity to the Exchange by lowering the minimum volume requirement. The Exchange believes that the proposal would thereby increase liquidity providing MPL Orders, which in turn would support the quality of price discovery on the Exchange and provide additional price improvement opportunities for incoming orders that take liquidity. The Exchange believes that by correlating the amount of credits to the level of MPL Orders that add liquidity sent by a member organization, the Exchange's fee structure would incentivize member organizations to submit more MPL Orders that add liquidity to the Exchange, thereby increasing the potential for price improvement and execution opportunities to incoming marketable orders submitted to the Exchange.

As noted above, the Exchange operates in a competitive and fragmented market environment, particularly as it relates to attracting non-marketable orders, which add liquidity to the Exchange. Based on the profile of liquidity-adding firms generally, the Exchange believes that additional member organizations could qualify for these tiers if they choose to direct order flow to the Exchange. However, without having a view of member organization's activity on other exchanges and off-exchange venues, the Exchange has no way of knowing whether the proposed rule change would result in any member

organization directing MPL Orders to the Exchange in order to qualify for a new proposed tier.

The proposed changes are not otherwise intended to address other issues, and the Exchange is not aware of any significant problems that market participants would have in complying with the proposed changes.

2. Statutory Basis

The Exchange believes that the proposed rule change is consistent with Section 6(b) of the Act,¹¹ in general, and furthers the objectives of Sections 6(b)(4) and (5) of the Act,¹² in particular, because it provides for the equitable allocation of reasonable dues, fees, and other charges among its members, issuers and other persons using its facilities and does not unfairly discriminate between customers, issuers, brokers or dealers.

As discussed above, the Exchange operates in a highly competitive market. The Commission has repeatedly expressed its preference for competition over regulatory intervention in determining prices, products, and services in the securities markets. In Regulation NMS, the Commission highlighted the importance of market forces in determining prices and SRO revenues and, also, recognized that current regulation of the market system "has been remarkably successful in promoting market competition in its broader forms that are most important to investors and listed companies."¹³ While Regulation NMS has enhanced competition, it has also fostered a "fragmented" market structure where trading in a single stock can occur across multiple trading centers. When multiple trading centers compete for order flow in the same stock, the Commission has recognized that "such competition can lead to the fragmentation of order flow in that stock."¹⁴

The Proposed Change Is Reasonable

The proposed modifications to two of the Adding Tiers for MPL Orders are reasonable because they provide additional incentives for member organizations to qualify for higher credits for adding liquidity in MPL Orders by lowering the minimum volume requirement, thereby

¹¹ 15 U.S.C. 78f(b).

¹² 15 U.S.C. 78f(b)(4) & (5).

¹³ See Securities Exchange Act Release No. 51808 (June 9, 2005), 70 FR 37495, 37499 (June 29, 2005) (S7-10-04) (Final Rule) ("Regulation NMS").

¹⁴ See Securities Exchange Act Release No. 61358, 75 FR 3594, 3597 (January 21, 2010) (File No. S7-02-10) (Concept Release on Equity Market Structure).

⁸ See Choe Global Markets U.S. Equities Market Volume Summary, available at https://markets.choe.com/us/equities/market_share/.

⁹ See *id.*

¹⁰ See Rule 7.31(d)(3). Limit Order is defined in Rule 7.31(a)(2).

encouraging the submission of additional liquidity to a national securities exchange. As noted, the Exchange believes that the proposed enhancements would enable more member organizations to add liquidity in MPL Orders. Submission of additional liquidity to the Exchange would promote price discovery and transparency and enhance order execution opportunities for member organizations from the substantial amounts of liquidity present on the Exchange. All member organizations benefit from the greater amounts of liquidity that will be present on the Exchange, which provides greater execution opportunities.

The Proposal Is an Equitable Allocation of Fees

The Exchange believes the proposal equitably allocates its fees among its market participants. By providing additional incentives for member organizations to qualify for an adding credit, the proposal would continue to encourage member organizations to send orders that provide liquidity to the Exchange, thereby contributing to robust levels of liquidity, which benefits all market participants, and promoting price discovery and transparency. The proposal would also enhance order execution opportunities for member organizations from the substantial amounts of liquidity present on the Exchange. All member organizations would benefit from the greater amounts of liquidity that will be present on the Exchange, which would provide greater execution opportunities and additional price improvement opportunities for incoming orders. The Exchange believes that by offering higher credits correlated to lower volumes of Adding ADV in MPL Orders, more member organizations will be able to choose to route their liquidity-providing orders to the Exchange to qualify for the proposed credits. As previously noted, based on the profile of liquidity-providing member organizations generally, the Exchange believes additional member organizations could qualify for the proposed credits if they choose to direct order flow to the Exchange. Additional liquidity-providing orders benefits all market participants because it provides greater execution opportunities on the Exchange.

The Proposal Is Not Unfairly Discriminatory

The Exchange believes its proposal is not unfairly discriminatory because the proposal would be provided on an equal basis to all member organizations that add liquidity, who would all be eligible

for the same credits on an equal basis. Accordingly, no member organization already operating on the Exchange would be disadvantaged by this allocation of fees. Further, as noted, the Exchange believes the proposal would provide an incentive for member organizations to continue to send orders that provide liquidity to the Exchange, to the benefit of all market participants.

For the foregoing reasons, the Exchange believes that the proposal is consistent with the Act.

B. Self-Regulatory Organization's Statement on Burden on Competition

In accordance with Section 6(b)(8) of the Act,¹⁵ the Exchange believes that the proposed rule change would not impose any burden on competition that is not necessary or appropriate in furtherance of the purposes of the Act. Instead, as discussed above, the Exchange believes that the proposed changes would encourage the submission of additional liquidity to a public exchange, thereby promoting market depth, price discovery and transparency and enhancing order execution opportunities for member organizations. As a result, the Exchange believes that the proposed change furthers the Commission's goal in adopting Regulation NMS of fostering integrated competition among orders, which promotes "more efficient pricing of individual stocks for all types of orders, large and small."¹⁶

Intramarket Competition. The proposed change is designed to attract additional order flow to the Exchange. The Exchange believes that the proposed changes would continue to incentivize market participants to direct order flow to the Exchange. Greater liquidity benefits all market participants on the Exchange by providing more trading opportunities and encourages member organizations to send orders, thereby contributing to robust levels of liquidity, which benefits all market participants on the Exchange. The proposed credits would be available to all similarly-situated market participants, and, as such, the proposed change would not impose a disparate burden on competition among market participants on the Exchange. As noted, the proposal would apply to all similarly situated member organizations on the same and equal terms, who would benefit from the changes on the same basis. Accordingly, the proposed change would not impose a disparate burden on competition among market participants on the Exchange.

¹⁵ 15 U.S.C. 78f(b)(8).

¹⁶ See Regulation NMS, 70 FR at 37498–99.

Intermarket Competition. The Exchange operates in a highly competitive market in which market participants can readily choose to send their orders to other exchange and off-exchange venues if they deem fee levels at those other venues to be more favorable. In such an environment, the Exchange must continually adjust its fees and rebates to remain competitive with other exchanges and with off-exchange venues. Because competitors are free to modify their own fees and credits in response, and because market participants may readily adjust their order routing practices, the Exchange does not believe its proposed fee change can impose any burden on intermarket competition.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

No written comments were solicited or received with respect to the proposed rule change.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Pursuant to Section 19(b)(3)(A)(ii) of the Act,¹⁷ and Rule 19b–4(f)(2) thereunder¹⁸ the Exchange has designated this proposal as establishing or changing a due, fee, or other charge imposed on any person, whether or not the person is a member of the self-regulatory organization, which renders the proposed rule change effective upon filing. At any time within 60 days of the filing of the proposed rule change, the Commission summarily may temporarily suspend such rule change if it appears to the Commission that such action is necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of the Act.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views, and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include file number SR–NYSE–2024–65 on the subject line.

¹⁷ 15 U.S.C. 78s(b)(3)(A)(ii).

¹⁸ 17 CFR 240.19b–4.

Paper Comments

• Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–1090.

All submissions should refer to file number SR–NYSE–2024–65. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549 on official business days between the hours of 10 a.m. and 3 p.m. Copies of the filing also will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR–NYSE–2024–65, and should be submitted on or before November 19, 2024.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.¹⁹

Sherry R. Haywood,

Assistant Secretary.

[FR Doc. 2024–25048 Filed 10–28–24; 8:45 am]

BILLING CODE 8011–01–P

SMALL BUSINESS ADMINISTRATION

[Disaster Declaration #20658 and #20659; CALIFORNIA Disaster Number CA–20024]

Administrative Declaration of a Disaster for the State of California

AGENCY: U.S. Small Business Administration.

ACTION: Notice.

SUMMARY: This is a notice of an Administrative declaration of a disaster for the State of California dated 10/23/2024.

Incident: Bridge Fire.

Incident Period: 09/08/2024 and continuing.

DATES: Issued on 10/23/2024.

Physical Loan Application Deadline Date: 12/23/2024.

Economic Injury (EIDL) Loan Application Deadline Date: 07/23/2025.

ADDRESSES: Visit the MySBA Loan Portal at <https://lending.sba.gov> to apply for a disaster assistance loan.

FOR FURTHER INFORMATION CONTACT:

Alan Escobar, Office of Disaster Recovery & Resilience, U.S. Small Business Administration, 409 3rd Street SW, Suite 6050, Washington, DC 20416, (202) 205–6734.

SUPPLEMENTARY INFORMATION: Notice is hereby given that as a result of the Administrator's disaster declaration, applications for disaster loans may be submitted online using the MySBA Loan Portal <https://lending.sba.gov> or other locally announced locations. Please contact the SBA disaster assistance customer service center by email at disastercustomerservice@sba.gov or by phone at 1–800–659–2955 for further assistance.

The following areas have been determined to be adversely affected by the disaster:

Primary Counties: Los Angeles

Contiguous Counties:

California: Kern, Orange, San Bernardino, Ventura

The Interest Rates are:

	Percent
<i>For Physical Damage:</i>	
Homeowners with Credit Available Elsewhere	5.625
Homeowners without Credit Available Elsewhere	2.813
Businesses with Credit Available Elsewhere	8.000
Businesses without Credit Available Elsewhere	4.000
Non-Profit Organizations with Credit Available Elsewhere ...	3.250
Non-Profit Organizations without Credit Available Elsewhere	3.250
<i>For Economic Injury:</i>	
Business and Small Agricultural Cooperatives without Credit Available Elsewhere	4.000
Non-Profit Organizations without Credit Available Elsewhere	3.250

The number assigned to this disaster for physical damage is 206585 and for economic injury is 206590.

The States which received an EIDL Declaration are California.

(Catalog of Federal Domestic Assistance Number 59008)

Isabella Guzman,

Administrator.

[FR Doc. 2024–25063 Filed 10–28–24; 8:45 am]

BILLING CODE 8026–09–P

SMALL BUSINESS ADMINISTRATION

[Disaster Declaration #20753 and #20754; GEORGIA Disaster Number GA–20014]

Presidential Declaration Amendment of a Major Disaster for Public Assistance Only for the State of Georgia

AGENCY: U.S. Small Business Administration.

ACTION: Amendment 4.

SUMMARY: This is an amendment of the Presidential declaration of a major disaster for Public Assistance Only for the State of Georgia (FEMA–4830–DR), dated October 9, 2024.

Incident: Hurricane Helene.

DATES: Issued on October 21, 2024.

Incident Period: September 24, 2024, and continuing.

Physical Loan Application Deadline Date: December 9, 2024.

Economic Injury (EIDL) Loan Application Deadline Date: July 9, 2025.

ADDRESSES: Visit the MySBA Loan Portal at <https://lending.sba.gov> to apply for a disaster assistance loan.

FOR FURTHER INFORMATION CONTACT:

Alan Escobar, Office of Disaster Recovery & Resilience, U.S. Small Business Administration, 409 3rd Street SW, Suite 6050, Washington, DC 20416, (202) 205–6734.

SUPPLEMENTARY INFORMATION: The notice of the President's major disaster declaration for Private Non-Profit organizations in the State of Georgia, dated October 9, 2024, is hereby amended to include the following areas as adversely affected by the disaster.

Primary Counties: Banks, Bleckley, Butts, Clinch, Dawson, Decatur, Echols, Elbert, Franklin, Gilmer, Greene, Habersham, Hancock, Hart, Jackson, Jasper, Lamar, Lanier, Lincoln, Lumpkin, Madison, Morgan, Oglethorpe, Pike, Putnam, Rabun, Stephens, Treutlen, Washington, White, Wilkes.

All other information in the original declaration remains unchanged.

(Catalog of Federal Domestic Assistance Number 59008)

Rafaela Monchek,

Deputy Associate Administrator, Office of Disaster Recovery & Resilience.

[FR Doc. 2024–25062 Filed 10–28–24; 8:45 am]

BILLING CODE 8026–09–P

¹⁹ 17 CFR 200.30–3(a)(12).

OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE

Request for Applications From Individuals Interested in Serving as an Indigenous Peoples' Representative on the Observer Delegation From the United States to the Partnership Council of the Indigenous Peoples Economic and Trade Cooperation Arrangement

AGENCY: Office of the United States Trade Representative.

ACTION: Request for applications.

SUMMARY: The Office of the United States Trade Representative (USTR) has led the United States' efforts on the Indigenous Peoples Economic and Trade Cooperation Arrangement (IPETCA) since the United States became an Observer to the IPETCA Partnership Council—the governing body of IPETCA—in April 2024. USTR is accepting applications from qualified individuals interested in serving a two-year term (with an option to extend for a third year) as an Indigenous Peoples' representative alongside U.S. government representatives on the observer delegation from the United States.

DATES: Submit applications no later than 5 p.m. EST on December 6, 2024.

ADDRESSES: Submit applications to the Office of Intergovernmental Affairs and Public Engagement (IAPE) at mbx.ustr.iape@ustr.eop.gov.

FOR FURTHER INFORMATION CONTACT: Anthony Reyes, IAPE Director and Advisor, at mbx.ustr.iape@ustr.eop.gov or 202.395.2226.

SUPPLEMENTARY INFORMATION:

I. Background

IPETCA is a non-binding arrangement initiated by New Zealand on the margins of its 2021 Asia-Pacific Economic Cooperation (APEC) host year. Participating economies include New Zealand, Australia, Canada and Chinese Taipei. The goal of IPETCA is to establish a framework for facilitating cooperation between participating economies to identify and remove barriers to Indigenous Peoples' economic empowerment and participation in trade. The texts of IPETCA and the IPETCA Partnership Council Terms of Reference are available at: <https://www.mfat.govt.nz/en/trade/nz-trade-policy/the-indigenous-peoples-economic-and-trade-cooperation-arrangement>.

In response to input during USTR's Tribal consultation meetings and engagement with Indigenous Peoples,

the United States became an Observer to the IPETCA Partnership Council in April 2024. The Partnership Council is composed of up to two representatives of each participating economy and up to two Indigenous Peoples' representatives from each participating economy unless decided otherwise. Among other functions, the IPETCA Partnership Council has developed and approved a work program to determine, organize and facilitate activities under the IPETCA and decide the priorities for shared cooperation activities. The Partnership Council also is expected to consider encouraging appropriate multilateral and regional organizations to support projects that enable participation of Indigenous businesses in trade and investment, while emphasizing the important contributions made by Indigenous women-owned businesses in the export of goods and services. The IPETCA Partnership Council is expected to meet four to five times annually, with at least one in-person event (location to be determined) at the call of the co-chairs of the IPETCA Partnership Council or their designee.

II. Requirements To Be an Indigenous Peoples' Representative

The U.S. Trade Representative anticipates appointing up to three people to serve as Indigenous Peoples' representatives on the Observer delegation from the United States to the IPETCA Partnership Council, to represent the interests in international trade policy of Indigenous communities in the United States, including American Indians, Alaska Natives, Native Hawaiians, and Pacific Islanders. USTR is accepting applications from qualified individuals interested in serving a two-year term, with an option to extend for a third year. USTR expects Indigenous Peoples' representatives who participate as part of the Observer delegation from the United States to attend all meetings of the IPETCA Partnership Council. This is expected to include three to four virtual meetings, and one in-person meeting each year. The in-person meeting typically is held on the sidelines of the APEC Economic Leaders Week meetings and will require international travel. USTR may be able to subsidize travel costs associated with in-person meetings of the IPETCA Partnership Council.

The foremost consideration for applicants is their ability to engage with U.S. government representatives to ensure robust participation by Indigenous Peoples in IPETCA meetings and activities, as appropriate. Other criteria include the applicant's

knowledge of and expertise in international trade policy, the work of USTR, and economic development relevant to their community. In addition to general trade, investment and development issues, representatives must have expertise in areas such as:

- Understanding barriers to Indigenous Peoples' access to and participation in international trade.
- Identifying possible solutions to better incorporate Indigenous Peoples into U.S. trade policy.
- Developing and presenting actionable recommendations to U.S. government officials.
- Understanding Indigenous government, economies, or business administration.
- Eliminating barriers to equity, equality, and economic opportunity and promoting understanding of the projected impact of proposed trade policies on Indigenous communities in the United States.

The Indigenous Peoples' representatives will serve at the discretion of the U.S. Trade Representative for two-year terms, with an option to extend for a third year. The U.S. Trade Representative may reappoint individuals for any number of terms.

USTR is committed to a trade agenda that advances racial and gender equity, equality and economic empowerment and will seek advice and recommendations on trade policies that enhance resiliency, sustainability and broad-based economic growth. USTR strives to build trusted, sustained lines of communication with those who will be impacted by trade policy decisions in order to better understand the projected impact of proposed trade policies on all communities, including underserved, marginalized and overburdened communities.

USTR strongly encourages diverse backgrounds and perspectives and will make appointments without regard to political affiliation and in accordance with equal opportunity practices that promote diversity, equity, inclusion and accessibility. USTR will strive to ensure balance in terms of points of view, sectors, demographics, geography, entity or organization size, and other factors relevant to USTR's needs.

III. Request for Applications

To apply, an applicant must meet the eligibility criteria described in Section II at the time of application. In addition, an applicant, if selected as an Indigenous Peoples' representative from the United States, will be required at all times during the representative's term of

service to comply with the following conditions:

1. They must be a U.S. citizen.
2. They cannot be a full-time employee of a U.S. governmental entity.
3. They cannot be a federally registered lobbyist.
4. They cannot be registered with the U.S. Department of Justice under the Foreign Agents Registration Act.
5. For a representative sponsored by an organization, they must be associated with a U.S. organization whose members (or funders or mission) have a demonstrated interest in issues relevant to Indigenous representation and economies.

6. For eligibility purposes, a 'U.S. organization' is an organization established under the laws of the United States, that is controlled by U.S. citizens, by another U.S. organization (or organizations), or by a U.S. entity (or entities), determined based on its board of directors (or comparable governing body), membership and funding sources, as applicable. To qualify as a U.S. organization, more than 50 percent of the board of directors (or comparable governing body) and more than 50 percent of the membership of the organization to be represented must be U.S. citizens, U.S. organizations, or U.S. entities. Additionally, at least 50 percent of the organization's annual revenue must be attributable to nongovernmental U.S. sources.

In order to be considered for appointment as an Indigenous Peoples' representative, qualified individuals should submit the following to the Office of Intergovernmental Affairs and Public Engagement at mbx.ustr.iape@ustr.eop.gov by the December 6, 2024, 5 p.m. EST deadline:

- Name, title, affiliation, and contact information of the applicant.
- The applicant's personal resume.
- A statement explaining how the applicant meets the eligibility criteria, why USTR would benefit from having the applicant on the U.S. Observer delegation, and how the applicant can serve the interests of all Indigenous communities in the United States.

USTR will consider applicants who meet the eligibility criteria in accordance with equal opportunity practices that promote diversity, equity, inclusion and accessibility.

Roberto Soberanis,

Assistant U.S. Trade Representative for Intergovernmental Affairs and Public Engagement, Office of the United States Trade Representative.

[FR Doc. 2024-25111 Filed 10-28-24; 8:45 am]

BILLING CODE 3390-F4-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

[FAA-2024-1636]

Agency Information Collection Activities: Requests for Comments; Clearance of a Renewed Approval of Information Collection: Generic Clearance for the Collection of Qualitative Feedback on Agency Service Delivery

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice and request for comments.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, FAA invites public comments about our intention to request the Office of Management and Budget (OMB) approval to renew an information collection. The **Federal Register** Notice with a 60-day comment period soliciting comments on the following collection of information was published on May 23, 2024. As part of a Federal Government-wide effort to streamline the process to seek feedback from the public on service delivery, FAA has an approved Generic Information Collection Request (Generic ICR): "Generic Clearance for the Collection of Qualitative Feedback on Agency Service Delivery."

DATES: Written comments should be submitted by November 29, 2024.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting "Currently under 30-day Review—Open for Public Comments" or by using the search function.

FOR FURTHER INFORMATION CONTACT: Barbara Hall at (940) 594-5913, or by email at: Barbara.L.Hall@faa.gov.

SUPPLEMENTARY INFORMATION:

Public Comments Invited: You are asked to comment on any aspect of this information collection, including (a) Whether the proposed collection of information is necessary for FAA's performance; (b) the accuracy of the estimated burden; (c) ways for FAA to enhance the quality, utility and clarity of the information collection; and (d) ways that the burden could be minimized without reducing the quality of the collected information.

OMB Control Number: 2120-0746.

Title: Generic Clearance for the Collection of Qualitative Feedback on Agency Service Delivery.

Form Numbers: NA.

Type of Review: Renewal of an information collection.

Background: The **Federal Register** Notice with a 60-day comment period soliciting comments on the following collection of information was published on May 23, 2024 (89 FR 45731). The information collection activity will garner qualitative customer and stakeholder feedback in an efficient, timely manner, in accordance with the Administration's commitment to improving service delivery. By qualitative feedback we mean information that provides useful insights on perceptions and opinions but are not statistical surveys that yield quantitative results that can be generalized to the population of study. This feedback will provide insights into customer or stakeholder perceptions, experiences and expectations, provide an early warning of issues with service, or focus attention on areas where communication, training or changes in operations might improve delivery of products or services. These collections will allow for ongoing, collaborative and actionable communications between the Agency and its customers and stakeholders. It will also allow feedback to contribute directly to the improvement of program management. Feedback collected under this generic clearance will provide useful information, but it will not yield data that can be generalized to the overall population. This type of generic clearance for qualitative information will not be used for quantitative information collections that are designed to yield reliably actionable results, such as monitoring trends over time or documenting program performance. Such data uses require more rigorous designs that address: The target population to which generalizations will be made, the sampling frame, the sample design (including stratification and clustering), the precision requirements or power calculations that justify the proposed sample size, the expected response rate, methods for assessing potential non-response bias, the protocols for data collection, and any testing procedures that were or will be undertaken prior fielding the study. Depending on the degree of influence the results are likely to have, such collections may still be eligible for submission for other generic mechanisms that are designed to yield quantitative results.

Respondents: 110,000 Individuals and Households, Businesses and Organizations, State, Local or Tribal Government.

Frequency: Once per request.

Estimated Average Burden per Response: 10 minutes.

Estimated Total Annual Burden: 18,330 hours.

Issued in Fort Worth, TX, on October 24, 2024.

Barbara L. Hall,

FAA Information Collection Clearance Officer, Performance, Policy, and Records Management, Branch, ASP-110.

[FR Doc. 2024-25084 Filed 10-28-24; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Railroad Administration

[Docket Number FRA-2006-25040]

Petition for Modification of Waiver of Compliance

Under part 211 of title 49 Code of Federal Regulations (CFR), this document provides the public notice that by letter dated August 21, 2024, Capital Metropolitan Transportation Authority (CMTY) petitioned the Federal Railroad Administration (FRA) for a modification of a waiver of compliance from certain provisions of the Federal railroad safety regulations contained at 49 CFR part 222 (Use of Locomotive Horns at Public Highway-Rail Grade Crossings), part 229 (Railroad Locomotive Safety Standards), part 231 (Railroad Safety Appliance Standards), part 234 (Grade Crossing Safety), and part 238 (Passenger Equipment Safety Standards). The relevant Docket Number is FRA-2006-25040.

Specifically, CMTY requested to amend its current waiver that provides relief for its commuter rail system that connects downtown Austin, Texas, with Austin's northern suburbs along 32 miles with 9 stations. CMTY seeks to add a fleet of four Stadler GTW fourth-generation diesel multiple unit (DMU) rail vehicles to its existing fleet of six Stadler GTW first-generation DMUs.

In support of its request, CMTY explained that their vehicles demonstrate "an equivalent level of safety and compliance," given the Alternative Vehicle Technology final rule amendments in 49 CFR part 238.

A copy of the petition, as well as any written communications concerning the petition, is available for review online at www.regulations.gov.

Interested parties are invited to participate in these proceedings by submitting written views, data, or comments. FRA does not anticipate scheduling a public hearing in connection with these proceedings since the facts do not appear to warrant a hearing. If any interested parties desire

an opportunity for oral comment and a public hearing, they should notify FRA, in writing, before the end of the comment period and specify the basis for their request.

All communications concerning these proceedings should identify the appropriate docket number and may be submitted at www.regulations.gov. Follow the online instructions for submitting comments.

Communications received by December 30, 2024 will be considered by FRA before final action is taken. Comments received after that date will be considered if practicable.

Anyone can search the electronic form of any written communications and comments received into any of the U.S. Department of Transportation's (DOT) dockets by the name of the individual submitting the comment (or signing the document, if submitted on behalf of an association, business, labor union, etc.). Under 5 U.S.C. 553(c), DOT solicits comments from the public to better inform its processes. DOT posts these comments, without edit, including any personal information the commenter provides, to www.regulations.gov, as described in the system of records notice (DOT/ALL-14 FDMS), which can be reviewed at <https://www.transportation.gov/privacy>. See also <https://www.regulations.gov/privacy-notice> for the privacy notice of www.regulations.gov.

Issued in Washington, DC.

John Karl Alexy,

Associate Administrator for Railroad Safety, Chief Safety Officer.

[FR Doc. 2024-25083 Filed 10-28-24; 8:45 am]

BILLING CODE 4910-06-P

DEPARTMENT OF TRANSPORTATION

Federal Railroad Administration

[Docket Number FRA-2017-0087]

Petition for Waiver of Compliance

Under part 211 of title 49 Code of Federal Regulations (CFR), this document provides the public notice that by letter received July 15, 2024, TEXRail petitioned the Federal Railroad Administration (FRA) for a waiver of compliance from certain provisions of the Federal railroad safety regulations contained at 49 CFR part 238 (Passenger Equipment Safety Standards). The relevant Docket Number is FRA-2017-0087.

Specifically, TEXRail seeks relief from § 238.309(b)(2), *Periodic brake equipment maintenance*, regarding the required clean, oil, test, and stencil

(COTS) air brake maintenance, for two years due to "the brake system and parts manufacturer delay in production." TEXRail further stated that the manufacturer, Knorr Air Brake Berlin, "is the only facility qualified to repair our [a]ir [b]rake equipment" and that the relief would allow TEXRail to continue revenue service while the equipment is awaiting the required COTS overhaul. TEXRail asserts that it will ensure the brake systems will remain in proper functioning condition and are safe to operate. Specifically, it will "complete a Tri-annual inspection, minus replacing the actual brake components" and perform a "daily Class 1 brake test." TEXRail states it will perform a "weekly Teloc download to ensure the brake system is working as intended during the Class 1 Brake Test."

TEXRail's existing grant of relief in this docket provides a waiver from certain other regulations pertaining to the design of TEXRail's Stadler FLIRT equipment. The equipment was built to current European design and regulatory standards, with modifications and updates for use in the United States.

A copy of the petition, as well as any written communications concerning the petition, is available for review online at www.regulations.gov.

Interested parties are invited to participate in these proceedings by submitting written views, data, or comments. FRA does not anticipate scheduling a public hearing in connection with these proceedings since the facts do not appear to warrant a hearing. If any interested parties desire an opportunity for oral comment and a public hearing, they should notify FRA, in writing, before the end of the comment period and specify the basis for their request.

All communications concerning these proceedings should identify the appropriate docket number and may be submitted at www.regulations.gov. Follow the online instructions for submitting comments.

Communications received by December 30, 2024 will be considered by FRA before final action is taken. Comments received after that date will be considered if practicable.

Anyone can search the electronic form of any written communications and comments received into any of the U.S. Department of Transportation's (DOT) dockets by the name of the individual submitting the comment (or signing the document, if submitted on behalf of an association, business, labor union, etc.). Under 5 U.S.C. 553(c), DOT solicits comments from the public to better inform its processes. DOT posts these comments, without edit, including

any personal information the commenter provides, to www.regulations.gov, as described in the system of records notice (DOT/ALL-14 FDMS), which can be reviewed at <https://www.transportation.gov/privacy>. See also <https://www.regulations.gov/privacy-notice> for the privacy notice of regulations.gov.

Issued in Washington, DC.

John Karl Alexy,

*Associate Administrator for Railroad Safety,
Chief Safety Officer.*

[FR Doc. 2024-25081 Filed 10-28-24; 8:45 am]

BILLING CODE 4910-06-P

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

[Docket No. NHTSA-2024-0050]

Notice of Technical Workshop and Demonstrations for Vehicle Classification Test Procedure

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT).

ACTION: Notice of technical workshop and demonstration and request for comments (RFC).

SUMMARY: NHTSA seeks public comment on draft test procedure (TP) number TP-523-00, which is intended to assess vehicles for compliance with certain off-road capabilities requirements for vehicle classification within the Corporate Average Fuel Economy (CAFE) program. This TP is prepared for the limited purpose of use by contracted independent laboratories conducting tests for NHTSA. The TP presents guidelines for a uniform testing and data recording format. TPs are not rules, regulations, or agency interpretations. NHTSA will host a demonstration of TP-523-00 to show how NHTSA intends to test vehicles to determine compliance with its regulations on vehicle classification.

DATES: A technical workshop (presentation) and public demonstration for the test procedure will be held on January 15, 2025, and are expected to begin at 8 a.m. The date, location, and agenda are subject to change, and all registered attendees will be notified of any changes. Comments regarding the TP, the workshop, or the demonstration must be received no later than November 30, 2024 in order to be addressed during the event. The agency may address any comments received during the event regarding the TP, the workshop, and the demonstration, but

comments should also be submitted to the docket for formal record per the “Comment” instructions indicated below. Comments submitted to the docket after November 30, 2024 will continue to be received and considered through February 15, 2025 to facilitate the final draft release of the TP.

ADDRESSES:

Workshop and Demonstration

Location: The workshop and demonstration will be held at the McNeese Convention Center in San Angelo, Texas. Directions to the meeting location and final agenda will be sent to registered participants as well as posted on the NHTSA Public Information Center (PIC) at <https://www.nhtsa.gov/corporate-average-fuel-economy/cafe-public-information-center>.

Documents for Comment: NHTSA’s Office of Vehicle Safety Compliance (OVSC) laboratory test procedure TP-523-00, described in this RFC, is available for viewing in PDF format in this Docket, as identified in the heading of this document.

Comments: You may submit comments to the Docket, identified as the docket number in the head of this document, by any of the following methods:

- **Federal rulemaking Portal:** To submit comments electronically, go to the U.S. Government regulations website at <http://www.regulations.gov>. Follow the online instructions for submitting comments.
- **Fax:** Written comments may be faxed to 202-493-2251.
- **Mail:** Send comments to: Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building Ground Floor, Room W12-140, Washington, DC 20590-0001.
- **Hand Delivery:** If you submit written comments by hand or courier, please do so at 1200 New Jersey Avenue SE, West Building Ground Floor, Room W12-140, Washington, DC between 9 a.m. and 5 p.m. Eastern Time, Monday through Friday, except Federal holidays. To be sure someone is there to help you, please call 202-366-9826 before coming.

Instructions: For detailed instructions on submitting comments and additional information, see the Public Participation section of this document, which can be found below. Note that all comments received will be posted to <http://www.regulations.gov>, including any personal information provided.

Privacy Act: Anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the

comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT’s complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (65 FR 19477-78) or you may visit <https://www.transportation.gov/privacy>. If you wish to provide comments containing proprietary or confidential information, please follow the instructions in the section of this notice titled “*How do I submit confidential business information?*”

FOR FURTHER INFORMATION CONTACT:

To register for event attendance: Please contact Ms. Tuwana Taft, Office of Vehicle Safety Compliance, National Highway Traffic Safety Administration, 1200 New Jersey Avenue SE, Washington, DC 20590. Telephone: (202) 366-1008. Email: tuwana.taft@dot.gov. Participants must register in order for NHTSA to determine an approximate head count and in order for NHTSA to deliver site details and a final agenda to all participants. Attendance will not be permitted without prior registration.

For technical issues: Mr. Michael Brace, Compliance Engineer, Office of Vehicle Safety Compliance, National Highway Traffic Safety Administration, 1200 New Jersey Ave. SE, Washington, DC 20590. Telephone: 313-218-2265. Email: michael.brace@dot.gov.

For legal issues: Mr. Paul Connet, Attorney-Advisor, Office of the Chief Counsel, National Highway Traffic Safety Administration, 1200 New Jersey Avenue SE, Washington, DC 20590. Telephone: 202-366-5547. Email: paul.connet@dot.gov.

SUPPLEMENTARY INFORMATION: On May 2, 2022, NHTSA published a final rule which stated the agency’s intention to use a new test procedure to validate non-passenger automobile (“light truck”) classification data provided by manufacturers in their pre-model reports submitted under 49 CFR part 537.¹ NHTSA is providing a draft version of TP-523-00 for comment. TP-523-00 is intended to improve NHTSA’s ability to verify light truck compliance with 49 CFR 523.5(b)(2)(i) through (v) by providing guidelines for a uniform testing and information recording format for contracting laboratories who perform testing for NHTSA.

Introduction

To investigate whether specific vehicles or products comply with Corporate Average Fuel Economy (CAFE) regulations, NHTSA’s Office of

¹ 87 FR 26025.

Vehicle Safety Compliance (OVSC) contracts with labs to conduct compliance testing. The OVSC laboratory test procedures are prepared for the limited purpose of use by contracted independent laboratories conducting compliance tests for the OVSC. OVSC laboratory test procedures are not rules, regulations, or NHTSA interpretations, and OVSC laboratory test procedures are not intended to limit the requirements of the applicable regulations.

Background

NHTSA administers the CAFE program under authority granted in the Energy Policy and Conservation Act (EPCA) of 1975, as amended by the Energy Independence and Security Act (EISA) of 2007.² Per Congress, light-duty vehicles into two basic classes for CAFE compliance purposes: passenger automobiles (“passenger cars”) and non-passenger automobiles (“light trucks”).³ The statutory definitions for these classes indicate that “passenger automobiles” do *not* include vehicles that “the Secretary decides by regulation . . . has a significant feature (except for 4-wheel drive) designed for off-highway operation, and . . . is a 4-wheel drive automobile or rated at more than 6,000 pounds gross vehicle weight.”⁴ Because passenger automobiles do not include these vehicles, these vehicles must therefore belong to the non-passenger automobile (light truck) category. Note that Congress expressly directed DOT (by delegation, NHTSA) to determine what a “significant feature (except for 4-wheel drive) designed for off-highway operation” would include.

To implement this Congressional directive to determine significant features designed for off-highway operation, NHTSA promulgated 49 CFR 523. Part 523 defines five different attributes of off-highway operation: “approach angle,”⁵ “breakover angle,”⁶ “departure angle,”⁷ “running

clearance,”⁸ and “front and rear axle clearance.”⁹ Section 523.5(b) describes how a vehicle may qualify as a non-passenger automobile (light truck) through off-highway operation capabilities. Specifically, NHTSA defined measurement criteria for each of the five attributes of off-highway operation,¹⁰ and a vehicle must meet the measurements for at least four out of those five attributes to qualify as an “off-highway capable” light truck.

NHTSA requires manufacturers to provide NHTSA dimension information for approach angle, breakover angle, departure angle, running clearance, and front and rear axle clearance for vehicles they wish to claim as off-highway capable as part of their pre- and mid-model year reports under 49 CFR 537.7(c)(5)(ii). Accurate information about these dimensions is critical for verifying a manufacturer’s CAFE compliance information, because if the information is inaccurate, it may be possible that a vehicle would not qualify as a non-passenger automobile (light truck). NHTSA will use TP–523–00 to verify that submitted dimension measurements these attributes are accurate and to confirm that vehicles have been properly classified accordingly. TP–523–00 also provides guidance regarding the expected precision of measurements and the allowable rounding approach for off-highway vehicle clearances and angles, as well as for reporting values in manufacturer’s pre-model year (PMY) and mid-model year (MMY) reports.

NHTSA publishes OVSC laboratory test procedures on NHTSA’s website so that interested parties may see how NHTSA is instructing its contracted labs to collect data to help OVSC investigate whether vehicles and vehicle equipment sold in the U.S. comply with certain regulatory requirements. A manufacturer should not depend solely on the test reports produced as a result of OVSC’s laboratory testing as the basis for certification that its vehicle or item of motor vehicle equipment complies with all applicable regulatory requirements, as OVSC’s laboratory tests establish whether a product’s attributes or performance passes or fails under some, but not necessarily all, conditions

and a line tangent to the rear tire static loaded radius arc and touching the underside of the automobile rearward of the rear tire. 49 CFR 523.2.

⁸ *Running clearance* means the distance from the surface on which an automobile is standing to the lowest point on the automobile, excluding unsprung weight. 49 CFR 523.2

⁹ *Axle clearance* means the vertical distance from the level surface on which an automobile is standing to the lowest point on the axle differential of the automobile.

¹⁰ 49 CFR 523.5(b)(2)(i)–(v).

and procedures described in NHTSA regulation. The findings in those reports are the findings of the test laboratory, and the OVSC uses these results as a part of its determination of a non-compliance.

OVSC Laboratory Test Procedure Draft and Request for Comment

To provide further information to stakeholders regarding how TP–523–00 would work in practice, NHTSA will hold a demonstration that stakeholders may attend in person. The scope of this demonstration is strictly limited to issues surrounding the implementation of the OVSC Laboratory Test Procedure TP–523.

NHTSA also invites public comment on TP–523–00. Consequently, this notice serves as a request for comments (RFC). NHTSA will review and consider the feedback, and certain comments may be addressed during the workshop and demonstration event if submitted by November 30, 2024.

The RFC is strictly limited to the contents of OVSC laboratory test procedure TP–523–00 and the corresponding demonstration. NHTSA is not seeking comments at this time about amending either the vehicle classification requirements in 49 CFR 523 nor the standards described in 49 CFR 531 or 49 CFR 533. TP–523–00 is available for viewing in PDF format in the Docket identified in the heading of this document.

Public Participation

How do I prepare and submit comments?

Your comments must be written and in English. To ensure that your comments are correctly filed in the Docket, please include the docket number indicated in this document in your comments.

Please limit your comments to 15 pages. We established this limit to encourage you to write your primary comments in a concise fashion. However, you may attach necessary additional documents to your comments. There is no limit on the length of the attachments.

If you are submitting comments electronically as a PDF (Adobe) file, NHTSA asks that the documents be submitted using the Optical Character Recognition (OCR) process, thus allowing NHTSA to search and copy certain portions of your submissions.

Please note that pursuant to the Data Quality Act, in order for substantive data to be relied upon and used by the agency, it must meet the information quality standards set forth in the OMB

² NHTSA’s authority is codified at 49 U.S.C. 32901 *et seq.*

³ 49 U.S.C. 32901, 32902.

⁴ 49 U.S.C. 32901.

⁵ *Approach angle* means the smallest angle, in a plane side view of an automobile, formed by the level surface on which the automobile is standing and a line tangent to the front tire static loaded radius arc and touching the underside of the automobile forward of the front tire. 49 CFR 523.2.

⁶ *Breakover angle* means the supplement of the largest angle, in the plan side view of an automobile that can be formed by two lines tangent to the front and rear static loaded radii arcs and intersecting at a point on the underside of the automobile. 49 CFR 523.2.

⁷ *Departure angle* means the smallest angle, in a plane side view of an automobile, formed by the level surface on which the automobile is standing

and DOT Data Quality Act guidelines. Accordingly, we encourage you to consult the guidelines in preparing your comments. OMB's guidelines may be accessed at <https://www.transportation.gov/regulations/dot-information-dissemination-quality-guidelines>.

How can I be sure that my comments were received?

If you submit comments by hard copy and wish Docket Management to notify you upon its receipt of your comments, enclose a self-addressed, stamped postcard in the envelope containing your comments. Upon receiving your comments, Docket Management will return the postcard by mail. If you submit comments electronically, your comments should appear automatically in the Docket identified in the heading of this document on www.regulations.gov. If they do not appear within two weeks of posting, NHTSA suggests that you call the Docket Management Facility at (202) 366-9826.

How do I submit confidential business information?

You should submit a redacted "public version" of your comment (including redacted versions of any additional documents or attachments) to the Docket using any of the methods identified under **ADDRESSES**. This "public version" of your comment should contain only the portions for which no claim of confidential treatment is made and from which those portions for which confidential treatment is claimed has been redacted. See below for further instructions on how to do this.

You also need to submit a request for confidential treatment directly to the Office of the Chief Counsel. Requests for confidential treatment are governed by 49 CFR part 512. Your request must set forth the information specified in part 512. This includes the materials for which confidentiality is being requested (as explained in more detail below); supporting information, pursuant to Section 512.8; and a certificate, pursuant to Section 512.4(b) and Part 512, appendix A.

You are required to submit to the Office of the Chief Counsel one unredacted "confidential version" of the information for which you are seeking confidential treatment. Pursuant to Section 512.6, the words "ENTIRE PAGE CONFIDENTIAL BUSINESS INFORMATION" or "CONFIDENTIAL BUSINESS INFORMATION CONTAINED WITHIN BRACKETS" (as applicable) must appear at the top of

each page containing information claimed to be confidential. In the latter situation, where not all information on the page is claimed to be confidential, identify each item of information for which confidentiality is requested within brackets: "[]."

You are also required to submit to the Office of the Chief Counsel one redacted "public version" of the information for which you are seeking confidential treatment. Pursuant to Section 512.5(a)(2), the redacted "public version" should include redactions of any information for which you are seeking confidential treatment (*i.e.*, the only information that should be unredacted is information for which you are not seeking confidential treatment).

NHTSA is currently treating electronic submission as an acceptable method for submitting confidential business information to the agency under Part 512. Please do not send a hardcopy of a request for confidential treatment to NHTSA's headquarters. The request should be sent to Dan Rabinovitz in the Office of the Chief Counsel at daniel.rabinovitz@dot.gov. You may either submit your request via email or request a secure file transfer link. If you are submitting the request via email, please also email a courtesy copy of the request to Paul Connet at paul.connet@dot.gov.

Will the agency consider late comments?

In our response, we will consider all comments that Docket Management receives before the close of business on the comment closing date indicated above under **DATES**. To the extent possible, we may also consider comments that Docket Management receives after that date.

How will the agency utilize comments received?

Comments received ahead of the workshop and demonstration may be addressed at the event. The agency will consider all comments received and will incorporate comments as it deems appropriate into the OVSC laboratory test procedure.

How can I read the comments submitted by other people?

You may read the comments received by Docket Management at the address given above under **ADDRESSES**. The hours of the Docket are indicated above in the same location. You may also see the comments on the internet, at www.regulations.gov, identified by the

docket number at the heading of this notice.

Otto G. Matheke III,
Director, Office of Vehicle Safety Compliance.
[FR Doc. 2024-25069 Filed 10-28-24; 8:45 am]
BILLING CODE 4910-59-P

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

Agency Information Collection Activities: Revision of an Approved Information Collection; Comment Request; Company-Run Annual Stress Test Reporting Template and Documentation for Covered Institutions With Total Consolidated Assets of \$250 Billion or More Under the Dodd-Frank Wall Street Reform and Consumer Protection Act

AGENCY: Office of the Comptroller of the Currency (OCC), Treasury.

ACTION: Notice and request for comment.

SUMMARY: The OCC, as part of its continuing effort to reduce paperwork and respondent burden, invites comment on a continuing information collection, as required by the Paperwork Reduction Act of 1995 (PRA). In accordance with the requirements of the PRA, the OCC may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number. The OCC is soliciting comment concerning a revision to its information collection titled "Company-Run Annual Stress Test Reporting Template and Documentation for Covered Institutions with Total Consolidated Assets of \$250 Billion or More under the Dodd-Frank Wall Street Reform and Consumer Protection Act"

DATES: Comments must be received by December 30, 2024.

ADDRESSES: Commenters are encouraged to submit comments by email, if possible. You may submit comments by any of the following methods:

- *Email:* prainfo@occ.treas.gov.
- *Mail:* Chief Counsel's Office, Attention: Comment Processing, Office of the Comptroller of the Currency, Attention: 1557-0319, 400 7th Street SW, Suite 3E-218, Washington, DC 20219.

- *Hand Delivery/Courier:* 400 7th Street SW, Suite 3E-218, Washington, DC 20219.
- *Fax:* (571) 293-4835.

Instructions: You must include "OCC" as the agency name and "1557-

0319” in your comment. In general, the OCC will publish comments on www.reginfo.gov without change, including any business or personal information provided such as name and address information, email addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

Following the close of this notice’s 60-day comment period, the OCC will publish a second notice with a 30-day comment period. You may review comments and other related materials that pertain to this information collection beginning on the date of publication of the second notice for this collection by the method set forth in the next bullet.

- **Viewing Comments Electronically:** Go to www.reginfo.gov. Hover over the “Information Collection Review” tab and click on “Information Collection Review” from the drop-down menu. From the “Currently under Review” drop-down menu, select “Department of Treasury” and then click “submit.” This information collection can be located by searching OMB control number “1557–0319” or “Company-Run Annual Stress Test Reporting Template and Documentation for Covered Institutions with Total Consolidated Assets of \$250 Billion or More under the Dodd-Frank Wall Street Reform and Consumer Protection Act.” Upon finding the appropriate information collection, click on the related “ICR Reference Number.” On the next screen, select “View Supporting Statement and Other Documents” and then click on the link to any comment listed at the bottom of the screen.

- For assistance in navigating www.reginfo.gov, please contact the Regulatory Information Service Center at (202) 482–7340.

FOR FURTHER INFORMATION CONTACT: Shaquita Merritt, Clearance Officer, (202) 649–5490, Chief Counsel’s Office, Office of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219. If you are deaf, hard of hearing, or have a speech disability, please dial 7–1–1 to access telecommunications relay services.

SUPPLEMENTARY INFORMATION: Under the PRA (44 U.S.C. 3501 *et seq.*), Federal agencies must obtain approval from the OMB for each collection of information that they conduct or sponsor. “Collection of information” is defined

in 44 U.S.C. 3502(3) and 5 CFR 1320.3(c) to include agency requests or requirements that members of the public submit reports, keep records, or provide information to a third party. Section 3506(c)(2)(A) of title 44 generally requires Federal agencies to provide a 60-day notice in the **Federal Register** concerning each proposed collection of information, including each proposed extension of an existing collection of information, before submitting the collection to OMB for approval. To comply with this requirement, the OCC is publishing notice of the revision of this collection.

Title: “Company-Run Annual Stress Test Reporting Template and Documentation for Covered Institutions with Total Consolidated Assets of \$250 Billion or More under the Dodd-Frank Wall Street Reform and Consumer Protection Act.”

OMB Control No.: 1557–0319.

Type of Review: Revision.

Affected Public: Businesses or other for-profit.

Description: Section 165(i)(2) of the Dodd-Frank Wall Street Reform and Consumer Protection Act¹ (Dodd-Frank Act) requires certain financial companies, including national banks and federal savings associations, to conduct annual stress tests² and requires the primary financial regulatory agency³ of those financial companies to issue regulations implementing the stress test requirements.⁴ Under section 165(i)(2), a covered institution is required to submit to the Board of Governors of the Federal Reserve System (Board) and to its primary financial regulatory agency a report at such time, in such form, and containing such information as the primary financial regulatory agency may require.⁵

On October 9, 2012, the OCC published in the **Federal Register** a final rule implementing the section 165(i)(2) annual stress test requirement.⁶ This rule describes the reports and information collections required to meet the reporting requirements under section 165(i)(2). These information collections will be treated as confidential (to the extent permitted by law).⁷

In 2012, the OCC first implemented the reporting templates referenced in

the final rule.⁸ The OCC uses the data collected to assess the reasonableness of the stress test results of covered institutions and to provide forward-looking information to the OCC regarding a covered institution’s capital adequacy. The OCC also may use the results of the stress tests to determine whether additional analytical techniques and exercises could be appropriate to identify, measure, and monitor risks at the covered institution. The stress test results are expected to support ongoing improvement in a covered institution’s stress testing practices with respect to its internal assessments of capital adequacy and overall capital planning.

The OCC recognizes that many covered institutions with total consolidated assets of \$250 billion or more are required to submit reports using reporting form FR Y–14A.⁹ The OCC also recognizes the Board has proposed modifications to the FR Y–14A and, to the extent practical, the OCC will keep its reporting requirements consistent with the Board’s FR Y–14A in order to minimize burden on covered institutions.¹⁰

The OCC’s proposed changes include only limited updates to reflect the changes made by the Board, and the proposed OCC reporting forms will substantially resemble the forms used by the OCC last year. The OCC’s proposed changes include removing the CECL Supplemental Schedule from the reporting instructions. The CECL Supplemental Schedule was a one-time schedule that reporting banks provided the during the first submission cycle following their implementation of the ASU 2016–13 standards. This collection was implemented to identify the effect and timing of the adoption of CECL and the associated transition provisions, as provided by section 301 of the regulatory capital rules. As all firms have now adopted ASU 2016–13, this supplemental collection is not needed on a going-forward basis for modeling or analytical purposes. The proposed changes also include a small number of revisions that do not stem from revisions proposed by the Board. These include minor corrections and eliminating references to LIBOR, which is no longer a reference rate, in the instructions.

If the Board proposes additional changes to the FR Y–14A reporting forms after the publication of this notice, the OCC expects to make

¹ Public Law 111–203, 124 Stat. 1376, July 2010.

² 12 U.S.C. 5365(i)(2)(A).

³ 12 U.S.C. 5301(12).

⁴ 12 U.S.C. 5365(i)(2)(C).

⁵ 12 U.S.C. 5365(i)(2)(B).

⁶ 77 FR 61238 (October 9, 2012) (codified at 12 CFR part 46).

⁷ 5 U.S.C. 552(b)(4).

⁸ See 77 FR 49485 (August 16, 2012) and 77 FR 66663 (November 6, 2012).

⁹ <http://www.federalreserve.gov/reportforms>.

¹⁰ 89 FR 52042 (June 21, 2024).

corresponding changes to the OCC reporting forms to minimize inconsistencies and reduce burden. The OCC's proposed new reporting forms and instructions are available on the OCC's website at <https://www.occ.treas.gov/publications-and-resources/forms/dodd-frank-act-stress-test/index-dodd-frank-act-stress-test.html>.

Estimated Burden

Estimated Frequency of Response: On occasion.

Estimated Number of Respondents: 4 annually and 4 biennially.

Estimated Total Annual Burden: 3,558 hours.

Comments submitted in response to this notice will be summarized and included in the request for OMB approval. All comments will become a matter of public record. Comments are invited on:

(a) Whether the collection of information is necessary for the proper performance of the functions of the OCC, including whether the information has practical utility;

(b) The accuracy of the OCC's estimate of the burden of the collection of information;

(c) Ways to enhance the quality, utility, and clarity of the information to be collected;

(d) Ways to minimize the burden of the collection on respondents, including through the use of automated collection techniques or other forms of information technology; and

(e) Estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information.

Patrick T. Tierney,

Assistant Director, Office of the Comptroller of the Currency.

[FR Doc. 2024-25037 Filed 10-28-24; 8:45 am]

BILLING CODE 4810-33-P

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

Agency Information Collection Activities: Information Collection Renewal; Submission for OMB Review; International Regulation—Part 28

AGENCY: Office of the Comptroller of the Currency (OCC), Treasury.

ACTION: Notice and request for comment.

SUMMARY: The OCC, as part of its continuing effort to reduce paperwork and respondent burden, invites comment on a continuing information

collection, as required by the Paperwork Reduction Act of 1995 (PRA). In accordance with the requirements of the PRA, the OCC may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number. The OCC is soliciting comment concerning the renewal of its information collection titled, "International Regulation—Part 28." The OCC also is giving notice that it has sent the collection to OMB for review.

DATES: Comments must be received by November 29, 2024.

ADDRESSES: Commenters are encouraged to submit comments by email, if possible.

You may submit comments by any of the following methods:

- *Email:* prainfo@occ.treas.gov.

- *Mail:* Chief Counsel's Office, Attention: Comment Processing, Office of the Comptroller of the Currency, Attention: 1557-0102, 400 7th Street SW, Suite 3E-218, Washington, DC 20219.

- *Hand Delivery/Courier:* 400 7th Street SW, Suite 3E-218, Washington, DC 20219.

- *Fax:* (571) 293-4835.

Instructions: You must include "OCC" as the agency name and "1557-0102" in your comment. In general, the OCC will publish comments on www.reginfo.gov without change, including any business or personal information provided, such as name and address information, email addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

Written comments and recommendations for the proposed information collection should also be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. You can find this information collection by selecting "Currently under 30-day Review—Open for Public Comments" or by using the search function.

You may review comments and other related materials that pertain to this information collection following the close of the 30-day comment period for this notice by the method set forth in the next bullet.

- *Viewing Comments Electronically:* Go to www.reginfo.gov. Hover over the

"Information Collection Review" tab and click on "Information Collection Review" from the drop-down menu. From the "Currently under Review" drop-down menu, select "Department of Treasury" and then click "submit." This information collection can be located by searching OMB control number "1557-0102" or "International Regulation—Part 28." Upon finding the appropriate information collection, click on the related "ICR Reference Number." On the next screen, select "View Supporting Statement and Other Documents" and then click on the link to any comment listed at the bottom of the screen.

- For assistance in navigating www.reginfo.gov, please contact the Regulatory Information Service Center at (202) 482-7340.

FOR FURTHER INFORMATION CONTACT:

Shaquita Merritt, Clearance Officer, (202) 649-5490, Chief Counsel's Office, Office of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219. If you are deaf, hard of hearing, or have a speech disability, please dial 7-1-1 to access telecommunications relay services.

SUPPLEMENTARY INFORMATION: Under the PRA (44 U.S.C. 3501 *et seq.*), Federal agencies must obtain approval from the OMB for each collection of information that they conduct or sponsor.

"Collection of information" is defined in 44 U.S.C. 3502(3) and 5 CFR 1320.3(c) to include agency requests or requirements that members of the public submit reports, keep records, or provide information to a third party. The OCC asks the OMB to extend its approval of the collection in this notice.

Title: International Regulation—Part 28.

OMB Control No.: 1557-0102.

Type of Review: Regular.

Affected Public: Businesses or other for-profit.

Description: This submission covers an existing regulation and involves no change to the regulation or to the information collection requirements. The OCC requests only that OMB extend its approval of the information collection.

12 CFR 28.3 Filing Requirements for Foreign Operations of a National Bank—Notice Requirement

Under 12 CFR 28.3(a), a national bank shall notify the OCC when it (1) files an application, notice, or report with the Board of Governors of the Federal Reserve System (FRB) to establish or open a foreign branch; or acquire or divest of an interest in, or close, an Edge corporation, Agreement corporation, foreign bank, or other foreign

organization; or (2) opens a foreign branch and no application or notice is required by the FRB for such transaction. Section 28.3(b) provides that in lieu of a notice, the OCC may accept a copy of an application, notice, or report submitted to another Federal agency that covers the proposed action and contains substantially the same information required by the OCC. Pursuant to § 28.3(c), the OCC may require additional information in the form of an application from a national bank seeking to join a foreign exchange, clearinghouse, or similar type of organization. A national bank shall furnish the OCC with any additional information the OCC may require in connection with the national bank's foreign operations.

12 CFR 28.14(c) Limitations Based Upon Capital of a Foreign Bank—Aggregation

A foreign bank shall aggregate business transacted by all Federal branches and agencies with the business transacted by all state branches and agencies controlled by the foreign bank in determining its compliance with limitations based upon the capital of the foreign bank. A foreign bank shall designate one Federal branch or agency office in the United States to maintain consolidated information so that the OCC can monitor compliance.

12 CFR 28.15(d), (d)(1), (d)(2), and (f) Capital Equivalency Deposits

Under § 28.15(d), a foreign bank should require its depository bank to segregate its capital equivalency deposits (CED) on the depository bank's books and records. Pursuant to § 28.15(d)(2), the instruments making up the CED that are placed in safekeeping at a depository bank to satisfy a foreign bank's CED requirement must be maintained pursuant to an agreement prescribed by the OCC that shall be a written agreement entered into with the OCC. Section 28.15(f) further provides that each Federal branch or agency shall maintain a capital equivalency account and keep records of the amount of liabilities requiring capital equivalency coverage in a manner and form prescribed by the OCC. Finally, under § 28.15(d)(1), a foreign bank's CED may not be reduced in value below the minimum required for that branch or agency without the prior approval of the OCC, but in no event may the value fall below the statutory minimum.

12 CFR 28.16(c) Deposit-Taking by an Uninsured Federal Branch—Application for an Exemption

A foreign bank may apply to the OCC for an exemption to permit an uninsured Federal branch to accept or maintain deposit accounts that are not listed in § 28.16(b). The request should describe the types, sources, and estimated amount of such deposits and explain why the OCC should grant an exemption, and how the exemption maintains and furthers the policies described in § 28.16(a).

12 CFR 28.16(d) Deposit-Taking by an Uninsured Federal Branch—Aggregation of Deposits

A foreign bank that has more than one Federal branch in the same state may aggregate deposits in all of its Federal branches in that state, but exclude deposits of other branches, agencies, or wholly owned subsidiaries of the bank. The Federal branch shall compute the average amount by using the sum of deposits as of the close of business of the last 30 calendar days ending with, and including, the last day of the calendar quarter, divided by 30. The Federal branch shall maintain records of the calculation until its next examination by the OCC.

12 CFR 28.18(c)(1) Recordkeeping and Reporting—Maintenance of Accounts, Books, and Records

Each Federal branch or agency shall maintain a set of accounts and records reflecting its transactions that are separate from those of the foreign bank and any other branch or agency. The Federal branch or agency shall keep a set of accounts and records in English sufficient to permit the OCC to examine the condition of the Federal branch or agency and its compliance with applicable laws and regulations.

12 CFR 28.20(a)(1) Maintenance of Assets—General Rule

The OCC may require a foreign bank to hold certain assets in the state in which its Federal branch or agency is located.

12 CFR 28.22(e) Voluntary Liquidation—Reports of Examination

The Federal branch or agency shall send the OCC certification that all of its Reports of Examination have been destroyed or return its Reports of Examination to the OCC.

Estimated Burden: \$296,843.60.

Estimated Frequency of Response: On occasion.

Estimated Number of Respondents: 52.

Estimated Total Annual Burden: 2,294 hours.

Comments: On August 23, 2024, the OCC published a 60-day notice for this information collection, (89 FR 68240). No comments were received.

Comments continue to be invited on:

(a) Whether the collection of information is necessary for the proper performance of the functions of the OCC, including whether the information has practical utility;

(b) The accuracy of the OCC's estimate of the burden of the collection of information;

(c) Ways to enhance the quality, utility, and clarity of the information to be collected;

(d) Ways to minimize the burden of the collection on respondents, including through the use of automated collection techniques or other forms of information technology; and

(e) Estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information.

Patrick T. Tierney,

Assistant Director, Office of the Comptroller of the Currency.

[FR Doc. 2024-25031 Filed 10-28-24; 8:45 am]

BILLING CODE 4810-33-P

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Action

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the removal of a person currently on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of this person is unblocked, and U.S. persons are permitted to engage in lawful transactions with them.

DATES: This action was issued on October 23, 2024. See **SUPPLEMENTARY INFORMATION** for relevant dates.

FOR FURTHER INFORMATION CONTACT: OFAC: Associate Director for Global Targeting, 202-622-2420; or Assistant Director for Sanctions Compliance, 202-622-2490 or <https://ofac.treasury.gov/contact-ofac>.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The SDN List and additional information concerning OFAC sanctions programs are available on OFAC's website: <https://ofac.treasury.gov>.

Notice of OFAC Action

On October 23, 2024, OFAC removed from the SDN List the person listed below, who was subject to prohibitions imposed pursuant to E.O. 13661.

Individual

1. SEMENOVA, Olena Yurevna (a.k.a. SEMENOVA, Elena Iurevna); DOB 06 Dec 1978; citizen Ukraine; Secondary sanctions risk; Ukraine-/Russia-Related Sanctions Regulations, 31 CFR 589.201 and/or 589.209; Passport ER747251 (Ukraine); National ID No. 2882908207 (Ukraine) (individual) [UKRAINE-EO13661].

Lisa M. Palluconi,

Acting Director, Office of Foreign Assets Control.

[FR Doc. 2024-25068 Filed 10-28-24; 8:45 am]

BILLING CODE 4810-AL-P

DEPARTMENT OF THE TREASURY**Office of Foreign Assets Control****Notice of OFAC Sanctions Action**

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the names of one or more persons that have been placed on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of these persons are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

DATES: This action was issued on October 24, 2024. See **SUPPLEMENTARY INFORMATION** section for relevant date(s).

FOR FURTHER INFORMATION CONTACT:

OFAC: Associate Director for Global Targeting, 202-622-2420; or Assistant Director for Sanctions Compliance, 202-622-2490 or <https://ofac.treasury.gov/contact-ofac>.

SUPPLEMENTARY INFORMATION:**Electronic Availability**

The SDN List and additional information concerning OFAC sanctions programs are available on OFAC's website: <https://ofac.treasury.gov>.

Notice of OFAC Action

On October 24, 2024, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following person is blocked under the relevant sanctions authority listed below.

Individual

SULEIMAN, Mirghani Idris (a.k.a. IDRIS, Margani Idries Suliman (Arabic: (ميرغني ادريس سليمان ادريس); a.k.a. IDRIS, Al-Mirghani; a.k.a. SULEIMAN, El Mirghani Idris; a.k.a. SULEIMAN, Mirghani Idriiss), H 22 B 7, Northern Elsafia, Bahri, Khartoum, Sudan; DOB 28 Dec 1959; POB Bahri, Khartoum, Sudan; nationality Sudan; Gender Male; Passport B00018824 (Sudan) expires 09 May 2023 (individual) [SUDAN-EO14098].

Designated pursuant to section 1(a)(ii)(A) of Executive Order 14098 of May 4, 2023, "Imposing Sanctions Certain Persons Destabilizing Sudan and Undermining the Goal of a Democratic Transition," for being a foreign person who is or has been a leader, official, senior executive officer, or member of the board of directors of the Rapid Support Forces, an entity that has, or whose members have, been responsible for, or complicit in, or to have directly or indirectly engaged or attempted to engage in actions or policies that threaten the peace, security, or stability of Sudan, relating to the tenure of such leader, official, senior executive officer, or member of the board of directors.

Lisa M. Palluconi,

Acting Director, Office of Foreign Assets Control.

[FR Doc. 2024-25121 Filed 10-28-24; 8:45 am]

BILLING CODE 4810-AL-P

DEPARTMENT OF THE TREASURY**Internal Revenue Service****Quarterly Publication of Individuals, Who Have Chosen To Expatriate**

AGENCY: Internal Revenue Service (IRS), Treasury.

ACTION: Notice.

SUMMARY: This notice is provided in accordance with IRC section 6039G of the Health Insurance Portability and

Accountability Act (HIPAA) of 1996, as amended. This listing contains the name of each individual losing United States citizenship (within the meaning of section 877(a) or 877A) with respect to whom the Secretary received information during the quarter ending September 30, 2024. For purposes of this listing, long-term residents, as defined in section 877(e)(2), are treated as if they were citizens of the United States who lost citizenship.

SUPPLEMENTARY INFORMATION:

Last name	First name	Middle name/initials
AASEN	ERIK	PHARR
ABBOT	BARBARA	ANNE
ABE	NAOMI.	
ABE	MASAMICHI.	
ABOU SAAB	SAMI.	
ABRAM	MARY	JACQUELINE
ABRAM	DARRYL	WAYNE
ABRAMS	MARGARET	LOUISA
ACHMANN	BRITTA.	
ACKERMAN	JEFFREY	M
ADAMS	RICHARD	GLENN
ADAMSON	SARA	ELIZABETH
ADAMSON	SHELLEY	LYNNE
ADAMYK	FRANCOISE	MARTHE
ADELMAN	IRENA	JOY
ADENLOF	EMELIE	ELIZABETH
ADRIANOPOULOS	ANDREW.	
AEBISCHER	STEVEN	WALTER MARCEL
AESCHLIMANN	FRANCESKA.	
AGAR	SOPHIE	ELIZABETH
AGNELLO	ROSANNE.	
AHN	MICHAEL.	
AHN	RACHAEL	SEYUN
AIELLO	ANTONY	NICOLAS
AL HUMOOD	MALIK	MOHAMMED
ALBERT	CORISANDE	CHARLOTTE
ALBERTS	NICOLE	MARY
ALBOKAE	NATAN.	
ALEXANDER	AIYANA.	
ALIOTH	REMI	ANTOINE
ALLEN	BRIAN.	
ALLEN	PATRICIA	JEAN
ALLEN	WILLIAM	MONTGOMERY
ALLISON	CYNTHIA	WILLIAMS
ALPERN	STEPHANE	NATHAN
ALTNEU	DANIEL	JAMES
ALTSTOCK	KASEY	M
AMICK	BENJAMIN	CARLISLE
AMMETER	FRANK	RICHARD
AN	KYUNGMIN	MIN
ANDERSEN	JACLYN	CHRISTINE
ANDERSEN	TADD	JONATHAN
ANDERSON	MICHAEL	FREDERICK
ANDERSON	VALERIE	JENNIE KARLINSKY
ANDERSON	BRUCE	FRULAND
ANDERSON	STEVEN	STANFORD
ANDREAS	KATHARINA	SOPHIE
ANDREAS	BERND	ALWIN
ANKESHIAN	ARA	HOVANES
ANTONIOLI	JANA	A
AOYAGI	NAOKO.	
AOYAGI	YASUO.	
AOYAGI	FUMI.	
APPLEGARTH	JANE	MARGARET
APPLETON	JEFFREY	TODD
ARAN EROL	IPEK	ZEYNEP
ARIGA	HANA.	
ARIMA	KAZUMASA.	
ARNOLD	CORINNA	MARIA
ARNSTEIN	AHARON	DANIAL
AROCHO	RAUL.	
ARONEY	STEPHANIE	LOUISE
ASAO	KEIKO.	
ATCHARIYAWIRIYA	ALISA.	
ATSUCHI	SATOSHI.	
ATTIOGBE	DOROTHEA	SEPOPO
AUBRET	FRANCOIS	MAURICE ETIENNE
AUER	MELANIE	NICOLE
AUFGANG	BARBARA	BENJAMIN
AUGRAND	LUCIE	CAROLINA OLIVIA
AUGRAND	SAMANTHA E	EMILY DINWIDDLE
AULESTIA	IKER.	
AVALOS	FERNANDO	HUGO
AVERY	NATALIE	M

Last name	First name	Middle name/initials
AYRES	PHILIP	DAVID
AYVAZIAN	ELISABETH	
BACHMAN	WILLIAM	DAVID
BACHMANN	MIRNA	MURIEL
BACK	BRIAN	A
BADDIRI	BARCILIN	TAPSIRIL
BAI	GENG	
BAIDA	Yael	
BAILEY	BILL	HENRY
BAILEY	CYNTHIA	MARIE
BAIRD	DONNA	JANE
BAJUELOS DOMINGUEZ	ANTONIO	LESLIE
BAKER	CAROLYN	
BALL	CARRIE	LOU
BALLERSCHEFF	ULRIKE	
BALLET	PHILIPPE	JEAN
BALLINGER	MARTIME	MARIE
BANNISTER	CECIL	H
BAPTISTA	ADRIANO	AUDO-GIANOTTI
BARBER	KATHERINE	JANE
BARDAS	ANNA	
BARELA	HANAKO	KAWABE
BARNARD	JIMMY	SHAUN
BARNES	BRIAN	PRESTON
BARNES	JONATHAN	IAN
BARNES	JACQUELINE	
BARNES	GERALDINE	MAE
BARR	GLENN	DOUGLAS
BARR	DANIEL	WILLIAM
BARRY	JENNIFER	SEARS
BARTH	GAIL	ELIZABETH
BARTON	DAVID	STEVEN
BASHUTSKI	JILL	DAWN
BASSAL	ALANA	DANIELLE
BASSAL	LORI	BETH
BASSAL	DAVID	JONATHAN
BASSANO	HEIDI	ANTOINETTE
BASTAMI	SOHAILA	SAHAR
BATES	PAULA	JANE
BATEY	MARK	
BAUER	STEPHANIE	ANN
BAUMGARTNER	NICOLE	KIM
BAUTISTA CONEJERO	MARINA	LUISA
BAWAZIR	HASHEM	ABDULAH
BAYLEY	DEREK	MOLINEUX
BEALS	KATHRYN	ELIZABETH
BEARFIELD	GEORGE	JOSEPH
BEAUMONT	JACQUELINE	
BEEVOR	MARK	ANDREW
BEHRSTOCK	JEREMY	
BEIGEL	CLAUDE	YVES
BELL	JUNKO	YAMADA
BELL	EDWIN	JAMES
BELL	PATRICIA	JEAN
BELL	DONALD	JAMES
BELL	DEBBIE	GAYE
BELL	CHARLOTTE	E
BELL	JOANNE	ELIZABETH
BELLAMY	KATHARINA	
BELLAVITI	SAMUEL	EMMANUEL
BELLO	ALICE	ALMA CELINE
BENDER	DOROTHEA	EVA MARIA EM
BENNETT	ELEANOR	KATHLEN
BENNIS	ALEXANDRA	FAYE
BENNY	DIANE	MARIE
BERGAN	MARIE	S
BERGERON	NOEMIE	CASSIOPE REGINE BESSETTE
BERGIN	LOUISE	GENEVIEVE
BERGMAN	DAVID	MARCUS
BERKE	STEVE	
BERNSTEIN	DAVID	M
BERRIS	DANIEL	JOHN
BERRY	LINDSAY	ANN
BERRY	SUSAN	EMILY

Last name	First name	Middle name/initials
BERTIN	GEOFFREY	ROBERT
BERTIN	TERRY	LEE
BESINS	DAVID	ALEXIS THIERRY PAUL
BEWSHER CAMPBELL	PENELOPE	IBOLYKA
BHARWANI	LAVINA	DEVIDAS
BIET	SAMANTHA	MARIE SOLON
BIJON	DUBRAVKA	MATIC
BINGLEY	WILLIE	JUNIOR
BIRD	TERRY	H
BIRGY	JEAN	EUDES GERALD
BIRKENBERG	BEATRICE	ANNE ROSE
BISTANY	KATHRYN	THERESE
BITTING	NATHAN	SCOTT
BIZEK	MARK	
BLACK	JOSEPH	ANDREW
BLACK	DIANA	MARGARET SUSAN
BLACKLAWS	CAROL	TODD
BLAKNEY	CATHRYN	DORION COLETT
BLANKENSHIP	BRENDA	LYNN
BLOW	STEPHEN	CHARLES
BLYTH	GEORGINA	RUTH
BOBOWSKI	NAULA	KATHERINE
BOGOIEVSKI	KARLOS	JOSEPH
BOGOIEVSKI	KOSTA	ROBERT
BOLT	ANETT	
BOND	CAMERON	MARSHALL
BONIN	STACY	NOEL
BONNETT	ANDREA	MARGOT
BONNETT	STEWART	ANTHONY
BORLE	ALAIN	GERALD
BORM	HEATHER	LYNN
BOSCARIOL	KIMBERLY	MARIE SMITH
BOSSHARDT	CHRISTOPHER	MARTIN
BOTTEQUIN	EZRA	AVRAHAM
BOUDREAU	NANCY	CHRISTINE
BOURQUE	RONALD	JOSEPH
BOWREY	WILLIAM	JOSEPH
BOYCE	LAURA	JOAN
BOYD	NEIL	THOMAS
BOYLE	GRAEME	WILLIAM
BOYLES	KATHERINE	ELIZABETH
BRADLEY	AGNES	
BRANCH	PATRICK	JOHN
BRAND	CATHY	LYNN
BRANDHORST	BRUCE	PETER
BRANDT	JANET	LYNN
BRASH	RUTH	MARGARET
BRASSEUR	CHRISTINE	HODGE
BRAZILLE	JEREMY	CLINT
BREEZE	CATHLEEN	MARY
BREHON	JILL	WOODROFFE
BRENDON	CAMILA	HELEN
BRENDON	RICHARD	EDGAR
BRETT	DEREK	BENJAMIN
BREUER	RAPHAEL	
BRICCHI	IGNACIO	
BRIDGES	MARK	P
BRIEMBERG	HANNAH	
BRIKMAN	HADAR	
BRINKERHOFF	BENJAMIN	LOUIS
BRINKERHOFF	ELISSA	J
BRINKERHOFF	TANYA	
BRINSMEAD	CAROL	KIMBERLY
BROILLET	JOEL	
BROMLEY	LAURA	KIRSTEN
BROUGHTON	JOANNE	
BROUGHTON	SEAN	WILLIAM
BROUX	JEREMY	FRANCOIS BERNARD
BROWN	ELIOT	SALANOY
BROWN	MATTHEW	JAMES
BROWN	SEBASTIAN	WILLIAM GEORGE
BROWN	MICHAEL	CHARLES
BROWN	TINA	L
BROWN	COLIN	CHARLES

Last name	First name	Middle name/initials
BROWN	MICHELLE	ANDREE
BROWNE	KATHARINE	NAOMI WHITFIELD
BRUCE	SUSAN.	
BRYAN	DANIEL	NEIL
BRYERS	DOREEN	MABLE
BSCHIERL	FRANK	RUDI
BUCHANAN-SLOVITT	AMANDA	J
BUCK	AKIKO.	
BUFFINGTON	CORAL	MAY
BUFFINGTON	JOHN	FRANCIS
BUHLER	LUKAS	SAMUEL
BULL	ROBERT	JOHN
BULLIS	DAVID	CURTIS
BURKE	SUSAN	ANNE
BURKE	EMILY	MEGHAN
BURKE	DANIEL	THOMAS
BURLA	ALICE.	
BURNAY	MARIE	BERENICE JULIE
BURNETT	RACHEL	HELENA
BURTON	KATARINA.	
BURTON	KATHARINE	JILL ZOE
BUSBY	CHIE.	
BUSCH	BARBARA	ANN
BUSH	HIROKO	MACHAMA
BUTLER	DARRYL	LEONARD
BUTLER	MEGAN	JENNIE
BUTTON	DIANE	COLLEEN
BUX	IQBAI	YAKUB
CABRA	MYRIAM	LUCIA
CADWALLADER	HANNAH	P
CADY	DEBORAH	O'LEARY
CALDWELL	MARVA	MUIR
CALLAN	PAMELA	KAY
CALLISON	JAMIE	CHRISTOPHER
CALLISON	JAMES	DANIEL
CAMERON	VICTORIA	LOUISE
CAMERON	ADRIAN	JAMES MCIVER
CAMPAIGNOLLE	MARGOT	SOPHIE
CAMPBELL	JULIA	MARIE
CAMPBELL	JOAN.	
CAMPBELL	MADELEINE	LOUISE
CANNING	SINEAD	EIMIR
CANOVAS-BARROSO	RODRIGO	ANTONIO
CANSANI	MARTINO.	
CANTRELL	CLINTON	JAMES
CAP	LINDA	LEE
CAPEL-BIRD	CLEMENCY	GEORGIA
CARNER	BENJAMIN	RYAN
CARNER	AVA	RENEE
CARNER	BEAU	PATRICK
CAROTA	LINDA.	
CARR	SEAN	RILEY
CARROLL	SEAN	FRANCIS
CARTER	KANAE	KASHII
CARTER	FRANCESCA	SKYE
CARUSS	ALEXANDRA	ROSE
CASBAS-HERNANDEZ	PATRICIA.	
CASHMAN	JAMES	PATRICK
CASSELLIS	LOGAN	LEE
CASTELLA	HARRY	OLIVER
CASTRO	SAMUEL	ELEAZAR
CAULFIELD	TIMOTHY	ALLEN
CAULFIELD	DAVID	CASE
CAVAGNARO	TIMOTHY	RICHARD
CAVALIER	CATHERINE	DOROTHY
CAVANAGH	JUSTINE.	
CERENZLA	SANDRA	JEANNE
CERNA	DAVID	MICHAEL
CHAIKEN	LAURIE	SYMA
CHALLANDER	CHAMPION	SHENG JIE OSCAR
CHAN	MARY	YEE MUN
CHAN	TERENCE	PUI HIN
CHANG	WAKAM.	
CHANG	MING-JANG.	

Last name	First name	Middle name/initials
CHANN	VEASNA.	
CHAPPELL	REBECCA	ELIZABETH
CHARBONNEAU	LOUISE	MARIE JEANNE
CHARLTON	ALAN	STEPHEN
CHARLTON	GRACE	MARY
CHARNOCK	CATHERINE	RUTH
CHARPENTIER	CEDRIC	JEAN JACQUES
CHARPENTIER	ELSA	MEGANE
CHARTIER	JOFFREY	W
CHATELAIN	ANDREE	RENEE
CHAUDHARY	VIJAY	LAXMI
CHAUDHARY	ANOOP	LAL
CHEHAB	CHRISTIAN	NAJI
CHEHAB	AVIS	DIANE
CHELESKI	CARL	ALEXANDER
CHEN	JUI	YI
CHEN	KUANG	JUNG
CHEN	WEI.	
CHEN	MIAN.	
CHENG	XINGYUN.	
CHENG	HO	FUNG G
CHERN	CHINN	RONG
CHEUNG	DAMIEN	CHING NOK
CHEUNG	VERONICA	YI KI
CHEW	CHIAT	NAUN
CHIANG	TE	CHENG
CHIN	FONG	LIN L
CHISHIMA	YOSHIKI.	
CHO	ILLHEE.	
CHOW	SUSAN	DANNEKER
CHOWDHARY	GEETA.	
CHRISTIE	COURTNEY	KATHLEEN
CHRISTLEY	PHILIPPA	ANNE JAYNE
CHUA	EVONNE	LAI PING
CHUNG	KANG	SUP
CLAFLIN	MATTHEW	GILES
CLAGHORN	PETER	WHITNEY
CLARK	AKANE	Y
CLARK	ANNALIE	RACHEL
CLARK	ANNE	MARIE
CLARK	PADDI	EVA
CLARK	GREGORY	SIMON
CLARKE	PREMA.	
CLARKE	DEMETRA	DARSAKLIS
CLARKE	CLARE	ALEV
CLARKE	AUGUSTA	ELFRIDA
CLARKE	MIA	LAUREN
CLIFFORD	BRADFORD	JOHN
CLISE	ERIN	BREWSTER
CLOUTIER	MYRIAM.	
COATES	DAVID	JEROME
COCKROFT	GARY	ANTHONY
CODACCI-PISANELLI	COSIMO	PIO
COGLIN-NEWMAN	LAUREL	JUANITA
COLAMARTINI	LAUREN	MICHELLE
COLAUTTI	JOANNE	MARIE
COLE	KIM	SUSAN
COLE	CLEA	ALEXANDRIA
COLLI	MAGALI	HUGUETTE LYDIE
COLLI	GREGOIRE	GUY JEAN CLAUDE
COLLIER	HAL	MECORNACK
COLLINS	BRIAN	STEWART
COLLINS	LAURIE	ADAIR
COLLINS	ASHLEY	READ
COLLINS	SARAH	JANE
COLLIS	JONATHON	AARON
COMEAU	CHRISTOPHER	JOHN
CONDON	KENT	P
CONGI	VANESSA	LOUISE
COOK	LUISA	JUNE NOEL
COPISAROW	RICHARD	MAURICE
COPLEY	NICHOLAS	PAUL
CORBETT	PHILIP	DAVID
CORDIER TRICARICO	CAROLINE	ANNE CHRISTINE

Last name	First name	Middle name/initials
CORDOVA	JORGE	ENRIQUE
CORETTI	MONICA	
CORMAGGI	SALVATORE	
CORMAGGI	ANTHONY	
CORMIER	DANIEL	PAUL
CORNELL	ROSEMARY	BETH
CORNU-THENARD	MAXIME	GEORGE
CORREIA	NUNO	FILIFE
COTTON	EMMA	JANE
COYLE	JAMIE	KATHERINE
COYLE	RYAN	D
CRAIG	DONALD	HAMILTON
CRAIG-GREEN	ROSEMARY	ANN
CRAMPTON	ROBERT	ARDEN
CRANE	MATTHEW	JOSEPH
CRAVEN-WILKINSON	JOCELYN	MARTHA
CRAWLEY	SUZANNE	CHRISTINE
CRAWLEY	PETER	L
CRONIN	MARI	
CROOK	JAMES	STEVEN
CUELLAR	YANIRA	GUADALUPE
CUNNINGHAM	CHRISTINE	MARY
CUNNINGHAM	ANDRE	
CURRY	MARY	RANDOLPH LEWIS
CUSACK	ELMA	
CZERWINSKA	JOANNA	BEATA
DABABNEH	BARHAM	TALAL
DACEY	JOHN	FRANCIS
DAHM	JACOBIA	VERENA
DALAL	MERWAN	TOUFIC
DALTON	PETER	ROBERT
DALTROP	OLIVER	
DALY	DIANA	JEAN
DANTCHEVA	HRISTINA	IVANOVA
DARKE	JONATHAN	SIMON
DARNBOROUGH	MARIE	LOUISE
DASKAS	NIKOLAOS	
DAVAGE	LAURA	MARKS
DAVIES	JOHN	
DAVILA	SANAE	SHINAMURA
DAVIS	DAVID	RONALD
DAVIS	GREGORY	ALEXANDER
DAVIS	HELEN	LESLIE
DAWES	MARTHA	GAIL
DAY	CAROLINE	M
DAZO	HERBERT	FRANCESCUS
DE DONNO	CHIARA	
DE JONG	JAN	
DE LEO	MARCO	DOMINIK
DE RUITER	ADRIAAN	JAN
DE WIT	TIM	MATTHEUS
DEARING	KEVIN	TODD
DEBANE	XAVIER	GEORGE
DEGEL	FLORENTINA	EVA MARIA
DEGENSZEJN	ELIZABETH	EUGENIA
DELANEY	SUZNNE	MARGARET
DEMAREST	HALANA	MICHELE
DEME	BRANDON	C
DENNY	MARY	LOUISE
DEPORTER	JOELLEN	KELLY
DEPORTER	CRAIG	DONALD
DERKSEN	LOUISE	CHRISTINE GABRIELL
DERKSEN	TODD	MYLES
DESSOULAVY	ERIC	GEORGE
DEVLIN	EDMUND	JAMES
DEVOS	PIETER	CHRISTIAAN H.C.
DEWI	RUBY	EKA
DEY	DONALD	WILLIAM
DEY	JACQUELINE	THELMA
DHILLON	AMOLAK	SINGH
DICK	LORRAE	ALEXANDRA
DICKS	CAROLYN	KESSLER
DICKSON	ALEXANDRA	JANE
DICKSON	ANDREA	ELLEN

Last name	First name	Middle name/initials
DIETRICH	DANIEL	EDWARD
DIGREGOR	SAMUEL	RALPH
DIGWEED	JENNIFER	LYNNE
DILIBERTO	JAMES	DANIEL
DILL	MICHA	LUKAS
DIMITROPOULOS-VASILIADES	SOPHIA	ANASTASIA
DIN	NEENA	
DIRSCHERL	JENNIFER	MARIE
DIXON	MANAMI	
DIXON	CHARLES	DWIGHT
DOBBYN	GERARD	PETER
DOBELL	DARCEY	JEAN
DOBLER	KATJA	
DOBSON	ROSA	MAY
DOBSON	DANIEL	NATHAN
DOMENJOZ	MOLLY	KATHLEEN
DOMINOWSKI	WLODZIMIERZ	ALEKSANDER
DONALDSON	ROBERT	GLENDON
DONALDSON	IAIN	
DONCASTER	PAMELA	JEAN
DONZELLI	YUKI	
DOOHAN	SUSAN	ELIZABETH
DORIN	NARDA	
DOROSH	MARY	NICOLA
DOSCHER	SUSAN	KATHERINE
DOSEK	JIRI	
DOSHI	JAPAN	SHAILESH
DOSHI	SHATADHA	JAPAN
DOSKOVA	HANA	
DOTSON	JOSEPH	PETER
DOU	HONG	
DOUGLAS	BRUCE	GEORGE
DOWELL	JEFFREY	THOMAS
DOWNEY	SUSAN	LYNNE
DU	YUE	
DU	YU	
DUBOIS	THOMAS	
DUERR	ZACHARY	JOHN
DUFF	ALLAN	EDWARD
DUFFY	SEAN	MICHAEL
DUFFY	KATYA	RUTH
DUNCAN	SCOTT	ANDREW
DUNKLE	JUSTIN	JOSEPH
DURRANT	ALEXANDER	LOY
DYCUS	SEAN	TIMOTHY
DYSON	SAMUEL	LEWIS
EASTEAL	PATRICIA	LYNN
EATON	SHANE	MICHAEL
EBINGER	RAPHAEL	THOMAS
EBISAWA	CHIYOKO	
EBISAWA	JUNICHI	
EDEL	ANITA	
EDWARDS	NICHOLAS	JOHN
EGERTON	MANYA	IVANNE
EGGLER	LENA	MARIE
EICHLER	BIANCA	
EIFFLER	JANEK	
EIJMAEL	MARIE	JOSEE SOPHIE JEANN
EJIMA	HIDEMORI	
EL MANAWY	ADAM	HISHAM
ELLIOTT	SUSAN	GALE
ELLIS	AARON	LEE
ELLIS	KATHLEEN	SHARP
ELLISON	LUCAS	ANDREW
ELMORE	ALISON	JANE
ELTERMAN	ROSY	
ENGELBERTINK	ROBIN	GARY
ENGI	PASCAL	DANIEL
ENGI	PHILIP	DAVID
ENNIS	RICHARD	CONNING
ENOKIDO	TAKESHI	
EROL	TUGRA	
ESHLEMAN	CHARLOTTE	FAYE
ESPLIN	DEBORAH	

Last name	First name	Middle name/initials
ESQUINCA	DANIELA	SOFIA
ESSER	JESSICA	ANN
ESSIG	SARAH	DIANA
EVANS	GWYNETH	SIAN
EVANS	KRISTEN	L
EVANS-COLES	SUZANNE	STACEY
EWENS	JUDITH	ROSALIND
EWERS	BELINDA	ELIZABETH
EWERT	JORDAN	BAILEY
EWERT	BRAYDEN	CONNOR
FANG	MAOSEN.	
FARDON	PAUL	A
FARMER	SANDY	ELLEN
FARNSWORTH	JULIE.	
FAROOQI	NAVAID	EJAZ
FARR	TIMOTHY	R
FARRIS	AMANDA	HOPE
FAULKNER	NATALIE	MARIE JARED
FAWDRY	RACHEL	ANN
FEDER	LARA	ESTRELLA
FEDUN	MICHAEL	JOHN
FEIST	BAERBEL.	
FEIST	PETER	GUENTER
FELLING	ANDREA	JANE
FENG	JING.	
FENTON	KAREN	ANN DELORES
FERGUSON	KAREN	ANN
FERN	ALISON	MARGARET
FERN	STEPHEN	JAMES
FERRANTE	COLLEEN	MARIE
FERRIS	DOUGLAS	LANCE
FERRISS	SARAH	ELIZABETH
FILAN	ERIN	LOUISE
FINDLAY	TOMOKO	T
FINLAY	ROSEMARY	DALE
FINLAYSON	GRAHAM	CAMPBELL
FINNEGAN	NUALA	LAVERTY
FIRST	COLLEEN	JOY
FISCHER	MARC	DANIEL
FISHER	CURTIS	WAYNE
FITZGERALD	ROBERT	NORBOURNE
FITZGERALD CLARK	DIANE	C
FITZROY	JILL	ELIZABETH
FLEMING	DEVON	BRYCE
FLEMMING	MICHELLE	ANN
FLETCHER	MARK	R
FLORES ALARCON	GABRIEL.	
FLOUTY	CLAUDINE	F
FLOYD	GREGORY	DANE
FOLEY	JESSIE	BAXTER
FONG	JUN	KIAT LIONEL
FORD	DENZIL	LEE DAWN
FORD	JEREMY.	
FORGET	ROBERT.	
FORTE	AMELIA	ANN
FORTE	RALPH	CARL
FOSTER	WENDY	LOUISE
FOSTER	PAMELA	DIANE
FOSTER	JILL	LEANNE
FRANCHINO	NICKOLAS	MICHAEL MARTIN
FRANK	DANIEL	BENNETT
FRANK	ANDREW	JOSEPH SCHAHINGER
FRANK	ELIZABETH	MARY
FRANK	DAVID	IAN
FRANK	KATE	LIBBEY FOOTE
FRANKEN	NERISSA.	
FRASER	GARY	CHRISTOPHER
FREI-STOCKER	ANDREA	BEATRIZ
FRENCH	MARISA	ASTRID
FRENCH	MILES	ALEXANDER
FRIEDRICH	LINA.	
FRIEND	NICOLA	C
FRIZENSCHAF	YANN	M
FRUMAU	VANESSA	LORAINÉ

Last name	First name	Middle name/initials
FRYBERGER	KEIKO.	
FRYER	MARGARET	TRACY
FUCHS	FREDERIQUE	MARGARETHA
FUENZALIDA	CHRISTINE	DENISE
FUJIMURA.		
FUJITA	RIE.	
FUKUMORI	KAORI.	
GADDE	NEELIMA.	
GAETTELIN	SUSAN	KATRIN
GAFFAR	LINDA	MARIE
GAILITS	NICOLA	SUZANNE STUKEL
GALANEK	SOFIA	ISABELLA
GALLAGHER	BETTY	JEAN
GALLARDO-GODOY	ALEJANDRA.	
GALTS	NANCY	AMELIA
GAMBLE	THOMAS	ETIENNE
GAME	DAVID	ANTHONY
GAN	SUZANNE	KAM
GANCAS	KAREN	LOUISE
GANDHI	KAVI	SANJIV
GAO	TINGJUAN.	
GAO	BO.	
GARCIA	MARIA	DEL MAR
GARCIA WICKETT	RAUSHANA	ALENE
GASTON	MARIA	VALERIE
GATEHOUSE	MARK	WILLIAM FRANCIS
GAULAND	AIDAN	THOMAS
GAULIN	JANE	NICOLE
GAUVIN	LUCIA	VARGAS
GAVIGAN	BARTHOLOMEW	JAMES
GAY	MAX	HANS-PETER
GAYOU	NANCY	LEE
GEBRIL	GABRIEL	MOHAMED
GEIGER	RONALD	ALAN
GEIGER	KATHLEEN	DIANA
GEIGER	ERIC	RONALD
GELLERT	JULIE	ANNE
GENDRON	FRANCOIS.	
GENZO	ISABELLA	CATALANOTTO
GEORGE	CARLISLE	ELDWIDGE
GEORGE	ALEXANDER.	
GERRETS	RENE	PIERRE
GIBSON	JOANNA	MARIANNE
GILL	THOMAS	WILLIAM
GINSBURG	ALEXANDER.	
GIOBRAN	LEANNE	MAREE
GIULIANY	BARBARA	ELIZABETH
GLADWELL	HILARY	JANE
GLAZA	SANN	RENEE
GLENCROSS	CARL	C
GLESSING	NATHAL	GERALD
GLOBER	EWAN	ALEXANDER MCLEAN
GOBLE	KATHRYN	ANN
GOCK	ROSEANNE	JOYCE
GODDARD	CAMERON	ROSS
GODSCHALK	HELEN	GRACE
GOEDE	MONIQUE	S
GOEDEL	NICOLE	ELVIERA
GOETTI	ROBERT	PAUL
GOETZ-HENDRICKSON	KERSTIN	ELIZABETH
GOLAY	LATA.	
GOLDBERG	JESSICA	ROSE
GOLDSMID	HENRY.	
GOLLIN	RACHEL	HESTER
GONZAGA COSTA	LUIZ	CARLOS
GONZALES	MARISELA.	
GORDON	MARY	ELLEN
GORDON	JOYCE	KAREN
GORDON	ISABEL	VOELKER
GORSKI	THADDEUS	ANTHONY
GOSSELIN	XAVIER.	
GOUGE	ANDREW	PAUL
GRACIA	LUIS.	
GRAD	KATHARINA	GRAD

Last name	First name	Middle name/initials
GRAHAM	BRENT	LEE
GRANT	ROSEMARY	CLARA ISOBEL
GRANT	SHELAINE	M
GRAY	STEPHANIE	EDITH
GREDLER	JENNIFER	
GREEN	MCELLE	RENEE
GREEN	MICHAEL	
GREENE	MARGARETHE	LEE
GREENSMITH	CHRISTOPHE	MICHEL
GREER	ANDREW	REID
GREET	NICHOLAS	MARK
GREGGERSEN	ERIC	
GREGORY	SCOTT	WALKER
GREGORY	ESTHER	CHARLOTTE
GREGORY	COLIN	
GREGORY	EVA	
GREIG	KEVIN	ROBERTSON
GREY	ALEXANDER	DOUGLAS
GREY	JONATHAN	WILLIAM
GRIFFITH	LISA	ANNE
GRIGSBY	PAULINA	VIRGINIA PHUONG
GRIMSRUD	JUDITH	LORRAINE
GROBLER	CLINTON	GUY
GROVES	SAMUEL	CARDER
GUAN	JENNIFER	
GUDEWILL	SALLY	MARIE
GUENKEL	ANNA	LENA
GUENTHER	THOR	ROMAN
GUILLARD	FRANCINE	I
GUIZADO MORALES	ANA	VICTORIA
GUJAR-GUGGI	LUCY	YOLANDA
GULER	HULYA	
GULLI	GIORGIO	
GUNN	JULIE	ANNE
GUNN	CAMPBELL	DAVID
GUNNING	JOHANNES	HERANUS
GUNOLD	AILEEN	ANNA BARBARA
GUO	XIAO	
GUPTA	KRITIKA	
GUPTA	KAVEEN	
GUTCHER	JAMES	ROBERT
GUTCHER	AMANDA	MAY
GUTIERREZ	EDGAR	JOSE
GUTIERREZ	ANA	SOFIA
HA	JOO	HYUN
HABY	JANETTE	BERNADETTE
HAGELBERG	ERIKA	
HAGEMEISTER	JAMES	ROSS
HAHN	CHARLES	WILLIAM
HALBE	KEVIN	DAVID
HALE	HELEN	MARY
HALL	DONALD	GARDNER
HALPINE	MARY	EILEEN
HAMMER	REBECCA	ANN
HAMPTON	JOEL	LLOYD
HAN	MANHO	
HAN	SANG	CHUL
HANAKAWA	TAKESHI	
HANER	SIMEON	THOMAS
HANNA	MARY	ELIZABETH
HANNEY	STEVEN	ALEXANDER
HANSELL	DEBORAH	JANE
HARDY	DYLAN	K
HARE	DARCY	
HARE MCCLURE	LAURA MARY	ELIZABETH
HARPER	KATHLEEN	MARGARET
HARPER	CHARLOTTE	ANNA
HARRIGAN	RYAN	DANIEL
HARRINGTON	ERIN	JEAN
HARRINGTON JOHNSON	HEIDI	
HARRIS	I	HIAM AP
HARRIS	SHELLEY	ANNE
HARRIS	JANYCE	JO
HARRISON	ELISA	ALESSANDRA LAVINIA

Last name	First name	Middle name/initials
HARTMANN	PATRICK	DAVID
HARTNETT	JUSTINE	ANNE CAROLINE
HAUBER	PETER	EMMANUEL
HAVERCROFT	CALLISTO	PAULETTE
HAWKESWORTH	JOSHUA	PETER TAPPER
HAWKINS	MICHELE	NADINE THERESE
HAYAKAWA	EMIKO.	
HAYES	CHRISTINE	ISABEL
HAYNES	JOHN	STEPHEN
HAYS	PAUL	WALTER
HE	XIAOWEN.	
HEASMAN	CLAIRE.	
HEASMAN	PAUL	DAVID
HEATH	WILLIAM	ALEXANDER
HEATON	NICHOLAS	JAMES
HEDENQUIST	JEFFREY	WAYNE
HEDINGER	LARISSA	MARISA
HEIDBREDER	ROBERT	KENT
HEIDECHE	SARA.	
HEIDUSCHKA	SIGRID	ANNA
HEIGL	ANDREAS	FRANZ
HEINRICH	AMY	ASAKO
HEINTZ	GRETITA	RUTH
HEINTZE	MIRJAM.	
HENG	SOKKEANG.	
HENGPOONTHANA	KEITH.	
HENGST	MARKOS	SOLOMON
HENRY	ISOBEL	LOUISE
HEPPELMANN	CYNTHIA	ROSE
HEPWORTH	JOHN	RAYMOND
HERNANDEZ	NANCY.	
HERTEL	MICHAEL	EDWARD
HEUMANN	HEINZ	PETER
HIERONYMI	PHILIPP	CHRISTIAN KARL
HIERONYMI	KADRIYE.	
HILL CLISE	MADELEINE.	
HILLERICH	COOPER	FRANK ELMO
HINRICHS	MARIE	ELIZABETH
HIRAYAMA	KOUKI	JOSEPH
HIROSE	KIMIKO.	
HIROSE	TOSHIYUKI.	
HOARE	LEONARD	JOHN
HODGSON	TINA	GWENDOLYNNE
HOEKSTRA	KATINKA	WAIOLI
HOFFMAN	RACHEL.	
HOFFMANN	BURGHARDT	DOUGLAS
HOGAN	RYAN	JAMES KINGSMILL
HOLDENMEYER	MICHAEL	JOHN CLAUDE
HOLTEN	SASKIA	JANE POLLY
HOMBERG	CARIN	SOPHIA
HOMEWOOD	JENNIFER	LAUREN
HOMPO	YUMIKO.	
HONG	RICHARD	JUNGWOO
HOPE	CAMERON	DOUGLAS
HOPE	NORA	HATTON
HORI	MASAYASU.	
HORIKOSHI	KINYA.	
HORIKOSHI	TOMOKO.	
HORINEK	ROBERT	EHRETH
HORN	RAINER	MORITZ THEODOR
HORNFIELD	HOWARD	L
HORNSBY	JOANNE	SARAH
HORTON	BENJAMIN	PETER
HOSHI	TAKEO.	
HOSOKAWA	SUSUMU.	
HOU	PEI	LING
HOU	DARREN.	
HOURELD	MARY	THERESA
HOUSWORTH	CARLINE	LAVERA
HOWDEN	SAM	SAM
HOWE	SUSAN	JOYCE
HOWELL	ELIZABETH	CARMEN
HOWSAM	JESSICA	KATE
HSIA	HUGNCHIU.	

Last name	First name	Middle name/initials
HSIL	STEPHANNE.	
HU	SHU	JUNG
HU	SEAN	HSIANG JUNG
HUANG	LING	LING
HUBER	JEFFREY	WAYNE
HUBER	SUZANNE	MARGARETE
HUBER	FRANCK	AUGUSTE
HUDZ	ERIC	ANTHONY
HUGHES	LAURA	DOROTHY
HUGHES	FAITH	ELIZABETH
HUHARDEAUX	ODILE.	
HULINSKY	IVAN.	
HULL	MARALEE	EVELYN
HUMPHREY	PATRICIA	ANN
HUMPHREY	BARRY	JAMES
HUNTER	SALLY	PATRICIA
HURIHANGANUI-POWERS	CARRIE	LYNN
HUTCHINGS	DAVID	GEORGE
HYATT	JAMES	OWEN
IFF	RETO	ROBERT
IGARASHI	MIKI.	
IHARA	MASASHI.	
IMAO	FUMIKO.	
IMAO	SHIGEYA.	
INABA	YASUKO.	
INMAN	BRANT	ALLEN
ITAKURA	YUKIKO.	
ITO	RYOKO.	
IVANOV	IVAN	DRAGOMIROV
IWASAKI	HIDETAKA.	
IZUSHIMA	HISAE.	
IZUSHIMA	MASAAKI.	
JABER	BRENDA	GAIL
JACKSON	KELSEY	MEGAN
JACKSON	ROGER	ANDREW
JACOBSON	JEFFERY	BENJAMIN
JACOBSON	JEREMY	MORRIS
JAKUBCZYK	KRYSZTOF	JAROSLAW
JALILI	ROZITA.	
JAMEYSON	KAREN	ANN
JANG	SUK	WOON
JANSSON	WENDY	LOUISE
JANZEN	KYLA	CARRIE
JARED	JOHN	MATTHEW
JEFFERSON	OLIVER	LAWRENCE
JEFFREY	MATTHEW	IAN
JEFFREY	MARIANNE	GAY
JENKINS	JAMES	PATRICK
JENSEN	DANIEL	ROSENGARTEN
JENSEN	HANNAH	ROSENGARTEN
JENSEN	JONATHAN	ROSENGARTEN
JHANGIANI	JAIDEEP	DEEPAK
JIANG	FANG.	
JITSUMOTO	TAKAHIRO.	
JOFRE	MICHELLE	CHARLOTTE JULIA
JOHN	REGINE	SUSANNE
JOHN	CLAIRE	ALEXANDRA
JOHNSEN	ANDREW	STEPHEN
JOHNSON	CAROLYN	ANNE
JOHNSON	ANNIKA	CHRISTINA
JOHNSON	KRISTEN	KATHLEEN
JOHNSON	MIRIAM	LENA
JOHNSON	RACHEL	EDA
JOHNSTON	DAVID	JOSEPH
JOHNSTON	SCOTT.	
JOLLER	MARTINA.	
JOMA	RONALD	ALEX
JONES	THOMAS	JUSTIN
JORGE	ANNE	ESTELLE FINNIGAN
JULMY	JESSICA	CHRISTIE
JUMONJI	MOTOKO.	
JUNG	HAE	SUK
JUSTICE	ROBERT	JAMES ALEXANDER
KABRA	VIKAS	KUMAR

Last name	First name	Middle name/initials
KADOWAKI	SHIRO.	
KADOWAKI	SHOKO.	
KAJI	FUMIO.	
KAJI	SACHIKO.	
KALESNIKOFF	JANET	LEANNE
KALIS	ALEXANDER	G
KALUGEROVICH	PERO.	
KAMINOH	MIDORI.	
KAMMAN	SVEN.	
KANEKO	TOYOHISA.	
KANETO	YASUKO.	
KANG	SUN	JA
KANG	WON	KYUNG
KAPUR	USHA.	
KARGER	CHRISTIAN	PETER
KARIM	FAHIM	ALHUSSEIN
KARITA	KEIZABURO.	
KARITA	JUNKO.	
KARLEN	DONNA	MARIE
KASHIMURA MATHIS	HIROKO.	
KATORI	HIROKO.	
KATZ	SAMSON	ROBERT
KATZ	DEBORAH	ROBIN
KAUFMANN	ADELAIDE	STEFANIE
KAVATHAS	CHRISTOS.	
KAWAHARA	YUKIKO.	
KAWAKAMI RAYNAUD	ERIKO.	
KAWAMOTO	TOKUO.	
KAWAMOTO	KUMIKO.	
KAZAMA	AKIRA.	
KAZAMA	SUMIE.	
KEALL	PATRICIA	LEE
KEARNEY	OLIVER	PATRICK TIMOTHY
KEARNEY	MARK	FRANCIS
KECK	JONAS	CARL
KELLY	VIRGINIA	MARY
KELPE	NICOLAS	CHARLES
KEMEL	MAKSIM.	
KENNEALLY	MATHEW	J
KENNEDY	KATE	LOUISE
KENNEDY	JENNIFER	YUST TWEEDALE
KENNEDY	GRETCHEN	S
KENNEDY	BLAKE	DANIEL
KEOGH	CLODAGH	ANN
KESALA	ALEX	RAYMOND
KHANGURE	SIMON	RUPE
KIDO	KATSUHIRO.	
KIKUCHI	SAIKO.	
KILPATRICK	GRIFFIN	ALEXANDER
KIM	MIN	JUNG
KINGSBURY	DAN	MCKEE
KINGSTON	CHARLES	MCGREGOR
KIPMAN	ALEX	ABEN-ATHAR
KIRKWOOD	PAMELA	JANE
KIST	JEFFERSON	BARRETT
KITAOKA	NATSUNE.	
KITCHEN-DUNN	FREDERICK	SIMON
KJESBU	JOACHIM	SEBASTIAN
KLASEN	ROLAND	MARNIX THEODOOR
KLAUS	SABINE	KATHARINA
KLEINER	JOHANNES.	
KLEMENT	MARKUS.	
KLEMENT	SUSANNE	CHRISTINA
KLEP	JEROEN	SEAN
KLINGHED	JESPER	KLAS
KLOSS	GIDEON.	
KNAPP	SARAH.	
KNIGHTON	CHARLOTTE	ALICE
KNOOP	MAURITS	MAX
KODA	CHIZUKO	KODA
KOH	CHIN	KIONG
KOHNSTAMM	JUSTIN	MICHAEL
KOL-BAR	MYRIAM.	
KOL-BAR	JONATHAN.	

Last name	First name	Middle name/initials
KOLBAS	EUGENIA	VERONICA
KOMORI	HIROFUMI.	
KOO	YOUNG	IM
KOOPMANS	ELISA	NOELLE
KOREJKO	JONATHAN	DAVID
KORNEYCHUCK	ELENA	A
KORTENAAR	PAUL.	
KOSAKA	YOUNG	J
KOSHIMIYA	TERUYO.	
KOSTER	SCOTT	JOSEPH
KOTEGAWA	HIDEKAZU.	
KOULIE	CHRISTIAN	OLIVIER
KOYL	MARY	LEE
KRAMER	CHRISTIAN	ALEX
KRATTIGER	FRANCESCO	SACHA ANTOINE
KRAUS	BARBARA	ERIKA
KREINDLER	LISA	SHARON
KREISBERG	DOMINIK	CHRISTOPHER
KROSKA	SHARON	KAY
KTONAS	PERIKLIS	YIANNIS
KUBLUN	IRENE.	
KUCZMA	RICHARD	PAUL
KUEHNBAUM	KATHRYN	ANN
KUENG	SEBASTIAN	BERNARD
KUHNE	ADRIEN	ALEXANDRE
KUIJPERS	EVERT	P
KULBASHIAN	HUNTER	ALEXAN
KUMILEWA DOMINOWSKA	BOTKA.	
KUMORI	KAZUYOSHI.	
KUMORI	KAZUKO.	
KUPPA	RAMGOPAL.	
KUWABARA	KEIKO.	
KUWABARA	NOBUYUKI.	
KWON	EVA	M
KWON	BYEONG	JUN
LA FLEUR	DAVID	CHARLES
LACANLALE	SHINOBU	MATSUMOTO
LACY	MARY	PAIGE
LAFLECHE	MURIELLE	THERESE
LAING	JENNIFER	ANN
LAIRD	SALLY	ANN
LAJOIE	REMY	RAMSEY
LAM	NIN	KIN
LAMBERT	IAIN	BAKER
LAMEYER	MICHIYO	MORITA
LANDRY	DONNA	DARLENE
LANSTROP	CHRISOTPHER	HOSTRUP
LARAMIE	CALE	JAMES
LARDEAU	JEREMY	OLIVIER LUC
LARRIEU	DANIELLE	EMMA
LASANCE	TODD	JAMES
LASCELLES	CHARLOTTE	SIERRA
LATOUR	ANDRE	ROGER
LATRY	MARY	KUNDE
LAU	ANDREW	HENRY
LAURENCE	DAVID	CH
LAURENS	MATHIEU	LOUIS KEVIN
LAVIGNE	ROBERTA	B
LAVYAD	KEREN	CHAYA SHIFRA
LAWER	TESSA	ELIZABETH
LAXTON	KATE	ANNE
LE	TRI	MINH
LE	NHAT	MINH
LE	CUONG	HUNG
LEA	JOHN	ALEXANDER
LEAMAN	CATHERINE	ELLEN
LEANG	HY.	
LEBAIL	KARINE	NA
LEBRETON	DENIS	SEBASTIEN
LEE	JUNGHEE.	
LEE	HYO	CHI
LEE	AI	LING
LEE	MENG	CHANG
LEE	BUM	JU

Last name	First name	Middle name/initials
LEE	KIT	WING SIMON
LEE	CHANG	HO
LEE	YOUNGJUN.	
LEE	JU	YOUNG
LEE	JORDAN	MARGARET-ANN
LEE	SYLVIA.	
LEE	HEE	JEAN
LEE	CHRISTINE	MARIE
LEE	RACHEL	MARIE
LEE	JAN	JIARONG
LEE	AMY	YUKYUNG
LEETZOW	JENNIFER	MAE
LEGG	JASON	J
LEGG	LAURA	IRENE
LEHET	NANCY	JEAN
LEIBIK	RUTH	ANN
LEICHT	KIMBERLY	HELEN
LEICHTWEIS	STEVEN	BOYD
LEIJDEKKER	JURGEN	PIETER
LENTI	MARGARET	MARY
LESTED	CHRISTOPHER	ALBERT
LESTED	CHRISTINE	MOCKLI
LESTED	BARBARA	ALLISON
LETCHER	LOIS	ILENE
LEVENSON	FRANCES.	
LEVETT	CHRISTIAN	JAMES ROBERT
LEVIE	JOHN	EDWARD
LEWELLEN	STEPHANIE	RENAE
LEWIS	NIGEL	ALAN
LEWIS	AMY	CHRISTINE
LEWIS	KAREN.	
LHIM	YU	SEOUN
LI	ZHENXIAN.	
LI	BINGSI.	
LI	JAN	YUANXIN
LI	CALVIN	PEI JUN
LIAO	RICHARD	CHIH WEI
LICHTENBERG	TAMMY	DARSHANA
LIEBERHERR	EVA	KATHARINA
LIGUORI	JOSEPH	PAT
LILLY	ALAN	DOUGLAS
LIM	HYE	KYUNG
LIN	ANDY	YU CHIEN
LINCOLN	STEVEN	JOHN
LINDEN	PATRICIA.	
LINDER	PATRICIA	SAMANTHA
LIU	AN.	
LIU	JIA.	
LIU	YUANSHEN.	
LLOYD	SPENCER	MICHAEL
LOCH	LESLIE.	
LOGAN	DELLA	RUTH
LOGAN	CHRISTINE	ANNE-MARIE
LOH	JONATHAN	KWUEN NIN
LOLLI-GHETTI	MICHAEL	THOMAS
LONGMAN	REBECCA	SUZANNE
LONGMAN	TERENCE	ALFRED
LONSETH	ERIKA	JANE
LOOFT	DORIS.	
LOS	NICHOLAS	CONSTANTINE
LOUDON	PETER	THOMAS
LOUGHEED	DIANE	ROSE
LOVELL	STEFANIE	JEAN MARIE
LOWE	ANDREA.	
LOWE	ELIZABETH	CEINWEN
LOWENSTEIN	MAX	DANIEL PERICLES
LOWENSTEIN	JOSEPH	AARON SOCRATES
LU	YU	YING
LU	CHRISTINE	YI JU
LU	JIANHUA.	
LUCID	JACK	MICHAEL
LUFT	HERBERT	SEBASTIAN
LUKEFAHR	HOWARD	GARRELT
LUKIANENKO	OLEKSII.	

Last name	First name	Middle name/initials
LUO	YUAN.	
LUO	QIPENG.	
LUOMANEN	LARS	AKE
LUZ	GREGORY	MANUEL
LUZZI	AMELIA	BENEDETTA
LYLE	SCOTT	EDWARD
LYON	JENNIFER	ROSE
LYONS	DARCIE	CLARK
LYONS	JACQUELINE.	
MA	HANHUI.	
MAAG-PELZ	JENNIFER	RENEE
MAC CLURE	MAGDALENA	LYON
MACADAM	JAMIE	LEA
MACDONALD	ALLAN	SEAN
MACDONALD	ELIZABETH	DEVINE
MACHIDA	FUMIHIKO.	
MACHIDA	NORIKO.	
MACHIN	ADAM	JAMES
MACHIN	JOANNE	ELIZABETH
MACHIN	DONNA	TERESA
MACKAY	PAULA	KATHLEEN
MACKENZIE	KELLY	ANNE
MACKINGA	NIKO	TORGIN
MACMILLAN	DONNA	KAY
MACRAE	LAUREN	MARIE
MAEDA	NOBUHIRO.	
MAEDA	SHIORI.	
MAINVIL	JOANNE	LOUISE
MAITA	NOBUAKI.	
MAITA	HIDEHIRO.	
MAK	MAN	YAN JOYCE
MAKINO	KOJI.	
MAKINO	JUNKO.	
MANGEOT	MARIE	ANTOINETTE S
MANN	KAREN	JANE
MANN	HARRY	GEORGE
MANNA	MARK	ROBERT
MANNHEIMER	ELIAS	THEODOR AHLSTROM
MANSFIELD	MARGUERITE	AGNES COLE
MARANTZ	MONICA	JANE
MARCUSON	ELIZABETH	CAROL
MARDUKHI	JIAN.	
MARIDAL	JAN	HAVARD
MARINIS	CONSTANTINE.	
MARKHAM	MARIA	LAUREEN
MARRIOTT	DION	JAMES
MARRIOTT	ROBIN	RALPH
MARSTON	ANGELA.	
MARTIN	SARAH	GWEN
MARTIN	LAURA	MARIE
MARTS	VANESSA	MAE
MASAKI	KAZUNARI.	
MASKENS	HORTENSE	ANNICK
MASSEY	FLOR	R
MASTERSON	STEPHEN	JAMES
MASTRO	BRENTON	EDWARD
MATHIS	CHRISTIAN	ANDREAS
MATSGARD	MELANIE	LOUISE
MATSGARD	JOHAN	ERIC WILHELM
MATSU	MARIAN	ANITA
MATSU	EDDIE	TATSUO
MATSUDA	RITSUKO.	
MATSUDA	KAYOKO.	
MATSUDA	TAKASHI.	
MATSUMOTO	CHIYOKO.	
MATSUO	SACHIKO.	
MATTHEWS	STEPHEN	SILLAR
MATTISON	DANIEL	ARTHUR LESLIE
MATTS	GEORGE FREDERICK	WAGER
MAUELL	CHRISTIAN	HERRMANN
MAY	LUKAS	EDMUND
MAYER	WENDY	ELIZABETH
MAZER	GLENN.	
MCAULEY	SHARON	DOROTHY

Last name	First name	Middle name/initials
MCCANN	SAYAKA	KIDA
MCCARTEN	ISABEL	D
MCCARTHY	PAUL	
MCCARTHY	DEBRA	LOUISE
MCCARTHY	SEAN	MICHAEL
MCCLURE	KEITH	ANDREW
MCCONNELL	THEODORE	ALBERT ANIL
MCCORMICK	JOAN	MARIE
MCCULLOCH	ANDREW	WILLIAM
MCDANNELS	ANDREW	PAT
MCDONALD	EVE	CAROLYN
MCDONALD	LINDSAY	JEAN
MCGLADE	MARK	
MCGRATH	ELIZABETH	FRANCES
MCKIMM	JOAN	MARIE
MCLAUGHLIN	DANIELLE	LEROUX
MCLAUGHLIN	CHRISTOPHER	VIVIAN
MCLEAN	GRAEME	WALLACE
MCMULLEN	BRIAN	TIMOTHY
MCNEVAN	SCOTT	GORDON
MCNICHOL	DEBRA	LYNNE
MCVICAR	MICHELE	FRANCES
MEACHAM	DAVID	GEORGE
MEADE-KING	KATHERINE	ELIZABETH LYELL
MEESSCHAERT	VALERIE	MARGARET
MEI	JING	
MEIER	ALEXANDER	NICOLAS
MEISSNER	NIKOLAOS	ALEXANDER
MELNICK	BURTON	ALAN
MEMARI	ALIREZA	
MENEGALDO	ELENA	
MENON	KUSUM	
MENON	ANNE	JOLEEN
MENON	RAVI	SHANKAR
MENZIES	ELLEN	FRANCES
MERIEAU	LINDA	LEE
MESAGNO	CHRISTOPHER	
METAXOGLU	KONSTANTINOS	
METCALF-HEPPELL	ASHLEY	MARIE
MEULEMAN	ANDRIES	THOMAS
MEYER	JEREMY	
MEYER	DEAN	JON
MICHAELS	ANNA	ELIZABETH
MICHALLIK	NICOL	ANGELA
MICHAUD	PHILIDA	JOY
MIDDLETON	MAURICE	EMERSON
MILES	PHILIP	
MILLAR	GEORGE	ALBERT LESLIE
MILLER	BRETT	DANIEL
MILLER	MICHELLE	IRENE
MILLER	ELIZABETH	LOUISE
MILLER	JASON	SAMUEL
MILLER	JULIA	ANNA
MILLS	ROBERT	ARTHUR
MILMAN	CHARLOTTE	MARIE
MILNE	DANETTE	DONA
MILNE	DUSTIN	W
MIMICK	KRISTIN	CLAUDIA
MINAMI	TOMOE	
MINOWA	KEIKO	
MINOWA	SHINJI	
MINTO	ANGELA	MARY
MINTO	PATRICK	WILLIAM
MISTELY	ANNIKA	
MITSCH PERIN	CHRISTINE	HILDE
MITTENDORFER	CLAUDIUS	
MIWA	TATSUMI	
MIZUTANI	RYOSUKE	
MIZUTANI	HIROMI	
MODARD	PHILIPPE	JACQUES ARTHUR
MOERITZ	FREDERICK	SIGMUND HANS
MOLDER	SARAH	DAWN
MOLLER	MARIE	FORUM
MOLLER	HANS	FORUM

Last name	First name	Middle name/initials
MONROE- GONIN	JESSICA	IRENE
MONTEITH	BARBARA	MARLENE
MONTGOMERY	SARAH	JANE
MOON	LAURA	SUSAN
MOORE	SHONA	MARIE
MORAES-EDWARDS	MELISSA	
MOREAU	ANTOINE	JEAN LOUIS
MORGAN	DANIEL	JOHN JEGOR
MORIOKA	NOBUYUKI	
MORIOKA	ARISA	
MORIYA	MASAAKI	
MORIYA	FUMIE	
MORKOS	ANTHONY	CHARBEL
MORRIS	FIONA	JANE
MORRIS	JOHN	HILL
MOSCHYTZ-LEDGLEY	MIRIAM	EVE MICHELLE
MOSES	BRYAN	LINDSAY
MOUNTAIN	ELFRIEDA	
MOY DE VITRY	JONATHAN	ANSEL
MOYA	JAVIER	ALONSO
MUELLER	PETER	ALOIS
MUELLER	ALFRED	CHRISTOPHER
MUI	JANICE	WAI-YING
MULLER	KATHRIN	A
MULLER	MATHIAS	WILLIAM MORITZ
MULLER	VERONICA	SUSANNE
MULLER	BARBARA	EDITH
MULLIGAN	SIGRUN	ALICE
MULLIGAN	JAMES	BYRON
MUMBLAT	ALEX	DAVID
MUNDADA	RASIKA	ASHISHKUMAR
MUNRO	GREGORY	PAUL
MURATA	KIYOTOSHI	
MURAYAMA	MASAKATSU	
MURGA	ANNA	DANIELLA
MURGA DORION	JUAN	CARLOS
MURNANE	MICHAEL	XAVIER
MUROYAMA	YUKI	
MURPHY	LAURA	JANE
MURPHY	JOSEPH	PATRICK
MURPHY	MICHAEL	DENNIS
MURPHY	COLUM	FINBAR
MURPHY	JAMES	EDWARD
MURPHY	SANDRA	LOU
MURRAY	ANGELA	CHRISTINE
MURRAY	STEPHEN	DOUGLAS
MURRAY	CARA	JANINE GILMORE
MURRAY	CRAIG	MASON GILMORE
MURRAY	CHRISTOPHER	ARTHUR HUGH
MURRAY	JULIANA	ELIZABETH
MUSSLER	JACOB	EUGENE
MYLES	DONAL	DESMOND
NADERHIRN	MICHAEL	
NAGAMATSU	YOKO	
NAGASHIMA	HAJIME	
NAGATA	RISA	
NAGEL	CHRISTOPHER	
NAKAGAWA	FUMI	
NAKAMURA	TOMOE	N
NAKAYAMA	NAOMI	
NAM	KI	PUNG
NAMTVEDT	ALICE	SCHJOTT
NANTAU	JACOB	M
NATTIER	CHRISTIANE	
NEEDHAM	CHRISTOPHER	JOHN
NEIL	LUCAS	JONATHAN
NELSON	ANDREW	PETER
NELSON	AILS	
NEMETI	MARC	
NENDISSA	JUDITH	SIGRID
NESTOPOULOS	MATTHEW	APOSTOLOS
NEUHAUS	RUTH	ELISABETH
NEUHAUS	WALTER	
NG	NICHOLAS	

Last name	First name	Middle name/initials
NG	NATHALIE.	
NG	NATHALIE.	
NGUYEN	THANH	VAN THI
NICHOLS	ALISON	PATRICIA
NICHOLS	JAMES	ROBERT
NICHOLSON	ALASDAIR	W
NICHOLSON	MEGAN	JANE
NICKEL	TOBIAS.	
NIELSEN	PHOEBE	ANNE
NIEMINEN	JOEEL	KALEVI
NISHIYAMA	HAYATO	AARON
NOBLE	SAMANTHA	JULIE
NOESKE	JONAS	DANIEL
NOMURA	YUKO.	
NONOYAMA	YOSHINOBU.	
NONOYAMA	TAKAKO.	
NORTON	ANNE-LUCIE.	
NOUR	KARIM	TAREK
NOZAKI	TAKAKO.	
NUFER	NICOLE	SUSAN IRMGARD
NUGTEREN	LYDIA	PEARL
NUSPL	PETER	P
NXUMALO	FIKILE.	
OAK MYALL	PATRICIA	ANN
O'CONNELL	LISA	KARINE
OCONNOR	GRAEME	DAVID
ODFJELL	MONICA	SOLUM
ODONE	ERIC	LEONEL
ODWYER	MIRIAM	JACINTA
OGILVY	BRUCE	MARK PATRICK
OGUMA	MASASHI.	
OIE	JUN.	
OKAI	TAECO.	
OKAI	TOSHIYUKI.	
OKASHIRO	CHITOSE.	
OKUDA	MASUSHI.	
OLIVER	WARWICH	GEORGE
OLLENBERGER	SHANE	DOUGLAS
OLVERA	NICOLAS	FRANCISCO
O'MAHONY	KARL	LIAM
O'NEILL	LAURA.	
ONO	TAKAYUKI.	
OPIE	DAVID	JOHN
ORABONA	FRANCESCO.	
O'REILLY	STEPHEN	GERARD
ORENSTEIN	LEILA	NAJBERG
ORIORDAN	RYAN	JEREMIAH
ORTA MORRAL	SANDRA.	
ORTEGA	ELIZABETH.	
OSBORNE	TERI	LYN
OSBORNE	MINNIE	ELIZABETH MARY LILIAN
O'SHAUGHNESSY	STEPHEN	MARTIN
O'SULLIVAN	PAUL	EAMON
OTSUKA HALLMAN	YASUE.	
OWENS	CHRISTOPHER	MARTIN
OWENS	JOYCE	RUTH
OWENS	SARAH.	
OYAMA	ENRICO	ISAMU
PACK	SUNG	YUNE
PADILLA PEREZ	HECTOR	ALEJANDRO
PAE	ANDREW	WISDOM
PAGE	ALICE	BARBARA HEATHER
PAK	SONG	TAE
PAKULIS	ANDREW	JOHN
PALMQUIST	CHARLES	HALVARD
PAN	FENG.	
PARDUE	STEPHANIE.	
PARIKH	ROHAN	APURVA
PARK	JISUK.	
PARKER	JUDITH	SYME
PARKER	KATHERINE	LINNET
PARKER	LAURIE	A
PARKER	AMY	J
PARSONS	JAMES	BRYAN

Last name	First name	Middle name/initials
PARTIN	ANGELA	LOUISE
PARUCHURI	PRAVEEN.	
PASCHER	FRANZ.	
PASKOWSKI	BRIAN	THOMAS
PATEL	VASHISTHA	N
PATRI	PALLAVI.	
PATRICK	JEFEREY	CLAYTON
PAUL	JOSHUA	SCOTT
PAULS	THOMAS	LAWRENCE
PAWLIK	KARIN	AGNES
PAWLIK	HANS	MICHAEL
PAYNE	EMMA	LUCY
PEARSON	JUSTIN	MATTHEW
PEARSON	DALE	BRIAN
PEDERSEN	RUNE	MICHAEL NORUP
PEDERSON	KEIKO	TOSHIMA
PELICHET	BARBARA	DOROTHEE
PELZIG	JACK.	
PEN	CHIH	HUI
PENG	ZHONG.	
PENNINGS	MARLOES	HENRIKE
PEPINGCO	MICHELLE	DANAE
PEREIRA DA CONCEICAO	CHRISTOPHE.	
PEREZ	STEVEN	FRANCIS
PERRIARD	SIMON	NICOLAS
PERROTTA	JOANY	JOSEFINA
PERRY	RENE	CLAUDETTE
PERRY	ANDREW	MICHAEL
PERSONS	ALEXIA	KAARINA
PETERANDERL	THOMAS	KLAUS DIETER
PETERS	TRISTAN	EDWARD
PETERS	STEPHEN	RALPH
PETERSON	RICHARD	LYLE
PETRUCCI	LAURIE	JANE
PETRUCCI	MARCELLO	
PETTEE	JULIA	ANNE
PETTY	JOB I	LYNN
PEUKERT	FELIX	TINHAN
PHILIP	MARTIN	J
PHILIPS	MENAKA	M
PHILLIPS	SAYOKO.	
PHILLIPS	ROBIN.	
PHUA	HWAN	KHOON
PICKARD	DAMON	LEE
PIEBENGA	BOYD	YELMER
PIEL	BARBARA	LYNN
PIETH	PETER	ARTHUR
PINCHBECK	OLIVER	JAMES HUNTER
PINE	DAVID.	
PINTO CORAZZARI	DANIEL.	
PIONE	RICHARD	DAVID
PITT	DONNA	L
PITTELLA DE SOUZA LEITE	CARLOS	ANTONIO
PLOMIN	JOSEPH	ROBERT
POEHLKER	MARA	HELENA
POLLACK	JACOB	NATHANIEL
POLLARD	MICHELANN	JENSSSEN
POLLARD	MATTHEW	ALAN
POPP	LENA	LUISE
PORCINO	ANN	THERESE
POSTACILAR	AHMET	HAKAN
POTHIER	NANE	CARINA
POTSKOWSKI	BRIAN	DOMINIC
POULETT	GRAHAM	JOHN
POUNTEY	MIRANDA	MARY
POWELL	OLIVER	JAMES
POYNOR	NIKKI	MOMOKO
PRECIOUS	TERESA	NORA
PREISIG	SIMON.	
PREVOST	MAYUMI	UEDA
PRIETO	ROSE	MAYO
PRIHAR	JANET	H
PRIOR	STEPHEN	JOHN
QIAN	STEVEN	S

Last name	First name	Middle name/initials
QUINOY	JOSE.	
RAINA	JYOTI.	
RAINES	JOHN	DALLAS
RAJAHALME	MAARIT.	
RAMAKRISHNAN	NARAYANAN.	
RAMOS	MARGARET	ANN
RANCOURT	YVETTE	GERMAINE
RAO	YI.	
RASMUSSEN	HELENE	LOUISE
RATHE	SUSAN	CORINNA
RATHLE	NICHOLAS	PAUL
RAYMENANTS	JOREN.	
RAYNER	ANDREW	PIERS
REGUEIRO	AMY	HORVATH
REICHLIN	DANIELLE.	
REID	DEBORAH	MARIE
REIMER	MURRAY	BRUCE
REINHOLD	MIYOKO	KIMURO
REINHOLD	STEPHAN.	
REMTULA	MALIHA.	
RENFROE	DAVID	SEAN
RHODES	ANNELIESE	MARY SUSAN
RIBEIRO	SUSAN	ANNE
RICHARDS	NICHOLAS.	
RICHARDS	SAMUEL	DODD
RIDLEY	JANE	MARGARET
RIDLEY	JONATHAN	MELVILLE
RIEDI	STEVEN.	
RIEDWEG	RYA.	
RIENDEAU	BERTRAND.	
RIETSCHLIN	DONNA	MARIE
RIGAUX	FABRICE	STEPHAN
RIMINGTON	REBECCA	MARY
RISHANI	MAZEN	KHALED
RITTER	BOBBY	STEVEN
ROBARCHEK	YUMI	N
ROBBINS	CAROLINE	ELIZABETH
ROBERT	MIA	ALEXANDRA
ROBERTSON	KEVIN	JAMES
ROBERTSON	GILLIAN.	
ROBINDORE	FINNEGAN	SAXBY
ROBINSON	AMY	LYNN
ROBINSON	JENNIFER	MARY
ROBINSON	KIRSTEN	M
ROCHELEAU	ROBERT	EDWARD
RODRIGUEZ	PHILIPPE	DANIEL
RODRIGUEZ HERNANDEZ	ANGEL	FRANCISCO
ROESCH	NATALIE	IRMA ROSA
ROESSLER	RHEA	MARLENE
ROETER	ESTHER	DANIELLE
ROGERS	KAZUKO	YOSHIDA
ROGGERONI CURO	ANA.	
ROLFE	CHRISTOPHER	CHARLES
ROLFS	CHADWICK	MICHAEL
ROLLAND	JACQUES	ROBERT
ROLLAND	VIVIAN	JOYCE
ROMAGNOLI	LEOPOLDO.	
ROMANOW	CORA	ANNE
ROMMERTS	KAY	JAGATH
ROO	GYONGSOO.	
ROOSENBRAND	ALEXIS	REGINA
ROPP	EVAN	D
ROPP	LEON	ELDON
RORKE	MARY	KATHRYN
ROSE	JODI	NICOLE
ROSE	MICHAEL	J
ROSEN	MIKAEL	ERIK
ROSENKRANZ	SANDRA	LEE
ROSTRUP	DANIEL.	
ROVEDO	CLARA	OFELIA
ROWCLIFFE	DAVID	JOHN
ROWE	CAROLYN	HARKONNEN
ROWE	ARTHUR	FRANCIS
ROY	DAVID	HAROLD

Last name	First name	Middle name/initials
ROYER	ROLAND	JEAN PAUL
ROYER	AGNES	CLAUDINE
RUBER	HANNA	ARAI
RUBERTO	AARON	JEDEDIAH
RUBINSTEIN	RONNA	
RUDD	ANTHONY	JOHN
RUEGG	DENICE	ALANE
RUETHI	JULIAN	SEAN
RUETHI	TIMOTHY	ALAN
RUGGIERI	LEON	RIVERA
RUIZ	GERARDO	
RULE	SHEILA	ANN
RUSSELL	REBECCA	ANNE
RUTHERFORD	REBECCA	RYMER
RYALLS	MIRIAM	MEE REE
RYAN	TARA	HURLEY
RYAN	NEIL	ANTHONY
RYDER	KERRI	PING
SABLAN	FRANCESCA	KRISTINA
SACKIN	DANIEL	HENRY
SADINSKY	NOEL	LYNNE
SAGURTON	ROBERT	MICHAEL
SAIDI	IBRAHIM	
SAITO	KAZUO	
SAITO	SHIHO	
SAJO	MARI	
SALE	JUDY	JEANNE
SALETE DE VARAS	CRISTINA	MARINA SILVIA
SAMMAN	JOSEPH	
SAMSON	DAVID	BERNARD
SANATINIA	LADAN	
SANCHEZ PATZY DE FROMHERZ	CLAUDIA	VERONICA
SANDER	EVELYN	MARGARETHE
SANDIE	SOPHIE	ELIZABETH
SANDLER	BENJAMIN	JOSEPH
SANDOVAL-RASCHER	KILIAN	MARTIN
SANTO	KATASHI	
SATO	SHIGERU	
SATO	MAIKO	
SAUL	ALEXANDRA	LUCY ANNE
SAUNDERS	PER CHRISTIAN	HARALD
SAUTIN	NICHOLAS	J W
SAVAGE	ROBERT	ALAN
SAVAGE	NANCY	ANNE
SAVAGE	JUSTIN	ALEXANDER
SAVARIN	CARINE	
SAWADA	SAYOKO	
SAYER	ANNA	
SCHACHTER	MICHAEL	ELI
SCHALLER-FORRER	CLAUDIA	ESTHER
SCHENKER	EDGAR	MATHIAS
SCHENSTROM	MICHAEL	
SCHILDHAUER	ERICH	JACOB
SCHIPHOF	AXEL	PAUL
SCHLESINGER	ALEXIS	LEE
SCHLIENZ	JULIE	LOUISE
SCHMAH	CAMILLE	MARISSA
SCHMIDT	MANFRED	
SCHMIDT	JULIANE	
SCHMIDT	ELLEN	DINWIDDIE
SCHNEGG	KEVIN	JOEL
SCHNEIDER	FRAN	UDO
SCHOCH	MANUEL	
SCHOENHOLZER	YVONNE	D
SCHRANK	ANNA	LOUISE
SCHUBEL	VASILY	GREGORY
SCHUFT	VICTOR	
SCHUITEMAN	MARY	JACQUELINE
SCHULTHESS	CHRISTINE	COLETTE-COOKSON
SCHULZ	YVAN	PIERRE
SCHUWEY	CHRISTOPHE	ALEXIS
SCHWAB	WILLIAM	ANSEN SUNDE
SCHWAEBE	NICOLE	HELEN
SCHWAERTZEL	DIRK	MAX

Last name	First name	Middle name/initials
SCHWARTZ	TOBEY	D
SCHWARZ	NATALIE.	
SCHWEINSBERG	MAXI	LOUISIANA
SCOTT	YOKO	K
SCOTT	KATHERINE	SARAH
SCOTT	DAVID	MAC ANDREW
SCOTT	THOMAS	XAVIER
SCOTTEN	TEAH	NICOLE
SCRIMSHAW	CHLOE	CAROLINE
SEBAG	RAYMOND	J
SEBASTIAN	JULIAN	JOACHIM
SEDGMEN	RAMONA	FERN
SEELEY	FIONA	JAYNE
SEELEY	NICOLAS	PAUL
SEELEY	LUKE	EDGAR
SEGAL	DAVID.	
SEGMULLER	MARKUS	GOTTFRIED
SEKKER	BRANDON	LEE
SELKER	MARLENE	GISELA
SEMMLER	KAREN	HILDEGARDE
SENESE	MILAN.	
SENG	GUIDO.	
SENG	SHAY	PING
SEPULVEDA	CARMEN	GLORIA
SEREX	ALAIN	OLIVIER
SESHADRI	LAKSHMI.	
SESHADRI	SEKHER.	
SETH	CHRISTOHER	JEREMY
SHADE	LESLIE	REGAN
SHAHDOUSTI	SAGHAR.	
SHALLAL	ALI.	
SHALLAL	RAMSEY.	
SHANAHAN	LILLY.	
SHANK	MONICA	JOY
SHANK	MARVIN	JAMES
SHANNON	ELIZABETH	ANN
SHANNONHOUSE	HUNTER.	
SHARP	CATHY	ADELLE
SHAW	FRANCISKA	KALANI WEN-HUE
SHEARING	ANTHONY	DENNING
SHEHADEH	HALIM	ISAM
SHEIKH	HAMZA	ABUDAAD
SHEMIRANI	MANDA.	
SHEN	HAIYAN.	
SHENG	LI.	
SHEPHERD	BRIAN	STUART
SHERKIN	RONALD	KEVIN
SHI	BING.	
SHIBUYA	KYOKO.	
SHIKI	MEGUMI.	
SHIMAZAKI	NOBUAKI.	
SHIMAZAKI	MARI.	
SHINE	ASHLEY	ELIZABETH
SHIOTA	CHIYO.	
SHIOTA	MASAKAZU.	
SHIVRAIN	VINOD	KUMAR
SHIVRAIN	SONIA	VINOD
SHOUCAIR	ALEXANDER	NICHOLAS
SHUM	ELTON.	
SHUMATE	MICHAEL	REED
SHUMKA	MARK	ANDREW
SIERRA	MARIE	ANN
SILLS	LAUREL	JO
SILVER	SAMANTHA	DAWN
SIMEC	PETER.	
SIMON	MARY	MONIKA
SIMPSON	GEOFFREY	JAMES
SIMPSON	JESSICA	DEBORAH
SINDRAM	MARGARET	KELLY
SINGER	ACHIYA.	
SINGH	JACK	JATINDER
SKLOPIC	DEJAN.	
SLOVITT	RICK	GARY
SMALLEY	JOSEPH	ALEXANDER

Last name	First name	Middle name/initials
SMIRNYAGINA	EKATERINA	V
SMITH	ANNE	LOUISE
SMITH	JUSTIN	TRENT
SMITH	JANELLE	ANNE
SMITH	GRACE	SUZANNE
SMITH	SALLY	LOIS
SMITH	LAUREN	MICHELLE
SMYTH	GREYE	CARROLL
SNOW	KEVIN	MICHAEL
SOBOLEWSKI	MARIO.	
SOENO	YASUKO.	
SOHI	SATINDER	JIT SINGH
SOMMER	NATHALIE	CHRISTIANE
SONG	NATALIE.	
SORG	CATHERINE	ELIZABETH
SOUTHAL	COLIN	HUGH
SPAGNOLI	JESSICA	JENNIFER
SPAGNOLI	JUSTIN	JULIANO
SPEELMAN	KATLEEN.	
SPENCER	ETHAN	MICHAEL
SPIELMANN	EVA	M
SPURR	JAMES	CHRISTOPHER
SRINIVASAN	NICOLE	CLAIRE
ST AMAND	CHRISTIANE	MARIE LUCIE
ST CLAIR	JACQUELINE	MARY
STACK	MICHAEL	GERARD
STADELMANN	PHILIP	DANIEL
STANDARD	BLAKE	ANDREW
STANTON	MICHAEL	LEE
STAPLER	JENNIFER	LYNN
STARKE	NIKOLAS	HENK
STARRATT	DEBRA	CAROL
STARRATT	DAVID	EMERY
STEADMAN	MICHAEL	ALEX PETER
STEEGE	ELIZABETH	LOWERY
STEELAND	ALEXANDRA	LOUISE
STEINBERG	BENJAMIN	ETHAN
STENBERG	LISE-LOTTE	MAIJA
STENZEL	SHEILA	RAE
STEPHENS	DAVID	EARL
STERENBORG	FIIMA	JAMILA LOUA
STERICKER	JOCELYN.	
STERLING	RENEE	W
STEVENS	SIMON	LAURENCE
STEWART	COLIN	LAWSON
STEWART	MARGARET	ANNE
STEWART	ALLAN	CAREY
ST-GERMAIN	CAROLINE	HOWELL
STIEGLER	JOHAN	LENNART
STIER	JOEL.	
STIER	VERONA.	
STONE	CHRISTINA	ROSEMARIE FORBES
STONE	KATHERINE	HELEN
STORM DEVOLZ	KARINE	LYDIA DOROTHEE
STOVALL	STEN	TORBEN
STRADA	SILVIO.	
STRIDE	ANDREW	JONATHAN
STRINGER	SONIA	DAWN
STROBEL	MAGNUS	EMANUEL
STROM	ERIC	BRADFORD
STUART	DEREK	DUNCAN
STUCKI	PAUL.	
STURMAN	MARK	CHARLES
STYPULKOWSKI	ARTUR.	
SU	CHANG	YU
SUBRAMANIAN	NITHYA.	
SULTAN	FARAH	MUHANAD
SUN	XIAOHUI.	
SUN	GUIZHU.	
SUN	TIANHAO.	
SUN	ZHAOLIN.	
SUN	HUI.	
SUTER	MARTIN	DAVID
SUTER	DEBORA	LEE

Last name	First name	Middle name/initials
SUTER	CARINA	JESSICA
SUTTON	LISA	CAROLINE
SUURA	YOSHIKO.	
SUZUKI	HIDEAKI.	
SWANSON	CATHERINE	ANN
SWARTZ	AVERY	ARMSTON
SWEENEY	THOMAS	GREGORY
SWIFT	SALLY	ANNE
SYMONS	JESSICA	HELEN
SYRING	MARTINA	ELISABETH
SZABO	VERONIKA.	
SZALONTAY	PETER.	
SZETO	JENNY.	
TABAK	SHOLOM	DOV
TAGGART	WILLIAM	ROBERT
TAGUCHI	MIYAKO.	
TAHARA BIVENS	HITOMI.	
TAIT-STYLES	EVAN	ANDREW
TAKAGI	KENICHI.	
TAKAGI	MASUMI.	
TAKAHASHI	HISAKO.	
TAKAHASHI	YUJI.	
TAKASAWA	KAORI.	
TAKASAWA	TATSUO.	
TAKEUCHI	HIROO.	
TAKIGAMI	NAOMI.	
TAKIGUCHI	MIEKO.	
TAKIGUCHI	SHOJI.	
TAKIZAWA	RIKU.	
TAM	MATTHIAS	LARRY
TAMAKI	MARY	CATHERINE
TAMURA	TETSUHIRO.	
TAMURA	YOSHIKO.	
TAN	ZACHARY	ZE KANG
TAN ANG	VANESSA	BIANCA
TANAKA	HIDENORI.	
TANAKA	TATSUO.	
TANAKA	YOKO.	
TANAKA	YASUJI.	
TANEMURA	SHIGEKI.	
TANEMURA	YASUE.	
TANNER	ELIZABETH	MARY DOROTHY
TANTARN	KIM	LEANDRA
TANZAWA	HAJIME.	
TANZAWA	KAHO.	
TARDIFF	JOHN	STANTON
TARDITO	FRANCESCA	SOFIA ARAS
TASHIRO	YOKO.	
TASHIRO	YOSHIO.	
TAVANO	ALESSIO.	
TAYLOR	SARAH	ELIZABETH BROOKS
TAYLOR	ROBERT	JAMES
TAYLOR	GRIZELDA	RUTH
TAYLOR	AUDE	AURELIA
TAYLOR	SHAUN	JUSTIN
TAYLOR	ANN	DEBORAH
TAYLOR	VALERIE	JANICE
TEEUWSEN	PETER	CHRISTIAN
TEICKE	MARIA VICTORIA.	
TEICKE	NICKLAS	BENEDIKT DORIAN
TEODOROVIC	LJUBICA.	
TEP	VINCENT.	
TEP	KARRONA.	
TERNES	AINSLEY	LAUREN
TERPSTRA	JUDITH	ANN KATRINA
TETLEY	REBECCA	LYNN
THAKUR	NEETA.	
THALINGER	CHRISTIAN	FRANZ
THEORET	MARIE	JOSEE
THIAN	ZI HE.	
THIEME	JUERGEN.	
THIESSEN	BROOK	MACKENZIE
THOMAS	KATHERINE	INGRID
THOMPSON	JANET.	

Last name	First name	Middle name/initials
THOMPSON	PETER	JOHN
THOMPSON	BENJAMIN	JOHN P
TILBERG	NATALIE	MARIA SALOME
TIMMERMANN	AXEL	
TINTINALLI	FRANK	ADOLPHE
TOBIN	DANIEL	JAMES
TOKASHIKI	KEN	
TOMAN	SUSAN	
TOMITA	HIDEO	
TOMLINSON	STEPHEN	DAVID
TOMOMATSU	HIROYUKI	
TOMPKINS	KARL	HENRY
TONG	CLARA	CARMEN
TORLINSKA	LUCYNA	
TORRES	MARIA	
TORRES CORREA	GIANNI	
TORRIE	TYLER	ALEXANDER
TOSHNEY	CAROLYN	HELEN
TOUHEY	CAROLYN	WEST-PRICE
TRAKRU	SUNIL	
TRASK	MURRAY	NORMAN
TRASK	MAVIS	ELIZABETH
TRATNER	NIGEL	
TRENCH	TIMOTHY	RODERICK HAMILTON
TRENEY	ALAIN	CLAUDE
TRENT	JOHN	OLAF
TRICARICO	PASQUALE	
TRIMBLE	LESLIE	ANN
TROTT	CHELSEA	D
TROTTIER	SUZANNE	
TROYER	MARK	PATRICK
TRUDGIAN	DAVID	CLAUDE
TRUNG	MIANH	
TSAI	JASON	R
TSE	HO	KEUNG
TSENG	YINTZU	CAROLYN
TSUCHIKAWA	RISA	
TSUI	RAY	CHUNG
TSUJIMOTO	MIYAKO	
TU	CHAO	WEI
TURNARETSCHER	SYLVIA	GAIL
TURNBULL	NICOLAS	GUY
TURNBULL	ANNABELLE	LEIGH
TURNER	SHARON	ANN
TURNER	JAMES	KENNETH
TURNHAM	JAMES	RICHARD
TURNURE	GEORGE	LAWRENCE
ULRIKSSON	BENGT	ANDERS
UMBRICO	LINDA	MARIE
UNDERHILL	PETER	ARKENBURGH
URABE	HAYATO	
URBAN	ROMINA	CLAUDIA
UROWITZ	JUDITH	BRINA
USUI	REI	
USUI	DAI	
UVIMOLCHAI	CHONNAPORN	DEBBIE
UZUNOV	VESKA	KOSTADINOVA
VACHON	MARY	LOUISE
VACHON	BRUCE	RAYMOND
VADNAIS	MONIQUE	YVETTE
VAN	VANESSA	C
VAN DER LEE	REINIERUS	H
VAN DER WOLF	EVELYN	ELEANOR
VAN DER ZEE	JULIUS	T
VAN DOMSELAAR	TOM	JASPER
VAN DYCK	BABETTE	ELAINE VERONIQUE
VAN OYEN	STEFAN	HUGO
VAN ROSSUM	MENNO	DANIEL
VAN SAARLOOS	PAULIAN	CORNELIEN
VAN ZWET	JEANNETTE	M
VANCURA	PATRICK	JOSEF
VANDEBROEK	INA	EMMA G
VELA	SHEILA	RAE
VELISSAROPOULOS	ARIANNE	

Last name	First name	Middle name/initials
VERLEDENS	MARTINE	MICHELE THERESE
VICHOT	DOMINIQUE	CLAUDE
VIDAL	MYRIAM	
VIGNALE	VINCENT	E
VIGON	BRAD	PAUL
VINCELI-JOMA	ADRIANA	KATERINA
VINCELLI	CARLA	LUCIA
VINTI GLAESER	LAURA	
VOGELER	SUZANNA	JULIET
VON MOOS	NADIA	RACHEL
VONIC	ANKA	
WADA	JUNKO	
WADE	JEFFREY	PAUL
WAECHTER	MARGARET	CLARE
WALDER	JAMES	NICHOLAS HAMPTON
WALKER	SELENA	NADIA
WALL	DIANE	
WALL	PHILIP	MALCOLM
WALLSMITH	DEBORAH	LYNNE
WALTER	MELISSA	EMERSON
WALTERS	WALLACE	WARREN
WANG	HSIAO	WEI
WANG	KUI	
WANG	JEE	SHIANG
WANG	WENSHOU	
WARD	BRODIE	THOMAS
WARMERDAM	VINCENT	DAMIAN
WARNANDER	CLAES	ROBERT
WARREN	ROBERT	PAUL
WARRIER	HRIDYA	
WARRIER	AJAY	HARIKUMAR
WATANABE	FUJIO	
WATANABE	KAZUhide	
WATANABE	YOSHIE	
WATANABE	ERIKO	
WATANABE	MAKIKO	
WATERS	CAMILLA	JEAN
WATSON	KEVIN	ROBERT
WATT	JUDY	BIK-WOON
WATT	KELSEY	ALEXANDRA
WAYLETT	PATRICK	GARRY
WEBB	TIMOTHY	ALAN
WEBBER	JOHN	LAWSON
WEBER	LUKE	ANDREW
WEBER	ERIC	CARL
WEBER	MARTIN	PETER
WEBER	KENNETH	ROMAN
WEE	JIAN	MING COLIN
WEI	LIPING	
WEI	JENNY	
WEINGART	SARAH	GAYLE
WEINSCHROD	PHILIPP	
WELCH-HAMMIAL	GENEVIEVE	ALOKA
WELLS	DAVID	WAYNE
WELLS	MICHAEL	PETER
WELSH	CHRISTINE	M
WELSH	FREDERICK	CANNON
WENG	HONGLI	
WENTZEL	CAROLYN	ANN
WEREMY	NICOLE	LOREE
WERENKA	JUDITH	ANNE
WERNER-KING	JANEEN	ANNE
WERTHEYM	MONIQUE	ALICE SIMONETTA
WEST	ROBIN	ELIZABETH
WESTER	SUSAN	BETH
WESTERVELT	CHRISTINA	
WESTLAND	JOHANNA	LISA
WESTLAND	BENJAMIN	ALEX
WESTLAND	ALICIA	JADE
WESTLAND	JASON	BRENT
WESTPHAL	CAROLYN	ELIZABETH
WESTPHAL	HELENA	DOROTHY MADELINE
WESTWOOD	JOYCE	LYNN
WHANG	TAEHEE	

Last name	First name	Middle name/initials
WHEATLEY	CLAIRE	MARGARET
WHINCOP	DANIEL	NOEL
WHINCOP	FIONA	
WHIPP	KATHLEEN	JANE
WHITBY	RACHEL	CRISTINA
WHITE	CLAY	THOMAS
WHITE	ARIEL	BLITHE MAXWELL
WHITEBREAD	CHRISTINE	
WHITEING	NEIL	PETER KRAUSE
WHITFORD	IAIN	J
WHITTINGHAM	JESSICA	NORA
WIBBERLEY	BENJAMIN	GUY
WIDMER	MARCO	JAKOB
WIDMER	LAURA	ISABEL
WIDOWITZ	ELMAR	
WIDOWITZ	SANDRA	
WIEBE	PATRICIA	KAREN
WIENECKE	GERT	
WIJCHGEL	WIEGER	NANCO
WILDER	EMMA	LOUISE
WILKE	ANGELA	CHRISTINE
WILKIE	CARLA	ANN
WILLAN	GERARD	L
WILLIAMS	JUSTINE	MILLICENT
WILLIAMS	MARIE	
WILLIAMS	ANDREW	CARL
WILLIAMS	MIRIAM	ZEHAVA
WILLIAMSON	MARLENE	EDITH
WILLIS	HAZEL	
WILSDON	JOSHUA	DAVID
WILSON	IAIN	AULD
WILSON	REBECCA	RUTH
WILSON	JONATHAN	
WINTON	GRANT	STUART
WIRTH	THOMAS	
WIWCHAR	MICHELE	ANN
WOLFRAM	JOY	EMELIE VALENTINA
WOLF-UNGAR	GISELLE	
WOLKEN	ADRIAN	GEORGE
WOLSEY	TROY	DANIEL JOHN STEWART
WOLTER	TOBIAS	
WONG	PATRICIA	ANN
WONG	KING	CHUNG
WONG	JUSTIN	KALEUNG
WOOD	JANET	LYNN
WOODCROFT	DIANE	AMOS
WOODLEY	JAMES	ARTHUR
WOODS	ROBIN	JAMES
WOODY	CORNELIA	ANNA
WOOMERT	JOHN	BARTON
WREN	ISABELLA	GRACE
WRIGHT	MARY	ANN
WRIGHT	MAXIMILIAN	JOHN
WRIGHT	VICTORIA	EFTYCHIA
WU	WEI	LUNG SAM
WU	MENGDI	
WU	XUFEI	
WU	JULIANA	L
WUETHRICH KELLERHALS	ELISABETH	
WYER	MARLA	VERNE
XIANG	SOPHIA	FEI FEI
XIE	TAO	
XU	LIN	
YAGUCHI	AYAKO	
YAGUCHI	TETSUYA	
YAJIMA	MARI	
YAMAGATA	AYAKA	
YAMAGUCHI	YOSHINORI	
YAMAMOTO	YOSHIKO	
YAMANOUCHI	CHISE	MIGITAKA
YAMASHITA	MIKA	
YAMAZAKI	JIRO	
YAMAZAKI	MITSUHIRO	
YAN	JUN	

Last name	First name	Middle name/initials
YAN	XIANGUANG.	YUN
YANG	JEONG	
YANG	LIU.	
YANG	JIONG.	
YANG	HANN.	BRYAN
YANZUK	CHRISTOPHER	
YAO	HONGYU.	PING O
YAO	LIPING	
YASUDA	RUMIKO	ANN
YASUDA	HIROMARO.	
YATES	SHEILA	KIEN-HUNG
YAZIJI	MICHAEL.	
YEO	HENRY	TAE BEN
YI	LI.	
YIN	XIAOWEI.	
YOKOSE	TOMOAKI.	
YOKOTA	MARI.	KA YEN
YOO	DAHEY.	
YOO	HEE	
YOSEF	DANNY	
YOSHIDA	MAKOTO.	ANGELO SAMI Y KAY
YOSHIZUMI	TETSUO.	
YOUNG	DOUGLAS.	
YU	YING.	
YUEN	KAREN	ANNE
ZAFEIROPOULOS	KONSTANTINOS.	
ZANOLLA	STEWART	
ZARKA	HISHAM	
ZAU	LILLIAN	TRIFONOV DIMITROVA
ZAUGG	MAXWELL	
ZECCHIN	ANDREA.	
ZENG	SHUXIANG.	
ZENSIUS	KIMBERLY	RENEE RENEE MARIE FRANCIS
ZHANG	PING.	
ZHANG	YAN.	
ZHANG	BIN.	
ZHANG	WEI.	SHAW MARGARET
ZHELEV	YORDAN	
ZHELEVA	MARIYA	
ZHENG	SHAOQUN.	
ZHENG	YONGMING.	SHAW MARGARET
ZHU	XIAOMING.	
ZIMMERMAN	JULIE	
ZIMMERMANN	ALLYSON	
ZIOTEK BADDOUR	WANDA	SHAW MARGARET
ZIPP	DANIEL	
ZOLFAGHARI	FARZAD.	
ZORICH	MIROSLAV.	
ZUEGER	PHILIP.	SHAW MARGARET
ZUMBRUNNEN	DANIEL	
ZWART	ANNA	

Dated: October 24, 2024.

Steven B. Levine,

Manager Team 1940, CSDC—Compliance
Support, Development & Communications.

[FR Doc. 2024-25123 Filed 10-28-24; 8:45 am]

BILLING CODE 4830-01-P

DEPARTMENT OF THE TREASURY

Internal Revenue Service

Agency Collection Activities; Requesting Comments on Form 709, Form 709-NA.

AGENCY: Internal Revenue Service (IRS),
Treasury.

ACTION: Notice and request for
comments.

SUMMARY: The Internal Revenue Service, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995. The IRS is soliciting comments concerning Form 709, United States Gift (and Generation-Skipping Transfer) Tax Return. Form 709-NA United States Gift (and Generation-Skipping Transfer) Tax Return of

Nonresident Not a Citizen of the United States.

DATES: Written comments should be received on or before December 30, 2024 to be assured of consideration.

ADDRESSES: Direct all written comments to Andres Garcia, Internal Revenue Service, Room 6526, 1111 Constitution Avenue NW, Washington, DC 20224, or by email to pra.comments@irs.gov. Include OMB Control No. 1545-0020 in the subject line of the message.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of this collection should be directed to Jason Schoonmaker, (801) 620-2128, at Internal Revenue Service,

Room 6526, 1111 Constitution Avenue NW, Washington, DC 20224, or through the internet at jason.m.schoonmaker@irs.gov.

SUPPLEMENTARY INFORMATION: The IRS is currently seeking comments concerning the following information collection tools, reporting, and record-keeping requirements:

Title: United States Gift (and Generation-Skipping Transfer) Tax Return.

OMB Number: 1545-0020.

Form Number: Form 709, 709-NA.

Abstract: Form 709 is used by individuals to report transfers subject to the gift and generation-skipping transfer taxes and to compute these taxes. The IRS uses the information to collect and enforce these taxes, to verify that the taxes are properly computed, and to compute the tax base for the estate tax. Form 709-NA is used to report certain transfers by a nonresident not a citizen of the United States that are subject to the federal gift tax and certain generation-skipping transfer (GST) taxes and to figure the tax due, if any, on those transfers. The Form 709-NA is

also used to allocate the lifetime GST exemption to property transferred during a transferor's lifetime.

Current Actions: Form 709-NA is a new form.

Type of Review: Revision to previously approved collection.

Affected Public: Individuals and household.

Estimated Number of Responses: 225,530.

Estimated Time per Respondent: 6 hours, 12 minutes.

Estimated Total Annual Burden Hours: 1,398,286.

The following paragraph applies to all of the collections of information covered by this notice:

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the collection of information displays a valid OMB control number. Books or records relating to a collection of information must be retained as long as their contents may become material in the administration of any internal revenue law. Generally, tax returns and tax return information are confidential, as required by 26 U.S.C. 6103.

Request for Comments: Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval. All comments will become a matter of public record. Comments are invited on: (a) Whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology; and (e) estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information.

Approved: October 24, 2024.

Jason M. Schoonmaker,
Tax Analyst.

[FR Doc. 2024-25092 Filed 10-28-24; 8:45 am]

BILLING CODE 4830-01-P



FEDERAL REGISTER

Vol. 89

Tuesday,

No. 209

October 29, 2024

Part II

Department of Justice

28 CFR Part 202

Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Person; Proposed Rule

DEPARTMENT OF JUSTICE**28 CFR Part 202****[Docket No. NSD 104]****RIN 1124-AA01****Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons****AGENCY:** National Security Division, Department of Justice.**ACTION:** Proposed rule; request for comments.

SUMMARY: The Department of Justice proposes a rule to implement Executive Order 14117 of February 28, 2024 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern), by prohibiting and restricting certain data transactions with certain countries or persons.

DATES: Written comments on this notice of proposed rulemaking (NPRM) must be received by November 29, 2024.

ADDRESSES: You may send comments, identified by Docket No. NSD 104, by either of the following methods:

- *Federal eRulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for sending comments.

- *Mail:* U.S. Department of Justice, National Security Division, Foreign Investment Review Section, 175 N Street NE, 12th Floor, Washington, DC 20002.

FOR FURTHER INFORMATION CONTACT:

Email (preferred):

NSD.FIRS.datasecurity@usdoj.gov.

Otherwise, please contact: Lee Licata, Deputy Chief for National Security Data Risks, Foreign Investment Review Section, National Security Division, U.S. Department of Justice, 175 N Street NE, Washington, DC 20002; Telephone: 202-514-8648.

SUPPLEMENTARY INFORMATION: In accordance with 5 U.S.C. 553(b)(4), a plain language summary of the proposed rule is available at www.regulations.gov.

Public Participation

Instructions: We encourage comments to be submitted via <https://www.regulations.gov>. Please submit comments only, include your name and company name (if any), and cite "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" in all correspondence. Anyone submitting business confidential

information should clearly identify the business confidential portion at the time of submission, file a statement justifying nondisclosure and referring to the specific legal authority claimed, and provide a non-confidential version of the submission. For comments submitted electronically containing business confidential information, the file name of the business confidential version should begin with the characters "BC." Any page containing business confidential information must be clearly marked "BUSINESS CONFIDENTIAL" at the top of that page. The corresponding non-confidential version of those comments must be clearly marked "PUBLIC." The file name of the nonconfidential version should begin with the character "P." Any submissions with file names that do not begin with a "BC" will be assumed to be public and will be posted without change, including any business or personal information provided, such as names, addresses, email addresses, or telephone numbers.

To facilitate an efficient review of submissions, the Department of Justice encourages but does not require commenters to: (1) submit a short executive summary at the beginning of all comments; (2) provide supporting material, including empirical data, findings, and analysis in reports or studies by established organizations or research institutions; (3) describe the relative benefits and costs of the approach contemplated in this NPRM and any alternative approaches; and (4) refer to the specific proposed subpart or defined term to which each comment is addressed. The Department of Justice welcomes interested parties' submissions of written comments discussing relevant experiences, information, and views. Parties wishing to supplement their written comments with a follow-up meeting may request to do so, and the Department of Justice may accommodate such requests as resources permit.

Table of Contents

- I. Executive Summary
- II. Background
- III. Advance Notice of Proposed Rulemaking and Comments
- IV. Discussion of the Proposed Rule
 - A. Subpart C—Prohibited Transactions and Related Activities
 - 1. Section 202.210—Covered Data Transactions
 - 2. Section 202.301—Prohibited Data-Brokerage Transactions
 - 3. Section 202.201—Access
 - 4. Section 202.249—Sensitive Personal Data
 - 5. Section 202.212—Covered Personal Identifiers

- 6. Section 202.234—Listed Identifier
- 7. Section 202.242—Precise Geolocation Data
- 8. Section 202.204—Biometric Identifiers
- 9. Section 202.224—Human Genomic Data
- 10. Other Human 'Omic Data
- 11. Section 202.240—Personal Financial Data
- 12. Section 202.241—Personal Health Data
- 13. Section 202.206—Bulk U.S. Sensitive Personal Data
- 14. Section 202.205—Bulk
- 15. Section 202.222—Government-Related Data
- 16. Section 202.302—Other Prohibited Data-Brokerage Transactions Involving Potential Onward Transfer to Countries of Concern or Covered Persons
- 17. Section 202.303—Prohibited Human Genomic Data and Human Biospecimen Transactions
- 18. Section 202.304—Prohibited Evasions, Attempts, Causing Violations, and Conspiracies
- 19. Section 202.305—Knowingly Directing Prohibited Transactions
- 20. Section 202.215—Directing
- 21. Section 202.230—Knowingly
- B. Subpart D—Restricted Transactions
 - 1. Section 202.401—Authorization To Conduct Restricted Transactions; Section 202.402—Incorporation by Reference
 - 2. Section 202.258—Vendor Agreement
 - 3. Section 202.217—Employment Agreement
 - 4. Section 202.228—Investment Agreement
- C. Subpart E—Exempt Transactions
 - 1. Section 202.501—Personal Communications; Section 202.502—Information or Informational Materials; and Section 402.503—Travel
 - 2. Section 202.504—Official Business of the United States Government
 - 3. Section 202.505—Financial Services
 - 4. Section 202.506—Corporate Group Transactions
 - 5. Section 202.507—Transactions Required or Authorized by Federal Law or International Agreements, or Necessary for Compliance With Federal Law
 - 6. Section 202.508—Investment Agreements Subject to a CFIUS Action
 - 7. Section 202.509—Telecommunications Services
 - 8. Section 202.510—Drug, Biological Product, and Medical Device Authorizations
 - 9. Section 202.511—Other Clinical Investigations and Post-Marketing Surveillance Data
 - 10. Other Exemptions
- D. Subpart F—Determination of Countries of Concern
 - 1. Section 202.601—Determination of Countries of Concern
 - a. China
 - b. Cuba
 - c. Iran
 - d. North Korea
 - e. Russia
 - f. Venezuela
- E. Subpart G—Covered Persons
 - 1. Section 202.211—Covered Person
 - 2. Section 202.701—Designation of Covered Persons
- F. Subpart H—Licensing

1. Section 202.801—General Licenses
2. Section 202.802—Specific Licenses
3. Conditions on General and Specific Licenses
- G. Subpart I—Advisory Opinions
 1. Section 202.901—Inquiries Concerning Application of This Part
- H. Subpart J—Due Diligence and Audit Requirements
 1. Section 202.1001—Due Diligence for Restricted Transactions
 2. Section 202.1002—Audits for Restricted Transactions
- I. Subpart K—Reporting and Recordkeeping Requirements
 1. Section 202.1101—Records and Recordkeeping Requirements
 2. Section 202.1102—Reports To Be Furnished on Demand
 3. Section 202.1103—Annual Reports
 4. Section 202.1104—Reports on Rejected Prohibited Transactions
- J. Subpart M—Penalties and Finding of Violation
 1. Section 202.1301—Penalties for Violations
 2. Section 202.1305—Finding of Violation
- K. Coordination With Other Regulatory Regimes
- L. Severability
- V. Analysis for Proposed Bulk Thresholds
 - A. Analysis of Sensitivity of Each Category of Sensitive Personal Data
 1. Human Genomic Data
 2. Biometric Identifiers
 3. Precise Geolocation Data
 4. Personal Health Data
 5. Personal Financial Data
 6. Covered Personal Identifiers
 - B. Grouping the Categories Into Tiers by Similar Sensitivity
 - C. Proposed Bulk Thresholds for Each Tier
- VI. Interpretation of “Information or Informational Materials” in IEEPA
 - A. The Berman Amendment Is Intended To Protect the Free Exchange of Ideas
 - B. The Berman Amendment Does Not Reach Transactions Involving Sensitive Personal Data Under This Proposed Rule
 - C. Exclusion for Materials Already Created and in Existence
- VII. Regulatory Requirements
 - A. Executive Orders 12866 (Regulatory Planning and Review) as Amended by Executive Orders 13563 (Improving Regulation and Regulatory Review) and 14094 (Modernizing Regulatory Review)
 1. Executive Summary
 2. Introduction
 3. Market Sectors Impacted by the Proposed Regulation
 - a. Sensitive Personal Data and Government-Related Data
 - i. Personal Financial Data
 - ii. Personal Health Data
 - iii. Precise Geolocation Data
 - iv. Human Genomic and Human ‘Omic Data
 - v. Biometric Identifiers
 - vi. Covered Personal Identifiers
 - b. The Data-Brokerage Market
 - i. Companies That May Meet the Definition of Data Brokers for the Purposes of the Proposed Rule
 - ii. Market Size
 - iii. Products Sold by Data Brokers
 - iv. Price Information
 - v. Customers of Data-Brokerage Products
 - c. Agreements Affected by the Proposed Regulation
 - i. Vendor Agreements
 - ii. Employment Agreements
 - iii. Investment Agreements
 - iv. Security Requirements
 - v. Due Diligence and Recordkeeping
 - vi. Audits
 - vii. Licenses
 4. Need for Regulatory Action
 5. Baseline (Without the Proposed Rule)
 - a. Baseline National Security and Foreign-Policy Risks by Category of Data
 - i. Human Genomic and Human ‘Omic Data
 - ii. Biometric Identifiers
 - iii. Precise Geolocation Data
 - iv. Personal Health Data
 - v. Personal Financial Data
 - vi. Covered Personal Identifiers
 - vii. Government-Related Data
 - b. Baseline: Total Potential U.S. Population Affected by Risks
 - c. Summary of Baseline (Without the Proposed Rule)
 6. Alternative Approaches
 7. Benefits of the Proposed Rule
 8. Costs of the Proposed Rule
 - a. Value of Lost and Forgone Transactions
 - i. Global Market Value of Genomic, Biometric, and Location Data
 - ii. U.S. Exports to Relevant Specific Categories and to Countries of Concern
 - iii. Estimates of U.S. Exports of Genomic, Biometric, and Location Data
 - iv. Estimates of U.S. Exports of Genomic, Biometric, and Location Data to the Six Countries of Concern
 - v. Total Estimated Value of Lost and Forgone Transactions
 - vi. Alternative Methodology for Estimating the Value of Lost and Forgone Transactions
 - b. Security Costs
 - i. Similar Security Standards and Frameworks
 - ii. Current Industry Compliance Level
 - iii. Costs of Compliance
 - c. Costs Associated With Compliance Program: Due Diligence, Recordkeeping, and Auditing
 - i. Due Diligence Costs
 - ii. Recordkeeping Costs
 - iii. Executive Order on Modernizing Regulatory Review Recordkeeping and Related Costs
 - iv. Auditing Costs
 - v. Estimated Recordkeeping Costs From the Reviewed Literature
 - vi. Summary of a Compliance Program: Due Diligence, Recordkeeping, and Auditing
 9. Summary of Regulatory Analysis
 - B. Regulatory Flexibility Act
 1. Succinct Statement of the Objectives of, and Legal Basis for, the Proposed Rule
 2. Description of and, Where Feasible, an Estimate of the Number of Small Entities to Which The Proposed Rule Will Apply
 3. Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Proposed Rule
 4. Identification of all Relevant Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rule

- C. Executive Order 13132 (Federalism)
- D. Executive Order 13175 (Consultation and Coordination With Indian Tribal Governments)
- E. Executive Order 12988 (Civil Justice Reform)
- F. Paperwork Reduction Act
- G. Unfunded Mandates Reform Act

I. Executive Summary

Executive Order 14117 of February 28, 2024, “Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern” (“the Order”), directs the Attorney General to issue regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest (“transaction”), where the transaction: involves United States Government-related data (“government-related data”) or bulk U.S. sensitive personal data, as defined by final rules implementing the Order; falls within a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because it may enable access by countries of concern or covered persons to government-related data or Americans’ bulk U.S. sensitive personal data; and meets other criteria specified by the Order. On March 5, 2024, the National Security Division of the Department of Justice (“DOJ” or “the Department”) issued an Advance Notice of Proposed Rulemaking (“ANPRM”) seeking public comment on various topics related to implementation of the Order.¹

This Notice of Proposed Rulemaking (“NPRM”) addresses the public comments received on the ANPRM, sets forth a proposed rule to implement the Order, and seeks public comment. The proposed rule identifies classes of prohibited and restricted transactions; identifies countries of concern and classes of covered persons with whom the regulations would prohibit or restrict transactions involving government-related data or bulk U.S. sensitive personal data; establishes a process to issue (including to modify or rescind) licenses authorizing otherwise prohibited or restricted transactions and to issue advisory opinions; and addresses recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts of the Department of Justice.

¹ 89 FR 15780 (Mar. 5, 2024).

II. Background

On February 28, 2024, the President issued Executive Order 14117 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern) ("the Order"), pursuant to his authority under the Constitution and the laws of the United States, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) ("IEEPA"); the National Emergencies Act (50 U.S.C. 1601 *et seq.*) ("NEA"); and title 3, section 301 of the United States Code. In the Order, the President expanded the scope of the national emergency declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data From Foreign Adversaries). The President determined that additional measures are necessary to counter the unusual and extraordinary threat to U.S. national security posed by the continuing efforts of certain countries of concern to access and exploit government-related data or Americans' bulk U.S. sensitive personal data.

The Order directs the Attorney General, pursuant to the President's delegation of his authorities under IEEPA, to issue regulations that prohibit or otherwise restrict United States persons from engaging in certain transactions in which a foreign country of concern or national thereof has an interest. Restricted and prohibited transactions include transactions that involve government-related data or bulk U.S. sensitive personal data, are a member of a class of transactions that the Attorney General has determined poses an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data, and are not otherwise exempted from the Order or its implementing regulations. The Order directs the Attorney General to issue regulations that identify classes of prohibited and restricted transactions; identify countries of concern and classes of covered persons whose access to government-related data or bulk U.S. sensitive personal data poses the national security risk described in the Order; establish a process to issue (including to modify or rescind) licenses authorizing otherwise prohibited or restricted transactions; further define terms used in the Order;

address recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts of the Department of Justice; and to take whatever additional actions, including promulgating additional regulations, as may be necessary to carry out the purposes of the Order.

The Order and this proposed rule fill an important gap in the United States Government's authorities to address the threat posed by countries of concern accessing government-related data or Americans' bulk U.S. sensitive personal data. As the President determined in the Order, "[a]ccess to Americans' bulk sensitive personal data or United States Government-related data increases the ability of countries of concern to engage in a wide range of malicious activities." As the ANPRM explained, countries of concern can use their access to government-related data or Americans' bulk U.S. sensitive personal data to engage in malicious cyber-enabled activities and malign foreign influence activities and to track and build profiles on U.S. individuals, including members of the military and other Federal employees and contractors, for illicit purposes such as blackmail and espionage. And countries of concern can exploit their access to government-related data or Americans' bulk U.S. sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, or members of nongovernmental organizations or marginalized communities to intimidate them; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

As the 2024 National Counterintelligence Strategy explains, "as part of a broader focus on data as a strategic resource, our adversaries are interested in personally identifiable information (PII) about U.S. citizens and others, such as biometric and genomic data, health care data, geolocation information, vehicle telemetry information, mobile device information, financial transaction data, and data on individuals' political affiliations and leanings, hobbies, and interests."² These and other kinds of sensitive personal data "can be especially valuable, providing adversaries not only economic and [research and development] benefits, but also useful [counterintelligence] information, as hostile intelligence services can use

vulnerabilities gleaned from such data to target and blackmail individuals."³

Nongovernmental experts have underscored these risks. For example, a recent study by the MITRE Corporation summarized open-source reporting, highlighting the threat of blackmail, coercion, identification of high-risk government personnel and sensitive locations, and improved targeting of offensive cyber operations and network exploitation posed by hostile actors' access to Americans' data derived from advertising technology.⁴

The development of artificial intelligence ("AI"), high-performance computing, big-data analytics, and other advanced technological capabilities by countries of concern amplifies the threat posed by these countries' access to government-related data or Americans' bulk U.S. sensitive personal data. For instance, the U.S. National Intelligence Council assessed in 2020 that "access to personal data of other countries' citizens, along with [artificial intelligence]-driven analytics, will enable [the People's Republic of China] to automate the identification of individuals and groups beyond China's borders to target with propaganda or censorship."⁵

Countries of concern can also exploit their access to government-related data regardless of volume to threaten U.S. national security. One academic study explained that "[f]oreign and malign actors could use location datasets to stalk or track high-profile military or political targets," revealing "sensitive locations—such as visits to a place of worship, a gambling venue, a health clinic, or a gay bar—which again could be used for profiling, coercion, blackmail, or other purposes."⁶ The MITRE report further explained that location datasets could reveal "U.S. military bases and undisclosed intelligence sites" or "be used to

³ *Id.*

⁴ Kirsten Hazelrig, Ser. No. 14, *Intelligence After Next: Surveillance Technologies Are Imbedded Into the Fabric of Modern Life—The Intelligence Community Must Respond*, The MITRE Corporation 2 (Jan. 5, 2023), <https://www.mitre.org/sites/default/files/2023-01/PR-22-4107-INTELLIGENCE-AFTER-NEXT-14-January-2023.pdf> [<https://perma.cc/3WA2-PGM2>].

⁵ Nat'l Intel. Council, *Assessment: Cyber Operations Enabling Expansive Digital Authoritarianism* 4 (Apr. 7, 2020), <https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-2020407-2022.pdf> [<https://perma.cc/ZKJ4-TBU6>].

⁶ Justin Sherman et al., Duke Sanford Sch. of Pub. Pol'y, *Data Brokers and the Sale of Data on U.S. Military Personnel* 15 (Nov. 2023), <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf> [<https://perma.cc/BBJ9-44UH>].

² Nat'l Counterintel. & Sec. Ctr., *National Counterintelligence Strategy* 2024 13 (Aug. 1, 2024), https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf [<https://perma.cc/9L2T-VXSU>].

estimate military population or troop buildup in specific areas around the world or even identify areas of off-base congregation to target.”⁷ As another example of these data risks and the relative ease with which they can be exploited, journalists were able to commercially acquire from a data broker a continuous stream of 3.6 billion geolocation data points that were lawfully collected on millions of people from advertising IDs.⁸ The journalists were then able to create “movement profiles” for tens of thousands of national security and military officials, and from there, could determine where they lived and worked as well as their names, education levels, family situations, and hobbies.⁹

The Order and this proposed rule seek to mitigate these and other national security threats that arise from countries of concern accessing government-related data or Americans’ bulk U.S. sensitive personal data.

No current Federal legislation or rule categorically prohibits or imposes security requirements to prevent U.S. persons from providing countries of concern or covered persons access to sensitive personal data or government-related data through data brokerage, vendor, employment, or investment agreements. For example, the scope and structure of the Protecting Americans’ Data from Foreign Adversaries Act of 2024 (*see* Pub. L. 118–50, div. I, 118th Cong. (2024)) do not create a comprehensive regulatory scheme that adequately and categorically addresses these national security risks, as explained in part IV.K of this preamble. Likewise, the Committee on Foreign Investment in the United States (“CFIUS”) has authority to assess the potential national security risks of certain investments by foreign persons in certain United States businesses that “maintain[] or collect[] sensitive personal data of United States citizens that may be exploited in a manner that threatens national security.”¹⁰ CFIUS only reviews certain types of investments in U.S. businesses; it does so on a transaction-by-transaction basis, instead of prescribing prospective and categorical rules regulating all such transactions; and its authorities do not

extend to other activities that countries of concern may use to gain access to government-related data or Americans’ bulk U.S. sensitive personal data, such as through purchases of such data on the commercial market or through vendor or employment agreements.¹¹

Similarly, Executive Order 13873 prohibits any acquisition, importation, transfer, installation, dealing in or use of by U.S. persons from acquiring certain information and communication technologies and services (“ICTS”) designed, developed, manufactured, or supplied by foreign adversaries where, among other things, the Secretary of Commerce determines that the transaction poses an “unacceptable risk to the national security of the United States or the security and safety of United States persons.”¹² In building upon the national emergency declared in Executive Order 13873, the President, in Executive Order 14034, determined that connected software applications operating on U.S. ICTS “can access and capture vast swaths of . . . personal information and proprietary business information,” a practice that “threatens to provide foreign adversaries with access to that information.”¹³ However, as with CFIUS legal authorities, the orders do not broadly empower the United States Government to prohibit or otherwise restrict the sale of government-related data or Americans’ bulk U.S. sensitive personal data, and the orders do not broadly restrict other commercial transactions, such as investment, employment, or vendor agreements, that may provide countries of concern access to government-related data or Americans’ bulk U.S. sensitive personal data.

The proposed rule would complement these statutory and regulatory authorities. It prescribes forward-looking, categorical rules that prevent U.S. persons from providing countries of concern or covered persons access to government-related data or Americans’ bulk U.S. sensitive personal data through commercial data-brokerage transactions. The proposed rule also imposes security requirements on other kinds of commercial transactions, such as investment, employment, and vendor agreements, that involve government-related data or Americans’ bulk U.S. sensitive personal data to mitigate the risk that a country of concern could access such data. The proposed rule would address risks to government-

related data or Americans’ bulk U.S. sensitive personal data that current authorities leave vulnerable to access and exploitation by countries of concern and provide predictability and regulatory certainty by prescribing categorical rules regulating certain kinds of data transactions that could give countries of concern or covered persons access to government-related data or Americans’ bulk U.S. sensitive personal data.

III. Advance Notice of Proposed Rulemaking and Comments

The National Security Division of the Department published an ANPRM on March 5, 2024 (former RIN: 1105–AB72), soliciting public comment on various topics related to the Order.¹⁴ The Department received and carefully reviewed 64 timely comments in response to the ANPRM from trade associations, public interest advocacy groups, think tanks, private individuals, and companies, as well as comments from several foreign governments. The Department also received two additional *ex parte* comments after the comment period closed, which DOJ publicly posted on *regulations.gov*.

During the comment period, the Department of Justice, both on its own and with other agencies, met with businesses, trade groups, and other stakeholders potentially interested in or impacted by the contemplated regulations to discuss the ANPRM. For example, the Department discussed the ANPRM with the Consumer Technology Association, the Information Industry Technology Council, Pharmaceutical Research and Manufacturers of America, the Biotechnology Innovation Organization, the Bioeconomy Information Sharing Analysis Center, the U.S. Chamber of Commerce, Tesla, Workday, Anthropic, and the Special Competitive Studies Project, and it provided briefings to the Secretary of Commerce and Industry Trade Advisory Committees 6, 10, and 12 administered by the Office of the U.S. Trade Representative and the Department of Commerce. The Department also discussed the Order and contemplated regulations with stakeholders at events open to the public, including ones hosted by the American Conference Institute, the American Bar Association, the Center for Strategic and International Studies, and the R Street Institute, and through other public engagements such as the Lawfare Podcast, ChinaTalk Podcast, CyberLaw Podcast, and the Center for

⁷ *Id.*

⁸ Suzanne Smalley, *US Company’s Geolocation Data Transaction Draws Intense Scrutiny in Germany*, The Record (July 18, 2024), <https://therecord.media/germany-geolocation-us-data-broker> [<https://perma.cc/ME9F-TAQ7>] (citing joint reporting by the German public broadcaster Bayerische Rundfunk and digital civil rights opinion news site *netzpolitik.org*).

⁹ *Id.*

¹⁰ 50 U.S.C. 4565(a)(4)(B)(iii)(III).

¹¹ *See generally* Foreign Investment Risk Review Modernization Act of 2018, Public Law 115–232, tit. XVII, secs. 1701–28, 132 Stat. 1636, 2173.

¹² E.O. 13873 of May 15, 2019, 84 FR 22689, 22690 (May 15, 2019).

¹³ E.O. 14034, 86 FR 31423, 31423 (June 9, 2021).

¹⁴ 89 FR 15780 (Mar. 5, 2024).

Cybersecurity Policy & Law's Distilling Cyber Policy podcast.

After the comment period closed, the Department of Justice, along with the Department of Commerce, followed up with commenters who provided feedback regarding the bulk thresholds to discuss that topic in more detail, including the Council on Government Relations Industry Association, Association of American Medical Colleges, Airlines for America, Bank Policy Institute, the Business Roundtable, Information Technology Industry Council, Centre for Information Policy Leadership, Biotechnology Innovation Organization, Software and Information Industry Association, Cellular Telephone Industries Association, the internet and Television Association, US Telecom, Ford Motor Company, Bioeconomy Information Sharing and Analysis Center, Coalition of Services Industries, Enterprise Cloud Coalition, Electronic Privacy Information Center, Center for Democracy and Technology, Business Software Alliance, Global Data Alliance, Interactive Advertising Bureau, U.S.-China Business Council, IBM, Workday, and individuals Justin Sherman, Mark Febrizio, and Charlie Lorthioir. The Department has also discussed the Order and the ANPRM with foreign partners to ensure that they understood the Order and contemplated program and how they fit into broader national security, economic, and trade policies.

The Department considered each comment submitted, including the *ex parte* comments that have since been publicly posted. Many of the comments were general in nature and supported the Department's efforts and approach with respect to the proposed rule. Overall, commenters were generally supportive of the intent of the proposed rule. However, several commentators representing industry questioned the effectiveness of the proposed rule as compared to the passage of a holistic federal privacy law, proposed revisions, and highlighted areas where the proposed rule would benefit from further clarity. The Department discusses comments, and any edits or revisions made in response to the comments, in the discussion of the proposed rule in part IV of this preamble.

IV. Discussion of the Proposed Rule

The proposed rule implements the Order through categorical rules that regulate certain data transactions involving government-related data or bulk U.S. sensitive personal data that could give countries of concern or covered persons access or the ability to

access such data and present an unacceptable risk to U.S. national security. The proposed rule (1) identifies certain classes of highly sensitive transactions with countries of concern or covered persons that the proposed rule would prohibit in their entirety ("prohibited transactions") and (2) identifies other classes of transactions that would be prohibited except to the extent they comply with predefined security requirements ("restricted transactions") to mitigate the risk of access to bulk U.S. sensitive personal data by countries of concern. The Attorney General has determined that the prohibited and restricted transactions set forth in the proposed rule pose an unacceptable risk to the national security of the United States because they may enable countries of concern or covered persons to access and exploit government-related data or bulk U.S. sensitive personal data.

In addition to identifying classes of prohibited and restricted transactions that pose an unacceptable risk to national security, the proposed rule identifies certain classes of transactions that are exempt from the proposed rule. For example, the proposed rule exempts transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof, and transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government, including those for outbreak and pandemic prevention, preparedness, and response. The proposed rule also defines relevant terms; identifies countries of concern; defines covered persons; and creates processes for the Department to issue general and specific licenses, to issue advisory opinions, and to designate entities or individuals as covered persons. The proposed rule also establishes a compliance and enforcement regime.

The Department relied upon unclassified and classified sources to support the proposed rule. Although the unclassified record fully and independently supports the proposed rule without the need to rely on the classified record, the classified record provides supplemental information that lends additional support to the proposed rule. The proposed rule would be the same even without the classified record.

Some commenters offered overarching comments. A few commenters made suggestions that addressed issues unrelated to the proposed rule, such as expressing views on U.S. positions in certain international negotiations over digital trade. No change was made in

response to these comments. These comments addressed unrelated issues that are not relevant to the scope of the proposed rule and that are directed to other agencies and forums, and they generally did not suggest any specific changes to the contemplated program. To the extent that these comments intended to suggest that the Order's and proposed rule's restrictions on access to sensitive personal data are inconsistent with international commitments by the United States, the Department disagrees.

The proposed rule's prohibitions and restrictions on access to U.S. sensitive personal data and government-related data by countries of concern are consistent with access restrictions on sensitive personal data that have long been imposed in other national security contexts, including for some transactions reviewed by CFIUS and the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector ("Team Telecom").¹⁵ Those access restrictions, in turn, are consistent with or otherwise permissible under trade and other international agreements.¹⁶ For example, the World Trade Organization's ("WTO") General Agreement on Trade in Services ("GATS"), like other trade agreements to which the United States is a party, includes an essential security interests exception that states that nothing in the agreement shall be construed to prevent a party to such an agreement from taking any action that it considers necessary for the protection of its essential security interests. As a result, rather than prohibiting such access restrictions, GATS and other relevant international agreements to which the United States is a party explicitly authorize national security-based restrictions on data access and data flows through the longstanding essential security exception. The proposed rule, like conditions restricting access in CFIUS or Team Telecom mitigation

¹⁵ See Foreign Investment Risk Review Modernization Act of 2018, *supra* note 11 (CFIUS); E.O. 13913, 85 FR 19643 (Apr. 4, 2020) (Team Telecom); *see, e.g.*, FCC, New Pacific Light Cable Network GU Holdings-Google National Security Agreement 20-044 Enclosure 1 (Dec. 16, 2021), https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.htm?f_key=448225&f_number=SCLLIC2020082700038 [<https://perma.cc/PD5E-BYWS>].

¹⁶ *See, e.g.*, Agreement on Trade-Related Aspects of Intellectual Property Rights art. 73, Apr. 15, 1994, amended Jan. 23, 2017, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, https://www.wto.org/english/docs_e/legal_e/31bis_trips_09_e.htm [<https://perma.cc/FSP4-BBZQ>]; General Agreement on Tariffs and Trade art. XXI, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194, https://www.wto.org/english/docs_e/legal_e/31bis_trips_e.pdf [<https://perma.cc/LE7M-ZM4F>].

agreements to address identified national security risks, is necessary to protect the essential security interests of the United States and is thus consistent with such international agreements to which the United States is a party.¹⁷ Notably, consistent with the United States Government's long-standing support of cross-border data flows, the proposed rule does not require data localization or wholly restrict data flows to any specific country. Rather, the proposed rule only limits data transfers in narrow, specifically defined circumstances necessary to safeguard security interests, and it is being developed through a process that enables stakeholder consultation and input. The proposed rule is also consistent with the United States' long-standing support for Data Free Flows Trust ("DFFT"). The categories of prohibited and restricted transactions in the proposed rule identify circumstances that present an unacceptable national security risk of enabling countries of concern to access and exploit Americans' sensitive personal data—circumstances that lack the trust required for free data flows.

Several commenters suggested various revisions to borrow or incorporate aspects of international or State privacy laws into this proposed rule. The Department generally declines to adopt these suggestions, except on a discrete issue discussed in part IV.A.7 of this preamble. The Department supports privacy measures and national security measures as complementary protections for Americans' sensitive personal data. Despite some overlap, privacy protections and national security measures generally focus on different challenges associated with sensitive personal data. General privacy protections focus on addressing individual rights and preventing individual harm, such as protecting the rights of individuals to control the use of their own data and reducing the potential harm to individuals by minimizing the collection of data on the front end and limiting the permissible uses of that data on the back end. National security measures, by contrast, focus on collective risks and externalities that may result from how

individuals and businesses choose to sell and use their data, including in lawful and legitimate ways.

For example, some commenters suggested adding a new exemption for transactions in which a U.S. individual consents to the sale or disclosure of their data to a country of concern or covered person. The proposed rule declines to adopt this exemption. Such a consent-based exemption would leave unaddressed the threat to national security by allowing U.S. individuals and companies to choose to share government-related data or Americans' bulk U.S. sensitive personal data with countries of concern or covered persons. It is precisely those choices that, in aggregate, help create the national security risk of access by countries of concern or covered persons, and the purpose of the Order and the proposed rule is to address the negative externality that is created by individuals' and companies' choices in the market in the first place. It would also be inconsistent with other national security regulations to leave it up to market choices to decide whether to give American technology, capital, or data to a country of concern or covered person. Export controls do not allow U.S. companies to determine whether their sensitive technology can be sent to a foreign adversary, and sanctions do not allow U.S. persons to determine whether their capital and material support can be given to terrorists and other malicious actors. Likewise, the proposed rule would not allow U.S. individuals to determine whether to give countries of concern or covered persons access to their sensitive personal data or government-related data. One of the reasons that the public is not in a position to assess and make decisions about the national security interests of the United States is that the public typically does not have all of the information available to make a fully informed decision about the national security interests of the United States.

Each subpart of the proposed rule, including any relevant comments received on the corresponding part of the ANPRM, is discussed below in the remaining sections of this preamble.

A. Subpart C—Prohibited Transactions and Related Activities

The proposed rule identifies transactions that are categorically prohibited unless the proposed rule otherwise authorizes them pursuant to an exemption or a general or specific license or, for the categories of restricted transactions, in compliance with security requirements and other

requirements set forth in the proposed rule.

1. Section 202.210—Covered Data Transactions

The Order authorizes the Attorney General to issue regulations that prohibit or otherwise restrict U.S. persons from engaging in a transaction where, among other things, the Attorney General has determined that a transaction “is a member of a class of transactions . . . [that] pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk sensitive personal data or United States Government-related data in a manner that contributes to the national emergency declared in this [O]rder.”¹⁸ Pursuant to the Order, the proposed rule categorically prohibits or, for the categories of restricted transactions, imposes security and other requirements on certain covered data transactions with U.S. persons and countries of concern or covered persons because the covered data transactions may otherwise enable countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data to harm U.S. national security.

The proposed rule defines a “covered data transaction” as any transaction that involves any access to any government-related data or bulk U.S. sensitive personal data and that involves: (1) data brokerage, (2) a vendor agreement, (3) an employment agreement, or (4) an investment agreement. *See* § 202.210. The Department has determined that these categories of covered data transactions pose an unacceptable risk to U.S. national security because they may enable countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data to engage in malicious cyber-enabled activities, track and build profiles on United States individuals for illicit purposes, including blackmail or espionage, and to intimidate, curb political dissent or political opposition, or otherwise limit civil liberties of U.S. persons opposed to countries of concern, among other harms to U.S. national security. For instance, one study has demonstrated that foreign malign actors can purchase bulk quantities of sensitive personal data about U.S. military personnel from data brokers “for coercion, reputational damage, and blackmail.”¹⁹ Countries of

¹⁷ See Press Release, Off. of the U.S. Trade Representative, *Statements by the United States at the Meeting of the WTO Dispute Settlement Body* (Jan. 27, 2023), <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/january/statements-united-states-meeting-wto-dispute-settlement-body> [<https://perma.cc/CQG5-9AZ5>] (emphasizing the United States' commitment to protect its essential security interests in the context of World Trade Organization disputes); General Agreement on Tariffs and Trade art. XXI, *supra* note 16.

¹⁸ 89 FR 15423.

¹⁹ Justin Sherman et al., *supra* note 6, at 14.

concern or covered persons could also exploit vendor, employment, or investment agreements to obtain access to government-related data or bulk U.S. sensitive personal data to harm U.S. national security.²⁰

In response to the ANPRM, commenters asked that the Department clarify when a transaction “involves” government-related data or bulk U.S. sensitive personal data. The Department has responded to those comments by revising the definition of a “covered data transaction” to any transaction that involves any access to the data by the counterparty to a transaction (rather than any transaction that involves government-related data or bulk U.S. sensitive personal data).

2. Section 202.301—Prohibited Data-Brokerage Transactions

The proposed rule prohibits any U.S. person from knowingly engaging in a covered data transaction involving data brokerage with a country of concern or a covered person. The proposed rule defines “data brokerage” as the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person (“the provider”) to any other person (“the recipient”), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. *See* § 202.214.

Because the data brokerage prohibition, along with the other prohibitions and restrictions, center around data transactions involving access to government-related data or bulk U.S. sensitive personal data, the Department addresses each of those key terms and related terms in detail in the following discussion.

3. Section 202.201—Access

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines “access” as logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology

systems, cloud-computing platforms, networks, security systems, equipment, or software.

One commenter suggested that the Department remove the term “divert” from the definition of “access” to avoid unintentionally capturing activities that do not involve actual access to data and that, according to the commenter, do not pose a risk to national security. The Department declines to do so. The definition of “access” is intentionally broad. It includes the term “divert” to ensure that the proposed rule covers data transactions that would enable a covered person to divert government-related data or bulk U.S. sensitive personal data from an intended recipient to a country of concern or a covered person, either for their own use or for the use of countries of concern or other covered persons, and to prevent countries of concern or covered persons from amassing data (including anonymized, encrypted, aggregated, or pseudonymized data), as discussed in part IV.A.13 of this preamble.

4. Section 202.249—Sensitive Personal Data

As previewed in the ANPRM, the proposed rule builds on the Order by further defining the six categories of “sensitive personal data” that could be exploited by a country of concern to harm U.S. national security if that data is linked or linkable to any identifiable U.S. individual or to a discrete and identifiable group of U.S. persons. These six categories are: (1) covered personal identifiers; (2) precise geolocation data; (3) biometric identifiers; (4) human genomic data; (5) personal health data; and (6) personal financial data. The proposed rule also categorically excludes certain categories of data from the definition of the term “sensitive personal data.” These exclusions include public or nonpublic data that does not relate to an individual, including trade secrets and proprietary information, and data that is, at the time of the transaction, lawfully publicly available from government records or widely distributed media, personal communications as defined in § 202.239, and information or informational materials as defined in § 202.226. Nothing in the proposed rule shall be construed to affect the obligations of U.S. Government departments and agencies under the Foundations for Evidence-Based Policymaking Act of 2018, Public Law 115–435 (2019), 44 U.S.C. 3501 *et seq.*

5. Section 202.212—Covered Personal Identifiers

The Order defines “covered personal identifiers” as “specifically listed classes of personally identifiable data that are reasonably linked to an individual, and that—whether in combination with each other, with other sensitive personal data, or with other data that is disclosed by a transacting party pursuant to the transaction and that makes the personally identifiable data exploitable by a country of concern—could be used to identify an individual from a data set or link data across multiple data sets to an individual,” subject to certain exclusions.²¹ The ANPRM thus contemplated three subcategories of covered personal identifiers: (1) listed identifiers in combination with any other listed identifier; (2) listed identifiers in combination with other sensitive personal data; and (3) listed identifiers in combination with other data that are disclosed by a transacting party pursuant to the transaction that makes the listed identifier exploitable by a country of concern, if they could be used to identify an individual from a dataset or to link data across multiple datasets to an individual.²² The ANPRM also contemplated two exceptions: (1) demographic or contact data that is linked only to other demographic or contact data; and (2) a network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifiers, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar services. The proposed rule expands the approach described in the ANPRM by making the exceptions applicable to all subcategories of covered personal identifiers, instead of being applicable only to listed identifiers in combination with any other listed identifiers. The listed identifiers are described in more detail in the next section.

With respect to the first subcategory, listed identifiers in combination with any other listed identifier: The ANPRM contemplated a list-based approach that would identify a comprehensive list of eight classes of data determined by the Attorney General to be reasonably linked to an individual under the Order’s definition of “covered personal identifiers.”²³

With respect to the second subcategory, listed identifiers in combination with other sensitive

²⁰ *See, e.g.*, Dep’t of Commerce, Final Determination: Case No. ICTS–20121–002, Kaspersky Lab, Inc., 89 FR 52434, 52436 (June 24, 2024), <https://www.govinfo.gov/content/pkg/FR-2024-06-24/pdf/2024-13532.pdf> [<https://perma.cc/LAS7-S7HF>] (describing how Kaspersky employees gained access to sensitive U.S. person data through their provision of anti-virus and cybersecurity software); *see generally* OFAC, U.S. Dep’t of Treas., *Guidance on the Democratic People’s Republic of Korea Information Technology Workers* (May 16, 2022), <https://ofac.treasury.gov/media/923131/download?inline> [<https://perma.cc/8DTV-Q34S>]; E.O. 14083, 87 FR 57369, 57373 (Sept. 15, 2022).

²¹ E.O. 14117, 89 FR 15421, 15428 (Feb 28, 2024).

²² 89 FR 15784–85.

²³ *Id.*

personal data: The ANPRM contemplated treating these combinations as combined data subject to the lowest bulk threshold applicable to the categories of data present.²⁴ The proposed rule generally adopts the approach described in the ANPRM, but instead of addressing this category in the definition of “listed identifiers,” the proposed rule incorporates this category as part of the definition of “bulk.”

With respect to the third subcategory, listed identifiers in combination with other data that are disclosed by a transacting party pursuant to the transaction that makes the listed identifier exploitable by a country of concern: The ANPRM indicated that the Department did not intend to impose an obligation on transacting parties to independently determine whether particular combinations of data would be “exploitable by a country of concern.”²⁵ The ANPRM provided several examples intended to be within the scope of this subcategory and several examples intended to be outside the scope of this subcategory and sought comment on ways in which this subcategory could be further defined.²⁶ In response, multiple commenters suggested anchoring this subcategory to the reasonable foreseeability that the other data could be used to link the listed identifier to a U.S. individual. As these commenters explained, without the connection to foreseeability, nearly any public data could become covered personal identifiers, because it is possible that the transacting party receiving the data could find some way of linking any public data point to an individual using the listed identifier.

The proposed rule largely adopts this suggestion. Rather than requiring companies to determine when linkage is reasonably foreseeable on a case-by-case basis, the proposed rule would define a category of data for which the Department believes it is reasonably foreseeable that the other data could be used to link the listed identifier to a U.S. individual: other data that makes the listed identifier linked or linkable to other listed identifiers or to other sensitive personal data. The proposed rule thus narrows the third subcategory to any listed identifier in combination with other data that is disclosed by a transacting party such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data. See § 202.212(a)(2). The proposed rule also incorporates the examples described in the ANPRM and

additional examples to illustrate how this subcategory would and would not apply.

6. Section 202.234—Listed Identifier

Adopting the approach contemplated in the ANPRM,²⁷ the proposed rule defines a “listed identifier” as any piece of data in any of the following data fields: (1) full or truncated government identification or account number (such as a Social Security Number, driver’s license or State identification number, passport number, or Alien Registration Number); (2) full financial account numbers or personal identification numbers associated with a financial institution or financial-services company; (3) device-based or hardware-based identifier (such as International Mobile Equipment Identity (“IMEI”), Media Access Control (“MAC”) address, or Subscriber Identity Module (“SIM”) card number); (4) demographic or contact data (such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers); (5) advertising identifier (such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising ID (“MAID”)); (6) account-authentication data (such as account username, account password, or an answer to a security question); (7) network-based identifier (such as internet Protocol (“IP”) address or cookie data); or (8) call-detail data (such as Customer Proprietary Network Information (“CPNI”). See § 202.234.

Under this definition, the term “covered personal identifiers” refers to a much narrower set of material than that covered by certain laws and policies aimed generally at protecting personal privacy.²⁸ It encompasses only the types of data and combinations thereof that are expressly listed. For example, the proposed rule’s definition of “covered personal identifiers” would not include an individual’s employment history, educational history, organizational memberships, criminal history, or web-browsing history. Some commenters suggested that the Department adopt a broader definition that aligns with the definition of

“personally identifiable information” used in State or European Union (“EU”) privacy laws to ease the burden of compliance. The Department declines to adopt this approach, and the proposed rule retains the definition stated in the ANPRM without change. Although it may be true that “personally identifiable information” is a familiar term in laws and guidance addressing the privacy and security of data held by the private sector and government, it is such a broad term that adopting a definition akin to it would significantly expand the scope of the regulations and therefore require that the Department regulate more commercial transactions or relationships than seem necessary, at least at this time, to mitigate the highest priority national security risks articulated in the Order. Furthermore, the commenters supplied no data to suggest that any cost savings realized from adopting an existing definition would outweigh the added burdens of regulating a larger swath of transactions.

Similarly, another commenter suggested broadening the definition of “covered personal identifiers” to add categories of data from State and EU privacy laws, such as web-browsing data and data that identifies or could lead to inferences about membership in protected classes such as race, religion, and national origin. The proposed rule makes no change in response to this comment. As previewed in the ANPRM, the proposed rule’s definition of “covered personal identifiers” is tailored to address the national security risks identified in the Order, and the Department is establishing the program by issuing proposed rulemakings in tranches based on priority. Also, the Department intends to regularly monitor the effectiveness and impact of the regulations once they become effective. Absent more specific information from commenters on this topic about the cross-border use of these additional kinds of identifiers by foreign governments in ways that could harm Americans, the proposed rule retains the definition stated in the ANPRM without change at this time.

One commenter suggested that the Department remove basic contact information from the listed identifiers. The proposed rule maintains the approach in the ANPRM without change.²⁹ The Order already contains an exception to the definition of “covered personal identifiers” for demographic or contact data that is linked only to other demographic or contact data. The proposed rule implements the exception articulated in the Order and previewed

²⁷ *Id.* at 15784.

²⁸ *C.f.*, e.g., California Consumer Privacy Act of 2018, Cal. Civ. Code sec. 1798.140(v)(1) (West 2024) (defining “personal information” in the context of a generalized privacy-focused regime); Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, art. 4(1) (defining “personal data” in the context of a generalized data privacy regime).

²⁴ *Id.* at 15785.

²⁵ *Id.*

²⁶ *Id.*

²⁹ 89 FR 15784.

in the ANPRM, which excludes such data from the definition of “covered personal identifiers.”³⁰

By contrast, another commenter recommended that “covered personal identifiers” be expanded to include demographic or contact data that is linked only to other demographic or contact data, because most Americans believe that information to be deserving of privacy protections. The Department declines to adopt this addition to the definition of “covered personal identifiers.” Such an expansion of the definition would be contrary to the Order, which specifically exempts this kind of data from its scope.³¹ Additionally, as the commenter acknowledges, a significant amount of this information is already publicly available to countries of concern, and therefore country of concern access to this type of information does not carry the same national security risk as access to the other covered personal identifiers identified in these regulations, even if it may raise separate privacy considerations.

A few commenters advocated removing truncated government identification and account numbers from the definition of “listed identifiers,” given their widescale use. One commenter supported the inclusion of these truncated identifiers because they are regularly used to identify individuals. The proposed rule continues to include these truncated identifiers as contemplated in the ANPRM because, as one commenter points out, they could be, and are, “used to identify an individual from a data set or link data across multiple data sets to an individual[.]” They therefore fall within the Order’s definition of “covered personal identifiers” when they are combined with certain other categories of data. Although these truncated numbers may be used widely, the proposed rule would not regulate how they are used in most transactions. Specifically, it would not regulate how these truncated numbers are used domestically, a company’s internal use of that data (other than with respect to covered persons who are employees), or transactions abroad involving third countries (other than with respect to certain conditions for the data brokerage to address onward sale).

The proposed rule also contains a non-substantive change in language designed to be more technically accurate and to clarify that any piece of data in any of the listed classes of data constitutes a listed identifier. See

§ 202.234. This change remains consistent with the examples previewed in the ANPRM and in the proposed rule showing that multiple pieces of data (such as account username and account password) in the same data field (account-authentication data) each count as separate listed identifiers.³²

7. Section 202.242—Precise Geolocation Data

The proposed rule defines “precise geolocation data” as data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within 1,000 meters. Examples of “precise geolocation data” include GPS coordinates and IP address geolocation. To help develop this definition, the Department examined the settings available to software developers in Android and iOS, the two most popular mobile device operating systems, for the precision of geolocation readings. Available options included accuracy to within 10 meters, 100 meters, 1,000 meters, 3,000 meters, and 10,000+ meters.³³ The Department selected 1,000 meters as the option that most carefully balanced the risk that countries of concern or covered persons could exploit U.S. persons’ precise geolocation data and current technology practices and standards. The Department also considered State privacy laws, with which companies are already familiar and which provide examples of the level of precision at which a device’s location warrants protection.³⁴

A few commenters suggested that the Department define “precise geolocation data” as that term is defined in the California Privacy Rights Act, which includes a geographic radius of 1,850 feet (approximately 563 meters). The Department did not accept this suggestion because our assessment of the relevant national security interests required a broader geographic area, in part due to the types of United States Government personnel and locations (such as military bases with large surrounding footprints) that are relevant to national security. By contrast, the California standard does not take these national security interests relating to

Government personnel into account. One commenter suggested that the Department omit the phrase “based on electronic signals or inertial sensing units,” which was included in the ANPRM definition of “precise geolocation data,” to make the term more technology-neutral as to the method of collection.³⁵ The Department has adopted this suggestion and deleted that phrase from the proposed definition.

8. Section 202.204—Biometric Identifiers

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines “biometric identifiers” as measurable physical characteristics or behaviors used to recognize or verify the identity of an individual, including facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints, gait, and keyboard usage patterns that are enrolled in a biometric system and the templates created by the system.

9. Section 202.224—Human Genomic Data

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines “human genomic data” as data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a human cell, including the result or results of an individual’s “genetic test” (as defined in 42 U.S.C. 300gg–91(d)(17)) and any related human genetic sequencing data. The term “human genomic data” does not include non-human data, such as pathogen genetic sequence data, that is derived from or integrated into human genomic data.

10. Other Human ‘Omic Data

The Department of Justice is considering regulating, as prohibited or restricted transactions in the final rule, certain transactions in which a U.S. person provides a country of concern (or covered person) with access to bulk human ‘omic data, other than human genomic data, as defined in § 202.224. At a high level, the ‘omics sciences examine biological processes that contribute to the form and function of cells and tissues.³⁶ The categories of ‘omic data that the Department is considering regulating could include

³² 89 FR 15785.

³³ *CLLocationAccuracy*, Apple Developer, <https://developer.apple.com/documentation/corelocation/cllocationaccuracy> [<https://perma.cc/AZ48-VSCP>]; *Change Location Settings*, Android Developer, <https://developer.android.com/develop/sensors-and-location/location/change-location-settings> [<https://perma.cc/5BY3-P7L3>].

³⁴ See, e.g., Cal. Civ. Code sec. 1798.140(w) (which uses a radius of 1,850 feet); Utah Consumer Privacy Act, Utah Code Ann. sec. 13–61–101(33)(a) (West 2024) (which uses a radius of 1,750 feet).

³⁵ 89 FR 15785.

³⁶ See, e.g., *Evolution of Translational Omics: Lessons Learned and the Path Forward* 23, 33 (Christine M. Mische et al., eds., 2012), https://www.ncbi.nlm.nih.gov/books/NBK202168/pdf/Bookshelf_NBK202168.pdf [<https://perma.cc/Q5YE-7XLM>].

³⁰ *Id.*

³¹ 89 FR 15428.

human epigenomic data, glycomic data, lipidomic data, metabolomic data, meta-multiomic data, microbiomic data, phenomic data, proteomic data, and transcriptomic data. The Department does not intend the definition of meta-multiomic data to include nonhuman data separated from human data or for the definition of microbiomics data to include data related to individual pathogens, even when derived from human sources. The Department is considering whether to include the following definitions of these terms in the final rule:

1. Epigenomic data: data derived from the analysis of human epigenetic modifications, which are changes in gene expression or cellular phenotype that do not involve alterations to the DNA sequence itself. These epigenetic modifications include modifications such as DNA methylation, histone modifications, and non-coding RNA regulation.

2. Glycomic data: data derived from the analysis of the structure, function, and interactions of glycans (complex carbohydrates) within human biological systems. The field of glycomics generally aims to understand the roles of glycans in cell-cell communication, immune responses, and various diseases.

3. Lipidomic data: data derived from a systems-level characterization of lipids from a human or human cell, including their identification, quantification, and characterization in biological systems. Routine clinical measurements of lipids for individualized patient care purposes would not be considered lipidomic data because such measurements would not entail a systems-level analysis of the complete set of lipids found in such a sample.

4. Metabolomic data: data derived from the analysis of metabolites, the small molecules produced during metabolism, that aim to understand disease mechanisms, identify biomarkers for diagnosis, and develop targeted treatments by revealing the dynamic biochemical activities in a living system. This data provides a general snapshot of an organism, tissue, or cell, offering insights into physiological and pathological processes.

5. Meta-multiomic data: The Department is considering the following options for defining meta-multiomic data:

(i) Datasets that include two or more categories of human 'omic data identified in this regulation, which can include data derived from the human

genome, proteome, transcriptome, epigenome, or metabolome; or

(ii) Datasets that include two or more categories of human 'omic data identified in this regulation and that include 'omic data from another species.

6. Microbiomic data: data derived from analysis of all the microorganisms of a given community within the human body (including a particular site on the human body). Microbiomic data is implicated in the field of metagenomics, which generally aims to investigate and understand genetic material of entire communities of organisms, including the composition of a microbial community.

7. Phenomic data: data derived from analysis of human phenotypes, including physical traits, physiological parameters, and behavioral characteristics.

8. Proteomic data: data derived from analysis of human proteomes, which refers to the entire set of proteins expressed by a human genome, cell, tissue, or organism. The field of proteomics generally aims to identify and characterize proteins and study their structures, functions, interactions, and post-translational modifications.

9. Transcriptomic data: data derived from analysis of a human transcriptome, which is the complete set of RNA transcripts produced by the human genome under specific conditions or in a specific cell type. The field of transcriptomics generally aims to understand gene expression patterns, alternative splicing, and regulation of RNA molecules.

The Department is considering excluding from the definition of other human 'omic data pathogen-specific data embedded in 'omic data sets.

The Department welcomes input from commenters regarding the potential risks and benefits that may arise from restricting or prohibiting covered data transactions with a country of concern or covered person involving some or all of these categories of other human 'omic data. The Department is particularly interested in comments addressing the health, economic, or scientific impacts of regulating such data transactions, as well as any national security implications. Specifically:

- In what ways, if any, should the Department of Justice elaborate or amend the definitions of these classes of other human 'omic data? If the definitions should be elaborated or amended, why?

- Should bulk data transactions involving these types of other human 'omic data be regulated? If so, which types of human 'omic data—including any not listed—should be regulated,

why should they be regulated, and how should they be regulated? Additionally, what bulk thresholds should apply and why?

- To what extent would the regulation of bulk data transactions involving these types of other human 'omic data affect individuals' rights to share their own biological samples (*e.g.*, blood, urine, tissue, etc.) or health, 'omic, and other data?

- What would be the effects of prohibiting or restricting transactions involving these data classes in the final rule, particularly with respect to:

- health outcomes
- health supply chain impacts
- research and administrative costs
- economic costs due to (1) imposing these regulations, or (2) allowing unregulated bulk access to human 'omic data

- What additional risks should be considered if these bulk data transactions are not regulated, specifically as they relate to:

- risks stemming from exploitable health information

- manipulation of bulk data for strategic advantage over the United States

- use of bulk datasets for the creation and refinement of AI or other similar advanced technologies

11. Section 202.240—Personal Financial Data

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines "personal financial data" as data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data, including assets liabilities, debts, and transactions in a bank, credit, or other financial statement; or data in a credit report or in a "consumer report" (as defined in 15 U.S.C. 1681a(d)).

One commenter sought clarification that personal financial data does not include inferences based on that data, suggesting, for example, that hotel record transactions may be personal financial data but an ultimate inference that the person is interested in business travel should not be considered personal financial data. As set forth in the Order and previewed in the ANPRM, the proposed rule would prohibit or restrict only certain categories of transactions in government-related data or bulk U.S. sensitive personal data, neither of which include inferences on their own.³⁷

³⁷ 89 FR 15783; 89 FR 15428–29.

12. Section 202.241—Personal Health Data

The ANPRM contemplated defining “personal health data” as “individually identifiable health information,” as defined under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), “regardless of whether such information is collected by a ‘covered entity’ or ‘business associate.’”³⁸

Several commenters supported defining personal health data as “individually identifiable health information.” That definition is similar to how those terms are defined in HIPAA and its implementing regulations. However, one commenter expressed confusion as to how cross-referencing that definition in this program would relate to “covered entities” or “business associates” under HIPAA. The proposed rule adopts much of the substance of the approach in the ANPRM while providing greater clarity to address this confusion. Instead of defining “personal health information” by cross referencing and incorporating HIPAA, the proposed rule reproduces the relevant substance of the HIPAA definition to provide greater clarity that the definition does not turn on the HIPAA-specific inquiry of whether data is handled by covered entities or business associates. Further, unlike the HIPAA definition, the proposed rule would not define health information in terms of whether the information identifies individuals, because the proposed rule applies regardless of whether data is de-identified.

As a result, the proposed rule defines “personal health data” as health information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. The term includes basic physical measurements and health attributes (such as bodily functions, height and weight, vital signs, symptoms, and allergies); social, psychological, behavioral, and medical diagnostic, intervention, and treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications. The proposed rule would operate on a categorical basis and would determine that the category of personal health data generally meets the requirements of being “exploitable by a country of

concern to harm United States national security” and “is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals” under section 7(l) of the Order. To be sure, it is possible to hypothesize a limited data set of discrete information related to an individual’s physical or mental health condition that is not inherently linked or linkable to U.S. individuals (such as a data set of only heights or weights with no identifying information). But based on the information currently available, it does not appear that such limited datasets accurately reflect how personal health data is stored, transmitted, and used in the real world, and thus it does not appear appropriate to adjust the proposed rule to account for this hypothetical at this time. The Department welcomes comments on the extent to which such datasets exist and are the subject of covered data transactions between U.S. persons and countries of concern or covered persons.

13. Section 202.206—Bulk U.S. Sensitive Personal Data

Adopting the approach contemplated in the ANPRM without change, the prohibitions and restrictions apply to “bulk U.S. sensitive personal data,” which the proposed rule defines as a collection or set of sensitive personal data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted. The bulk thresholds of data set by the proposed rule are addressed in detail in part V of this preamble.

Several commenters requested that the Department align the categories of sensitive personal data with State data privacy laws, particularly to exclude encrypted, pseudonymized, de-identified, or aggregated data from the proposed rule’s coverage. In contrast, other commenters supported the Department’s treatment of pseudonymized, de-identified, or encrypted data, including to prevent the data from being re-identified in the future and to recognize that not all techniques for pseudonymization, de-identification, encryption, or aggregation are equally effective. The Department declines to adjust the proposed rule to exclude anonymized, encrypted, pseudonymized, or de-identified data, and the proposed rule adopts the approach described in the ANPRM without change. As the Order emphasizes, even where types of sensitive personal data are “anonymized, pseudonymized, or de-identified, advances in technology,

combined with access by countries of concern to large datasets, increasingly enable countries of concern that access this data to re-identify or de-anonymize data,” which could reveal exploitable sensitive personal information on U.S. persons.³⁹ As the Department has recently explained, “[o]pen-source reporting has repeatedly raised concern[s] that supposedly anonymized data is rarely, if ever, truly anonymous.”⁴⁰ As a recent study has explained, for example, “[a]ggregated insights from location data” could be used to damage national security.⁴¹ Examples abound. Researchers in 2024 used a little more than a year’s worth of “raw, ‘ping’-level data, a year’s worth of location data from de-identified smartphones in 26 major metropolitan areas encompassing nearly every SEC office and most public firm headquarters to identify non-public investigations and enforcement actions, and glean insights about how those visits affected financial markets.”⁴² In 2018, the publication of a global heatmap of anonymized users’ location data collected by a popular fitness app enabled researchers to quickly identify and map the locations of military and government facilities and activities.⁴³ Similarly, in 2019, *New York Times* writers were able to combine a single set of bulk location data collected from cell phones and bought and sold by location-data companies—which was anonymized and represented “just one slice of data, sourced from one company, focused on one city, covering less than one year”—with publicly available information to identify, track, and follow “military officials with security clearances as they drove home at night,” “law enforcement officers as they took their kids to school,” and “lawyers (and their guests) as they

³⁹ 89 FR 15426; see also E.O. 14083, 87 FR 57369, 57372–73 (Sept. 15, 2022).

⁴⁰ *In Camera*, Ex Parte Classified Decl. of David Newman, Principal Deputy Assistant Att’y Gen., Nat’l Sec. Div., U.S. Dep’t of Just., Doc. No. 2066897 at Gov’t App. 74–75 ¶¶ 100–01, *TikTok Inc. v. Garland*, Case Nos. 24–1113, 24–1130, 24–1183 (D.C. Cir. July 26, 2024) (publicly filed redacted version) (hereinafter “Newman Decl.”).

⁴¹ Sherman et al., *supra* note 6, at 15.

⁴² William C. Gerken et al., *Watching the Watchdogs: Tracking SEC Inquiries using Geolocation Data 2–4* (Aug. 30, 2024) (unpublished manuscript), <https://ssrn.com/abstract=4941708> [<https://perma.cc/L7L9-WU3T>].

⁴³ E.g., Richard Perez-Pena & Matthew Rosenberg, *Strava Fitness App Can Reveal Military Sites, Analysts Say*, N.Y. Times (Jan. 29, 2018), <https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html> [<https://perma.cc/FT3A-W547>]; Jeremy Hsu, *The Strava Heat Map and the End of Secrets*, Wired (Jan. 29, 2018), <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/> [<https://perma.cc/6TWD-P76B>].

³⁸ *Id.*; see 42 U.S.C. 1320d(6); 45 CFR 160, 103.

traveled from private jets to vacation properties.”⁴⁴ A 2019 research study concluded that “99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes,” thus “suggest[ing] that even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by [the EU’s General Data Protection Regime] and seriously challenge the technical and legal adequacy of the de-identification release-and-forget model.”⁴⁵ Other studies and reports have reported similar results.⁴⁶ As a result, as the Department recently explained, “[a]dversaries can use these datasets to reverse-engineer anonymized data and identify people, subjects, or devices that were supposedly anonymized.”⁴⁷

Similar concerns exist with respect to encrypted data. Countries of concern amass large quantities of encrypted data including by harvesting encrypted data now in order to decrypt it in the future should advances in quantum technologies render current standard public-key cryptographic algorithms ineffective.⁴⁸ Encryption keys can also

be stolen, handed over under compulsion, and otherwise obtained for use in decrypting datasets.⁴⁹

A few commenters suggested that the approach contemplated in the ANPRM would weaken national security by failing to differentiate between data that is encrypted or otherwise protected and data that is not. In their view, encryption is an important tool to secure data from unauthorized access, and treating encrypted and non-encrypted data alike could discourage the use of encryption, weakening the overall security of data. Other commenters, however, supported treating pseudonymized, encrypted, de-identified, and aggregated data as sensitive personal data because of the ability to re-identify such data and the rapid advancements in re-identification techniques. The Department declines to modify the proposed rule in response to these comments. As contemplated in the ANPRM, the proposed rule explicitly recognizes and relies upon the privacy and national security-preserving value of high quality, effective methods of encryption, de-identification, pseudonymization, and aggregation by specifically authorizing certain otherwise prohibited transactions so long as they meet the security requirements described in part IV.B.1 of this preamble, including by using data-level control(s) such as these techniques in combination with other security requirements. At the same time, as contemplated in the ANPRM, the proposed rule also recognizes that ineffective methods of encryption, de-identification, pseudonymization, and aggregation present the same unacceptable national security risk of access by countries of concern and covered persons as the risks posed by such access to identifiable data that is not secured through any of these techniques. The proposed rule thus allows otherwise prohibited employment agreements, vendor agreements, and investment agreements

only if they use any combination of the data-level requirements necessary to prevent access to covered data by covered persons or countries of concern, as requirements laid out in the security requirements to be published by the Department of Homeland Security (“DHS”), in addition to organizational- and system-level requirements.

Commenters also requested that the Department use existing State privacy law definitions to define the categories of sensitive personal data, such as personal financial data. Commenters stated that many companies already know how to comply with State privacy laws. The Department has considered these comments. However, as discussed in part IV.A.6 of this preamble, the cited definitions do not necessarily align with the specific national security goals of these regulations. Therefore, the proposed rule adopts the approach described in the ANPRM without change and does not adopt the State privacy law definitions of the terms in the proposed rule.

14. Section 202.205—Bulk

As previewed in the ANPRM, the proposed rule’s prohibitions apply to bulk amounts of U.S. sensitive personal data (in addition to the separate category of government-related data). The proposed rule defines “bulk” as any amount of such data that meets or exceeds thresholds during a given 12-month period, whether through one covered data transaction or multiple covered data transactions involving the same U.S. person and the same foreign person or covered person. The proposed rule sets specific thresholds for each category of sensitive personal data. See § 202.205. Certain specified data transactions that exceed those thresholds are “covered data transactions” and thus subject to the proposed rule’s prohibitions unless they are otherwise authorized by the proposed rule. See § 202.210. The Department has determined the proposed bulk thresholds based on the analysis previewed in the ANPRM and described in more detail in part V of this preamble.

A few commenters expressed concerns that it would be necessary to decrypt data to determine whether it meets a relevant bulk threshold and suggested discarding the bulk thresholds as a result. They noted that decrypting data is generally less secure and could lead to unauthorized access. The proposed rule makes no change in response to these comments, for several reasons. First, many businesses engaging in the categories of prohibited and restricted transactions generally use

⁴⁴ Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html> [<https://perma.cc/X3VB-429P>].

⁴⁵ Luc Rocher et al., *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models*, 10 *Nature Commc’ns*, at 1 (2019), <https://www.nature.com/articles/s41467-019-10933-3.pdf> [<https://perma.cc/SYJ7-KA95>]; see also Alex Hern, ‘Anonymised’ Data Can Never Be Totally Anonymous, Says Study, *The Guardian* (Jul. 23, 2019), <https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds> [<https://perma.cc/5BF8-745A>].

⁴⁶ See, e.g., Alex Hern, *New York Taxi Details Can Be Extracted From Anonymised Data, Researchers Say*, *The Guardian* (June 27, 2014), <https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn> [<https://perma.cc/6SYK-6ZEG>] (reporting that a researcher “discovered that the anonymous data” of taxi records “was easy to restore to its original, personally identifiable format,” taking a “matter of only minutes to determine which [license] numbers were associated with which pieces of anonymised data” and only an hour to “de-anonymise the entire dataset,” making it possible to “figure out which person drove each trip” and to determine taxi drivers’ supposedly anonymous home addresses); Ryan Singel, *Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims*, *Wired* (Dec. 17, 2009), <https://www.wired.com/2009/12/netflix-privacy-lawsuit/> [<https://perma.cc/B96P-AY97>] (reporting on researchers who de-anonymized a Netflix dataset of movie ratings by using publicly available information, which revealed “political leanings and sexual orientation” in some cases, and reporters who “quickly” de-anonymized supposedly anonymous AOL search-engine logs “to track down real people”).

⁴⁷ Newman Decl., *supra* note 40, at Gov’t App. 33 ¶ 105.

⁴⁸ David Lague, *U.S. and China Race to Shield Secrets from Quantum Computers*, *Reuters* (Dec. 14,

2023), <https://www.reuters.com/investigates/special-report/us-china-tech-quantum/> [<https://perma.cc/9HAA-46XA>]; Nat’l Counterintel. & Sec. Ctr., *Protecting Critical and Emerging U.S. Technologies From Foreign Threats 5* (Oct. 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf [<https://perma.cc/L6ZU-8HU7>]; Nat’l Cybersec. Ctr. of Excellence, *NIST SP 1800–38B, Migration to Post-Quantum Cryptography*, at 1 (draft Dec. 2023), <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf> [<https://perma.cc/FXF2-BJ62>].

⁴⁹ *Can Encrypted Data be Hacked?*, IT Foundations (Apr. 19, 2021), <https://itfoundations.com/can-encrypted-data-be-hacked/> [<https://perma.cc/E3TN-YAVV>].

the data in the course of operating their business, rather than merely serving as a pass-through for encrypted data as the comments suggest. While encrypting data in transit and data at rest is and should be a standard security technique, and encrypting data in use is increasingly common, data is routinely decrypted while it is being actively accessed, processed, filtered, sorted, searched, analyzed, displayed, and otherwise used by a business (for example, when an authorized employee or user opens and searches an encrypted file or database). However, nothing in the proposed rule imposes a legal requirement to decrypt data to comply. Instead, the proposed rule requires only that U.S. persons implement a risk-based compliance program tailored to their individual risk profiles. And data may also be encrypted using cryptographic methods that permit some computation and analysis to be performed on cyphertext that ascertains the kinds and volume of data without decrypting the data.⁵⁰ Businesses can map the kinds and volumes of their data to evaluate it against the bulk thresholds in the data life cycle in which it is either decrypted for access or encrypted in use.

Second, even beyond mapping data in use, companies choosing to engage in these categories of data transactions can and should have some awareness of the volume of data they possess and in which they are transacting. For example, typically data-using entities maintain metrics, such as user statistics, that can help estimate the number of impacted individuals for the purposes of identifying whether a particular transaction meets the bulk threshold.⁵¹ Given that the bulk thresholds are built around order-of-magnitude evaluations

of the quantity of user data, it is reasonable for entities to conduct similar order-of-magnitude-based assessments of their data stores and transactions for the purposes of regulatory compliance. Companies already must understand, categorize, and map the volumes of data they have for other regulatory requirements, such as State laws requiring notification of data breaches of specific kinds of data above certain thresholds.⁵²

Third, this concern appears premised on a scenario in which a U.S. business handles only encrypted data on which no computational functions can be performed to determine the kinds and volume of data, never accesses the decrypted data in its business, does not have other proxies or metrics to determine the kinds and volumes of data in which it is transacting, and must comply with the prohibitions and restrictions in the proposed rule. This scenario appears to be an edge case at best, and the comments do not provide a real-world example of this scenario or its frequency. Indeed, as discussed in some of the examples contained in the proposed rule, if a U.S. entity merely provides a platform for, or transports data between, a U.S. customer and a covered person or country of concern, and thus does not know or reasonably should not know of the kind or volume of data involved, then it generally would not “knowingly” engage in a prohibited transaction if the U.S. customer uses that platform or infrastructure to engage in a prohibited transaction with a covered person. Instead, the U.S. customer would generally be responsible for having “knowingly” engaged in the prohibited transaction, as illustrated in the clarification of the “knowingly” standard and the new examples incorporated into the proposed rule. See § 202.230. Similarly, if a U.S. entity merely stores encrypted data on behalf of a U.S. customer and does not possess the encryption key, and if the U.S. entity does not know or reasonably should not know the kind or volume of data involved, the U.S. entity generally would not meet the “knowingly” standard of the proposed rule.

Fourth, to the extent that there is a U.S. business that handles only encrypted data on which no computational functions can be performed to determine the kinds and volume of data, never accesses the decrypted data in its business, does not have other proxies or metrics to

determine the kinds and volumes of data it is transacting, and is subject to the prohibitions and restrictions in the proposed rule, that U.S. business would have choices under the proposed rule. It would be able to engage with the Department and seek an advisory opinion or a specific license tailored to its business. Similarly, it would have choices about how best to comply as part of its individualized, risk-based compliance program. For example, it can choose not to engage in prohibited or restricted transactions with countries of concern or covered persons as part of its individualized risk-based compliance program. If the U.S. business chooses to engage in categories of transactions potentially subject to the proposed rule, it can conduct reasonable due diligence on the source of its encrypted data (such as engaging with and obtaining contractual commitments from its customers) to determine the volume and kinds of data in which it is transacting. Or, if it chooses to engage in restricted transactions with countries of concern or covered persons, it can assume that its transactions involve bulk volumes of sensitive personal data and comply with the security requirements and other applicable conditions out of an abundance of caution.

Even if this hypothetical U.S. business were to choose to engage in categories of transactions potentially subject to the proposed rule, and it voluntarily decided to briefly decrypt the data to determine the kinds and volume of its data as part of its risk-based compliance program, commentators have not provided evidence that such a brief decryption would meaningfully increase the risks of unauthorized access relative to the risks involved in routine decryption for business use. Encryption is one security tool designed to mitigate the risk of unauthorized access to data.⁵³ Entities should use encryption as a tool whenever possible, including when data is at rest, in transit, and in use. However, using encryption does not eliminate risk or the requirement to perform appropriate due diligence. If an entity is using data at any point or has access to both encrypted data and the encryption key, that entity has full se into and control over the data on its systems for the

⁵⁰ Abbas Acar et al., *A Survey on Homomorphic Encryption Schemes: Theory and Implementation*, 51 [No. 4] ACM Computing Survs. 79:1, 79:2 (2018), <https://dl.acm.org/doi/pdf/10.1145/3214303> [<https://perma.cc/AM69-7ZWV>]. In addition, to the extent that businesses use emerging techniques (such as homomorphic encryption) that permit computations to be performed on encrypted data without first decrypting it, these techniques may enable businesses to map their data even if it remains encrypted.

⁵¹ Justin Ellingwood, *User Data Collection: Balancing Business Needs and User Privacy*, DigitalOcean (Sept. 26, 2017), <https://www.digitalocean.com/community/tutorials/user-data-collection-balancing-business-needs-and-user-privacy> [<https://perma.cc/GCX5-RGSK>]; Jodie Siganto, *Data Tagging: Best Practices, Security & Implementation Tips*, Privacy108 (Nov. 14, 2023), <https://privacy108.com.au/insights/data-tagging-for-security/> [<https://perma.cc/8PQA-89DA>]; National Institutes of Health, *Metrics for Data Repositories and Knowledgebases: Working Group Report 7*, (Sept. 15, 2021), <https://datascience.nih.gov/sites/default/files/Metrics-Report-2021-Sep15-508.pdf> [<https://perma.cc/8KBQ-HWRK>].

⁵² See, e.g., Del. Code. Ann. tit. 6, sec. 12B—100 to—104 (West 2024); N.M. Stat. Ann. sec. 57—12C—10 (LexisNexis 2024).

⁵³ *What Is Encryption?*, Cloudflare, <https://www.cloudflare.com/learning/ssl/what-is-encryption/> [<https://perma.cc/T3KT-BURX>]; Cybersec. & Infrastructure Sec. Agency, *Zero Trust Maturity Model 5*, 27 (v. 2.0 Apr. 2023), https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf [<https://perma.cc/F9LB-JVL9>].

purposes of this regulation.⁵⁴ Entities are responsible for balancing risks within their systems, with encryption serving as one available tool for achieving risk management goals alongside other tools like data governance and data minimization plans, role-based and least-privilege access controls, and identity management through multifactor authentication.⁵⁵

It is the responsibility of the regulated entity to manage risk that already exists, which includes making choices about the best way to manage its own particular risk and tradeoffs between various data risk management strategies, including technical measures like encryption, organizational policies, and access management. Other options include altering commercial activities to minimize the size and scope of covered data transactions and utilizing a strong data governance regime to minimize the type and quantity of data collected. If data cannot remain encrypted while in use, the risk of temporarily decrypting data to comply with regulations can be offset by measures such as well-designed data collection, data management, and data security programs. Given these factors, any risk associated with a hypothetical U.S. business' decision to temporarily decrypt data that would otherwise remain encrypted at all times in the business' life cycle would appear to be much more remote and attenuated than the risk that accrues by allowing the U.S. business to engage in a transaction that grants a country of concern or covered person access to encrypted government-related data or bulk U.S. sensitive personal data.

15. Section 202.222—Government-Related Data

As set forth in § 202.222, the proposed rule would not impose any bulk

threshold requirements on transactions involving government-related data. The proposed rule defines subcategories of government-related data for locations and personnel, as contemplated in the ANPRM. For the location subcategory, the proposed rule defines “government-related data” as any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List in § 202.1401 that the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights to the detriment of national security about locations controlled by the Federal Government, including insights about facilities, activities, or populations in those locations, because of the nature of those locations or the personnel who work there. The purpose of this list is to prevent countries of concern from exploiting the geolocation data in these locations, such as by using aggregated geolocation data to draw inferences about facilities, activities, or populations located there that could undermine U.S. national security or foreign policy or to conduct intelligence or counterintelligence operations against government employees or contractors, or against government facilities, as discussed in parts II, IV(D) and V(A) of this preamble. As set forth in the proposed rule, the locations that the Department might add to this list may include the worksites or duty stations of Federal Government employees or contractors who occupy national security positions, as that term is defined in 5 CFR 1400.102(a), wherever they are located. The locations may also include military installations, embassies or consulates, or other facilities worldwide that support the Federal Government in achieving its national security, defense, intelligence, law enforcement, or foreign policy missions. The proposed rule thus modifies the definition contemplated in the ANPRM by setting forth more details about the types of locations that will be listed on the Government-Related Location Data List.⁵⁶

The proposed rule also proposes a format for the Government-Related Location Data List and proposes some areas for inclusion on that List. See § 202.1401. This is not yet a comprehensive list of locations. The Department anticipates that the final rule will include additional locations associated with military, other Government, or other sensitive facilities or locations that meet the criteria in the definition. These locations may include,

for example, military bases, embassies, or law enforcement facilities.

For the personnel subcategory, the proposed rule adopts the ANPRM's contemplated definition without change by defining “government-related data” as any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and intelligence community.⁵⁷

Commenters were generally supportive of the proposed rule's protections for government-related data. A few commenters requested that the proposed rule provide clarity as to what constitutes a “former senior official” and a “recent former employee.” The proposed rule defines “recent former employees or contractors” as employees or contractors who have worked for or provided services to the United States Government, in a paid or unpaid status, within the 2 years preceding a proposed covered data transaction. See § 202.245. The proposed rule defines a “former senior official” as either a “former senior employee” or “former very senior employee,” as those terms are defined in the ethics regulations pertaining to post-employment conflicts of interest for former Executive Branch or independent agency employees. 5 CFR 2641.104. See § 202.220.

One commenter expressed concern that, with respect to the personnel subcategory, companies will have to ask individuals whether they are former government employees when collecting their data and retain that information to ensure they can comply with the regulations. The commenter argued that this could have the unintended consequence of inadvertently creating a database of sensitive information that bad actors could target. While the Department appreciates that concern and agrees that this unintended consequence should be avoided, the Department has designed the proposed rule to specifically avoid this problem by defining the personnel subcategory based on how the U.S. person markets the data, not on whether a particular dataset contains data on former government employees or contractors. In other words, the personnel subcategory applies only to transactions in which the U.S. person has already identified and described sensitive personal data as being about certain government personnel. This subcategory does not apply on the basis of the presence or absence of data linked to

⁵⁴ Clare Stouffer, *What Is Encryption? How It Works + Types of Encryption*, Norton: Blog (July 18, 2023), <https://us.norton.com/blog/privacy/what-is-encryption> [<https://perma.cc/RC3D-NS95>].

⁵⁵ Nat'l Sec. Agency & Cybersec. & Infrastructure Sec. Agency, *Recommended Best Practices for Administrators: Identity and Access Management* (n.d.), https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20identity%20and%20access%20management%20recommended%20best%20practices%20for%20administrators%20pp-23-0248_508c.pdf [<https://perma.cc/B7VP-4RWF>]; Mohammed Khan, *Data Minimization—A Practical Approach*, ISACA (Mar. 29, 2021), <https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-a-practical-approach> [<https://perma.cc/8APH-5E5A>]; Cybersec. & Infrastructure Sec. Agency, *Protecting Sensitive and Personal Information From Ransomware-Caused Data Breaches* (n.d.), https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf [<https://perma.cc/Q7TN-NLR4>].

⁵⁶ 89 FR 15787.

⁵⁷ *Id.*

certain government personnel in the underlying sensitive personal data.

One commenter suggested removing the qualifier that data had to be “marketed” as data about members of the military or intelligence community because certain data can still be “linked or linkable” to members of the military through geolocation without being explicitly marketed as such. As the Order’s second category of government-related data confirms, sensitive personal data that is linked to categories of data that could be used to identify current or certain former government personnel can present a national security risk, even if a transacting party does not market it as linked or linkable to those personnel.⁵⁸ The Department is still considering how to address this issue, specifically whether to include, and how to define, this category of information in the proposed rule while minimizing the unintended consequence described above in this section. The Department appreciates any views from the public.

16. Section 202.302—Other Prohibited Data-Brokerage Transactions Involving Potential Onward Transfer to Countries of Concern or Covered Persons

As previewed in the ANPRM, the proposed rule also includes a prohibition specific to data brokerage to address transactions involving the onward transfer or resale of government-related data or bulk U.S. sensitive personal data to countries of concern and covered persons.⁵⁹ See § 202.302. The proposed rule defines “data brokerage” as the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person (“the provider”) to any other person (“the recipient”), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. See § 202.214. The proposed rule prohibits any U.S. person from knowingly engaging in a covered data transaction involving data brokerage with any foreign person that is not a covered person unless the U.S. person contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving that data with a country of concern or covered person. This narrow circumstance is the only instance in which the proposed rule’s regulation of covered data transactions could impact transactions involving third countries (*i.e.*, U.S. persons’ covered data

transactions in which a country of concern or covered person is not a party).

Commenters generally supported the feasibility of using contractual requirements to address the resale of data as contemplated in the ANPRM. They noted, however, that it may be difficult for U.S. persons to enforce those requirements or to ensure that the data is not subsequently resold in violation of those provisions. Several aspects of the proposed rule are designed to address these concerns. First, in addition to requiring a contractual commitment from the foreign person not to engage in a subsequent covered data transaction with a country of concern or covered person, as contemplated in the ANPRM, the proposed rule adds a requirement for U.S. persons engaged in such transactions to report any known or suspected violations of the required contractual provision. This requirement creates a mechanism to provide the necessary information for the Department to investigate and take appropriate action to address any violations of the proposed rule. Second, relying on both its own investigations and its investigations of any known or suspected violations reported by private parties, the Department intends to exercise the designation authority under the proposed rule to designate as covered persons, as appropriate, foreign third parties that violate the contractual provisions required by this prohibition. See § 202.701. Third, consistent with the overall approach to compliance and enforcement under the proposed rule, the Department expects U.S. persons engaged in these kinds of data brokerage transactions to take reasonable steps to evaluate whether their foreign counterparties are complying with the contractual provision as part of implementing risk-based compliance programs under the proposed rule. Absent indications of evasion, conspiracy, or knowingly directing prohibited transactions, U.S. persons that conduct adequate due diligence as part of a risk-based compliance program would not have engaged in a prohibited transaction if the foreign counterparty later violates the required contractual provision or if the U.S. person fails to detect such violations. Depending on the circumstances, a U.S. person’s failure to conduct adequate due diligence may subject the U.S. person to enforcement actions if that failure would constitute an evasion of the regulations, such as repeatedly knowing of violations by a foreign person and continuing to engage in data-brokerage

transactions with that foreign person. The Department welcomes public input on any additional measures that should be considered as part of the final rule. In addition, after the final rule goes into effect, the Department intends to monitor the effectiveness of the measures to address the risk of onward sale and make any appropriate adjustments.

Although not specifically raised by commenters, the Department is considering the specific language used to describe the contractual requirement. As previewed in the ANPRM,⁶⁰ the proposed rule frames the contractual requirement as an obligation to provide that the foreign party “refrain from engaging in a subsequent covered data transaction involving the same data with a country of concern or covered person.” See § 202.302(a)(1). The Department invites public comment on this language, including whether any alternative language (such as inserting “knowingly” before “refrain” or “contractually requires that the foreign person use best efforts not to engage”) would be more appropriate.

Commenters expressed varying views about the contemplated definition of “data brokerage.” Several commenters expressed concerns about the breadth of the definition of “data brokerage” in the ANPRM.⁶¹ Some commenters suggested that the proposed term, and in particular the phrase “or similar commercial transactions,” creates uncertainty as to its scope and fails to distinguish between selling data for monetary purposes and transferring data pursuant to normal business operations. Some commenters urged the Department to limit the scope of the proposed rule to “data brokers” by adopting the definition used in existing State privacy laws, such as California’s.⁶² Others proposed ways that the Department should narrow the definition, including by requiring that the data be sold in exchange for monetary or other valuable consideration; that the data must be the object of the transaction and not shared incident to the development, testing, or sale of a product or service; or that the data must be knowingly transferred or sold. Other commenters suggested that the Department amend the definition of “sale” to exclude the disclosure of sensitive personal data to service providers processing data on behalf of a U.S. company, to third parties for providing products or services requested by a U.S. company, or for

⁶⁰ *Id.*

⁶¹ See 89 FR 15788.

⁶² See Cal. Civ. Code 1798.99.80 (West 2024).

⁵⁸ 89 FR 15429.

⁵⁹ 89 FR 15792.

disclosures or transfers to subsidiaries or affiliates of U.S. companies. Still other commenters supported the approach contemplated by the ANPRM for defining data brokerage by reference to transactions, not the identities of the parties, noting that the ANPRM's approach is stronger than existing State privacy laws, and encouraged the adoption of a broad definition.

The Department declines to revise the definition of "data brokerage" in response to these comments. The definition of "data brokerage" in the proposed rule is intentionally designed to address the activity of data brokerage that gives rise to the national security risk, regardless of the kind of entity that engages in it. Both first-party data brokerage (*i.e.*, by the person that directly collected the U.S. person's data) and third-party data brokerage (*i.e.*, by a person that did not directly collect the U.S. person's data, such as a subsequent reseller) present similar national security risks: the outright sale and transfer of sensitive personal data to a country of concern or covered person. For this reason, the proposed definition intentionally regulates data transactions, including transactions that transfer data to entities in countries of concern for product development, an issue raised by numerous commenters, because those transactions give rise to the risks discussed in the Order. In addition, commenters did not provide any specific evidence that the proposed definition of data brokerage would have any measurable economic impact related to product development or testing.⁶³ Consequently, the proposed rule maintains the approach described in the ANPRM without change.

A few commenters expressed concern about how this provision might affect the ability of biomedical and pharmaceutical manufacturers to share clinical trial data with drug and device regulators in countries of concern. Relatedly, a few commenters expressed concerns that the proposed rule's inclusion of aggregated and anonymized data would prohibit companies from using clinical trial data to launch clinical trials in countries of concern or sharing safety and efficacy data obtained from clinical trials in the United States with countries of concern. The proposed rule includes two exemptions responsive to these comments, in sections 202.510 and 202.511. These exemptions allow certain transactions relevant to medical research, marketing, and safety, as explained in more detail below.

17. Section 202.303—Prohibited Human Genomic Data and Human Biospecimen Transactions

As previewed in the ANPRM, the proposed rule includes a prohibition to specifically address the risks posed by covered data transactions involving access by countries of concern to U.S. persons' bulk human genomic data and human biospecimens from which that bulk data can be derived, such as covered data transactions that give access to bulk human genomic data to laboratories owned or operated by covered persons or provide them with human biospecimens from which such data can be derived. The proposed rule prohibits any U.S. person from knowingly engaging in any covered data transaction involving human genomic data that provides a country of concern or covered person with access to bulk U.S. sensitive personal data that consists of human genomic data or human biospecimens from which such data could be derived, where the number of U.S. persons in the dataset is greater than the applicable bulk threshold at any point in the preceding 12 months, whether in a single covered data transaction or aggregated across covered data transactions. This prohibition applies to any of the categories of covered data transactions that involve access to bulk human genomic data or human biospecimens from which bulk human genomic data can be derived, even when the transactions involve an employment, investment, or vendor agreement. In other words, transactions falling within the scope of proposed § 202.303 are never treated as restricted transactions under the proposed rule. Relatedly, and as discussed in more detail with respect to the categories of exempt transactions, the proposed rule exempts (1) transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof, or transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government, including those for outbreak and pandemic prevention, preparedness, and response; and (2) data transactions, including the sharing of human biospecimens from which human genomic data may be derived, that are required or authorized by certain specified international arrangements addressing global and pandemic preparedness.

One commenter sought clarification that vendor, employment, and investment agreements involving access to bulk human genomic data, or human biospecimens from which such data

could be derived, are prohibited transactions under subpart C of the proposed rule rather than restricted transactions under subpart D of the proposed rule. The commenter suggested that the proposed rule should clarify that such vendor, employment, and investment agreements are prohibited because they present the same policy concerns as other categories of transactions involving access to this kind of data. The Department agrees. As shown by Example 49 in the ANPRM, vendor, employment, and investment agreements involving access to this kind of sensitive personal data are prohibited rather than restricted.⁶⁴ For the avoidance of doubt, § 202.303 of the proposed rule clarifies that the authorization for restricted transactions, *see* §§ 202.401–202.402, does not apply to any transactions involving access to bulk human genomic data or bulk human biospecimens.

18. Section 202.304—Prohibited Evasions, Attempts, Causing Violations, and Conspiracies

Adopting the approach contemplated in the ANPRM without change, the proposed rule prohibits any transactions that have the purpose of evading or avoiding the proposed rule's prohibitions, or that cause a violation of or attempt to violate the proposed rule's prohibitions. The proposed rule also prohibits conspiracies formed to violate the proposed rule's prohibitions.

One commenter suggested expanding the scope of the regulations to prohibit transactions involving algorithms or artificial intelligence models that are trained and developed using bulk U.S. sensitive personal data in certain circumstances. The commenter described a scenario in which the transfer of such an algorithm or model provides a means to evade the prohibitions—for example, where a transaction gives a country of concern or covered person access to the model, and the model makes the underlying bulk U.S. sensitive personal data on which it was trained available to that country of concern or covered person. According to the commenter, this access could occur by querying the model in such a way that results in it sharing all of or a highly relevant component of the underlying data on which it was trained, such as a query that resulted in identification of people with a particular medical condition.⁶⁵ Apart

⁶⁴ 89 FR 15794.

⁶⁵ Tim Johansson & Balder Janryd, Preventing Health Data from Leaking in a Machine Learning System 4–6 (2024) (First Cycle 15 credits, KTH Royal Institute of Technology), <https://kth.diva->

⁶³ See *infra* note 418 and accompanying text.

from concerns over access to the underlying data, a model could also provide insights into counter-intelligence targeting that would not otherwise be observable from the underlying sensitive personal data. The Department shares these concerns. In response to the comment, the proposed rule includes Examples 5 and 6 in § 202.304(b) highlighting how these regulations would apply in certain scenarios where bulk U.S. sensitive personal data would be licensed or sold to support algorithmic development, including cases of evasion, or where sensitive personal data could be extracted from artificial intelligence models. The Department will continue to evaluate the national-security risks in this emerging area as it considers the effectiveness of this regulation. To the extent that there are broader concerns about national-security risks from the export of artificial intelligence models or algorithms regardless of the access they provide to sensitive personal data (such as their ability to provide insights that would not otherwise be observable from the data on which they are trained), the Department believes that other authorities, such as export controls and Executive Order 13859 of February 11, 2019 (Maintaining American Leadership in Artificial Intelligence),⁶⁶ are more appropriate in the first instance to address those concerns.

19. Section 202.305—Knowingly Directing Prohibited Transactions

Adopting the approach contemplated in the ANPRM without change, the proposed rule prohibits U.S. persons from knowingly directing any covered data transaction that would be a prohibited transaction (including restricted transactions that do not comply with the security requirements) if engaged in by a U.S. person.

20. Section 202.215—Directing

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines “directing” to mean that the U.S. person has any authority (individually or as part of a group) to make decisions on behalf of a foreign entity and exercises that authority. For example, a U.S. person would direct a transaction by exercising

their authority to order, decide to engage, or approve a transaction that would be prohibited under these regulations if engaged in by a U.S. person.

21. Section 202.230—Knowingly

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines “knowingly” to mean, with respect to conduct, a circumstance, or a result, that the U.S. person had actual knowledge of, or reasonably should have known about, the conduct, circumstance, or result. To determine what an individual or entity reasonably should have known in the context of prohibited transactions, the Department will take into account the relevant facts and circumstances, including the relative sophistication of the individual or entity at issue, the scale and sensitivity of the data involved, and the extent to which the parties to the transaction at issue appear to have been aware of and sought to evade the application of these proposed rules. As a result of the knowledge standard, the regulations incorporating the word “knowingly” do not adopt a strict liability standard.

The “knowingly” language is also not intended to require U.S. persons, in engaging in vendor agreements and other classes of data transactions with foreign persons, to conduct due diligence on the employment practices of those foreign persons to determine whether the foreign persons’ employees qualify as covered persons. For instance, as illustrated by Examples 37 and 38 in the ANPRM, which are incorporated into the proposed rule, it would not be a prohibited transaction for a U.S. person to enter into a vendor agreement to have bulk U.S. sensitive personal data processed or stored by a foreign person that is not a covered person, even if that foreign person then employs covered persons and grants them access to the data (absent any indication of evasion or knowing direction).⁶⁷ In those circumstances, the U.S. person would not be expected to conduct due diligence on the foreign person’s employment practices as part of its risk-based compliance program.

Several commenters sought clarity about liability where service providers have little or no knowledge of the data that customers keep or transact on their infrastructure. They also requested that the Department distinguish between data controllers and data processors. In response to these comments, the proposed rule has provided additional examples to clarify the function of the

“knowingly” standard. See § 202.230(b)(2)–(6). As the examples demonstrate, if a U.S. entity merely provides a software platform or owns or operates infrastructure for a U.S. customer, and thus does not know or reasonably should not know of the kind or volume of data involved, then the U.S. entity generally would not “knowingly” engage in a prohibited transaction if the U.S. customer uses their platform or infrastructure to engage in a prohibited transaction. Instead, the U.S. customer would generally be responsible for having “knowingly” engaged in the prohibited transaction. Likewise, if a U.S. entity merely stores encrypted data on behalf of a U.S. customer and does not have access to the encryption key (or has access only to an emergency backup encryption key usable only at the customer’s explicit request), and if the U.S. entity is reasonably unaware of the kind or volume of data involved, the U.S. entity generally would not meet the “knowingly” standard of the proposed rule.

The Department declines, however, to draw a categorical distinction between processors and controllers in the proposed rule. Inserting a categorical distinction based on the kind of entity would be inconsistent with the structure and overall approach of the proposed rule, which addresses activities that present an unacceptable national security risk. In addition, as the new examples illustrate, the same kinds of entities can engage in different kinds of activities, some of which (such as merely providing a software platform) raise different risks than others (such as providing a software platform and services to handle and process the data). The “knowingly” standard provides the requisite flexibility to address the national security risks while providing a basis to distinguish responsibility based on the activities and roles that particular entities may have. The proposed rule thus adopts the approach described in the ANPRM with the additional examples described above in this section to illustrate the “knowingly” standard.

Similarly, one comment sought clarification that the proposed rule would apply only to U.S. persons that have or maintain control over the bulk U.S. sensitive personal data involved in a prohibited or restricted transaction. As the commenter explained, an automobile manufacturer should not have compliance obligations with respect to bulk U.S. sensitive personal data that is transferred via an aftermarket device that was installed in a vehicle fleet by the owner. As

portal.org/smash/get/diva2:1865596/FULLTEXT01.pdf [<https://perma.cc/S5S8-M3Df>]; see, e.g., Anuj Mudaliar, *ChatGPT Leaks Sensitive User Data, OpenAI Suspects Hack*, Spiceworks (Feb. 1, 2024), <https://www.spiceworks.com/tech/artificial-intelligence/news/chatgpt-leaks-sensitive-user-data-openai-suspects-hack/> [<https://perma.cc/AS5E-FATZ>].

⁶⁶E.O. 13859, 84 FR 3967 (Feb. 11, 2019).

⁶⁷89 FR 15792.

previewed in the ANPRM, the proposed rule imposes prohibitions and restrictions only on U.S. persons that are engaged in covered data transactions that meet certain criteria. In the commenter's example, the U.S. automobile manufacturer has not engaged in a covered data transaction with respect to the aftermarket device. As a result, no change was made to the proposed rule in response to this comment.

B. Subpart D—Restricted Transactions

1. Section 202.401—Authorization To Conduct Restricted Transactions; Section 202.402—Incorporation by Reference

The proposed rule sets forth three classes of transactions (vendor agreements, employment agreements, and investment agreements) that are prohibited unless the U.S. person entering into the transactions complies with the “security requirements” referenced in section 202.248. The goal of the proposed security requirements is to address national security and foreign-policy threats that arise when countries of concern and covered persons access government-related data or bulk U.S. sensitive personal data that may be implicated by the categories of restricted transactions. The security requirements have been developed and proposed by the Cybersecurity and Infrastructure Security Agency (“CISA”) in coordination with the Department. CISA has published the proposed requirements—the CISA Proposed Security Requirements for Restricted Transactions—on its website, as announced via a **Federal Register** notice requesting comment on those proposed security requirements issued concurrently with this proposed rule. The proposed security requirements require U.S. persons engaging in restricted transactions to comply with organizational and system-level requirements, such as ensuring that basic organizational cybersecurity policies, practices, and requirements are in place, as well as data-level requirements, such as data minimization and masking, encryption, or privacy-enhancing techniques. After CISA receives and considers public input, it will revise as appropriate and publish the final security requirements. The Department of Justice will then incorporate by reference the published final security requirements in the final rule that the Department issues. Interested parties can view CISA's proposed security requirements on CISA's website at <https://www.cisa.gov/> and can review CISA's notice

requesting comments on the proposed security requirements in the notice docketed as CISA–2024–0029 (October 29, 2024).

The proposed rule also clarifies that restricted transactions are not prohibited only if they comply with the security requirements and other applicable requirements for conducting restricted transactions. The proposed rule includes a new example that makes it clear that U.S. persons engaging in restricted transactions may not, absent a license, use measures other than the security requirements and other applicable conditions to mitigate the risk posed by country-of-concern or covered-person access.

Some commenters provided feedback on the security requirements that would govern restricted transactions. As explained in the ANPRM, CISA will be soliciting comments on the proposed security requirements as part of a separate notice-and-comment process in parallel with this NPRM, and the Department urges commenters to provide any comments on the security requirements through that process.

2. Section 202.258—Vendor Agreement

The proposed rule defines a “vendor agreement” as any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration. The ANPRM contemplated defining the term “cloud-computing services” as that term is defined in NIST Special Publication (“SP”) 800–145.⁶⁸ NIST SP 800–145 describes cloud computing in a way that includes different essential characteristics, deployment models, and service models, such as “Infrastructure as a Service (IaaS),” “Platform as a Service (PaaS),” and “Software as a Service (SaaS).”⁶⁹ Because cloud computing is just one example of several types of services that may be involved in a vendor agreement, it does not appear useful to separately or specially define that term in the proposed rule at this time. The Department may consider issuing guidance in the future that describes cloud computing in reference to the NIST definition.

⁶⁸ 89 FR 15788.

⁶⁹ See Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing* (NIST, SP 800–145, Sept. 2011), <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [<https://perma.cc/HUJ5-B2JS>].

3. Section 202.217—Employment Agreement

The proposed rule defines an “employment agreement” as any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level.

4. Section 202.228—Investment Agreement

The proposed rule defines an “investment agreement” as any agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to (1) real estate located in the United States or (2) a U.S. legal entity. The proposed rule categorically excludes certain passive investments that do not pose an unacceptable risk to national security because they do not give countries of concern or covered persons a controlling ownership interest, rights in substantive decision-making, or influence through a non-controlling interest that could be exploited to access government-related data or bulk U.S. sensitive personal data. Specifically, the proposed rule excludes from “investment agreement” investments (1) in any publicly traded security, in any security offered by any investment company that is registered with the United States Securities and Exchange Commission, such as index funds, mutual funds, exchange-traded funds, or made as limited partners (or equivalent) into a venture capital fund, private equity fund, fund of funds, or other pooled investment fund, if the limited partner's contributions and influence are circumscribed as set forth in the proposed rule; (2) that give the covered person less than 10 percent of total voting and equity interest in a U.S. person; and (3) that do not give a covered person rights beyond those reasonably considered to be standard minority shareholder protections.

With respect to the requirement of a de minimis percentage of total voting and equity interest, the Department is considering a range of different proposals. The proposed rule's definition of “investment agreement” would apply to investments that give a covered person a certain percentage or more of total voting and equity interest in a U.S. person, even where that investment is not accompanied by other

formal rights beyond standard minority shareholder protections. The proposed rule would include this de minimis threshold to account for the unacceptable national security risk posed by otherwise passive investments that may provide investors with meaningful economic leverage or informal influence over access to a company's assets (like sensitive personal data) even when the investors do not obtain formal rights, control, or access beyond standard minority shareholder protections. The proposed rule would tentatively set this threshold number at 10 percent to exclude truly passive investments while also capturing investments that informally may provide covered persons with influence that presents unacceptable national security risks. The Department is also considering de minimis thresholds that are significantly lower and higher than this percentage, such as the 5 percent threshold above which investors must publicly report their direct or indirect beneficial ownership of certain covered securities under the Securities Exchange Act of 1934, 15 U.S.C. 78m(d). As a result, the final figure in the proposed rule could potentially cover passive investments that provide less (or more) than 10-percent voting and equity interests in a U.S. person. The Department invites public comment on the specific de minimis threshold that should be used in this exception for passive investments.

C. Subpart E—Exempt Transactions

As previewed in the ANPRM, the proposed rule exempts several classes of data transactions from the scope of the proposed rule's prohibitions.

1. Section 202.501—Personal Communications; Section 202.502—Information or Informational Materials; and Section 402.503—Travel

The proposed rule exempts three classes of data transactions to the extent that they involve data that is statutorily exempt from regulation under IEEPA: personal communications, information or informational materials, and data that is ordinarily incident to travel to or from another country.

One comment suggested clarifying that the exemption for personal communications that do “not involve a transfer of anything of value” under 50 U.S.C. 1702(b)(1) is “inclusive of business and commercial transactions.” The proposed rule makes no change in response to this comment, as the clarification does not seem necessary at this time, given the scope of the statutory exemption and the proposed

rule. Section 1702(b)(1) applies to any “personal communication,” so it would be inappropriate to rely on that statutory language to exempt, as this comment suggests, “business and commercial transactions.” Further, the categories of sensitive personal data encompassed by the proposed rule do not include any personal communications. For example, fingerprints and other biometric identifiers, human genetic testing results, and data about financial assets and liabilities are not “communications” from one person to another. Any clarification of the phrase “a transfer of anything of value,” therefore, does not appear necessary. To the extent the commenters, a group of trade associations representing telecommunications providers, are concerned that personal communications between individuals that do not involve a transfer of anything of value are business transactions from their perspective, as purveyors of telecommunications services, the Department refers the commenters to the qualified exemption for telecommunications services in proposed § 202.509.

The Department discusses the exemption for information or informational materials in part VI of this preamble.

Although not raised by commenters, the proposed rule also adds a separate exemption for data transactions that are ordinarily incident to travel to or from another country, such as arranging travel or importing baggage for personal use. This exemption implements and tracks the statutory exemption in 50 U.S.C. 1702(b)(4).

2. Section 202.504—Official Business of the United States Government

Adopting the approach contemplated in the ANPRM without change, the proposed rule exempts data transactions to the extent that they are for (1) the conduct of the official business of the United States Government by its employees, grantees, or contractors; (2) any authorized activity of any United States Government department or agency (including an activity that is performed by a Federal depository institution or credit union supervisory agency in the capacity of receiver or conservator); or (3) transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government. Most notably, this exemption would exempt grantees and contractors of Federal departments and agencies, including the Department of Health and Human Services, the Department of Veterans Affairs, the National Science

Foundation, and the Department of Defense, so that those agencies can pursue grant-based and contract-based conditions to address risks that countries of concern can access sensitive personal data in transactions related to their agencies' own grants and contracts, as laid out in section 3(b) of the Order—without subjecting those grantees and contractors to dual regulation.

3. Section 202.505—Financial Services

Section 2(a)(v) of the Order exempts any transaction that is “ordinarily incident to and part of the provision of financial services, including banking, capital markets, and financial insurance services, or required for compliance with any Federal statutory or regulatory requirements, including any regulations, guidance, or orders implementing those requirements.”⁷⁰ The proposed rule defines these exempt transactions in further detail. Notably, the proposed rule exempts the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces, while still prohibiting these marketplaces from conducting data transactions that involve data brokerage), as well as exempting the transfer of personal financial data or covered personal identifiers for the provision or processing of payments or funds transfers.

Numerous commenters expressed support for the financial-services exemption. Commenters expressed appreciation for the exemption's careful scoping to enable business and commercial transactions. Commenters sought specific edits to the payment-processing part of the exemption to ensure that it covers operations involving payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention, and payment-related loyalty point program administration. The Department appreciates these suggested clarifications, and the proposed rule incorporates these proposed edits by explicitly adding the provision of services ancillary to processing payments and funds transfers, with the suggested examples, to the list of exempt financial services transactions.⁷¹ The financial-services exemption aims to identify the low-risk business and

⁷⁰ 89 FR 15423.

⁷¹ 89 FR 15794.

commercial transactions that should continue unimpeded while also ensuring that the Order and its implementing regulations do not serve as a broader economic decoupling from countries of concern. These edits are consistent with that purpose.

Another commenter also suggested that investment-management services be included in the financial-services exemption. The Department does not intend to impede activities that are ordinarily incident to and part of the provision of investment-management services that manage or provide advice on investment portfolios or individual assets for compensation (such as devising strategies and handling financial assets and other investments for clients) or provide services ancillary to investment-management services (such as broker-dealers executing trades within a securities portfolio based upon instructions from an investment advisor). For further clarity, the proposed rule explicitly adds investment-management services to the financial-services exemption set out in §§ 202.505(a)(1) and 202.505(a)(6).

One commenter requested an exemption for cargo-related information containing listed identifiers. The Department believes this comment is focused on scenarios in which bulk personal identifiers are transferred as part of shipping purchased goods internationally. The Department declines to adopt a separate exemption, or an expansion of the scope of the exemption for transfers of data required by or authorized by Federal law or international agreement, for cargo-related information because the proposed rule already exempts the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services. This existing exemption appears to adequately address the scenario raised by the commenter. Thus, the proposed rule adopts the approach described in the ANPRM.

Although not raised by any commenters, the Department is also considering whether and how the financial-services exemption should apply to employment and vendor agreements between U.S. financial-services firms and covered persons where the underlying financial services provided do not involve a country of concern. Under this exemption, U.S. persons would be required to evaluate whether a particular data transaction (such as a transaction involving data brokerage or a vendor, employment, or investment agreement) is “ordinarily incident to and part of” the provision of financial services such that it is treated

as an exempt transaction.⁷² At one end of the spectrum, and as previewed by Example 53 in the ANPRM, if a U.S. financial institution or financial-services company uses a data center operated by a covered person in a country of concern to facilitate payments to U.S. persons in that country of concern, the proposed rule would treat that vendor agreement as “ordinarily incident to and part of” the facilitation of those payments—and thus exempt.⁷³ See § 202.505(b)(3). On the other end of the spectrum, and as previewed by Example 27 in the ANPRM, if a U.S. financial institution or financial-services company hires a covered person as a data scientist with access to its U.S. customers’ bulk personal financial data to develop a new app that could be sold as a standalone product to the company’s customers, the proposed rule would treat this employment agreement as not “ordinarily incident to and part of” the financial services provided by the U.S. company—and thus not exempt.⁷⁴ See § 202.217(b)(4).

Between those two ends of the spectrum, the Department is considering whether the transactions in the following new examples should be treated as exempt transactions or as restricted transactions:

- *New example in § 202.505(b)(4).* Same as Example 3 (see § 202.505(b)(3)), but the underlying payments are between U.S. persons in the United States and do not involve a country of concern: A U.S. bank or other financial institution, to facilitate payments that do not involve a covered person or country of concern (e.g., between U.S. persons in the United States), stores and processes the customers’ bulk financial data using a data center operated by a third-party service provider in a country of concern, which is a covered person. Should the vendor agreement with the covered person, which is otherwise a restricted transaction, be treated as “ordinarily incident to and part of” the

U.S. financial institution’s facilitation of payments that do not involve a covered person or country of concern?

- *New example in § 202.505(b)(12).* A U.S. company provides wealth-management services and collects bulk personal financial data on its U.S. clients. The U.S. company appoints a citizen of a country of concern, who is located in a country of concern, to its board of directors. In connection with the board’s data security and cybersecurity responsibilities, the director could access the bulk personal financial data. Should the employment agreement with the covered person as a board director, which is otherwise a restricted transaction, be treated as “ordinarily incident to and part of” the U.S. company’s provision of wealth-management services to its U.S. clients?

The Department is tentatively considering treating the transactions in both examples as restricted transactions because it does not believe that an employment agreement (including the hiring of board members) or a vendor agreement that gives a covered person access to U.S. persons’ bulk sensitive personal data is a reasonable and typical practice in providing the underlying financial services that do not otherwise involve covered persons or a country of concern. These transactions therefore appear to pose the same unacceptable national security risk regardless of the kinds of underlying services provided by the U.S. person. The Department welcomes public comment to inform its resolution of this issue, including the extent to which it is reasonable, necessary, and typical practice for U.S. financial-services firms to hire covered persons as employees or vendors with access to U.S. persons’ bulk sensitive personal data as part of providing financial services that do not involve a country of concern; why U.S. financial-services firms hire covered persons instead of non-covered persons in those circumstances; and any additional compliance costs that would be incurred if the transactions in these examples were treated as restricted transactions. In addition, after issuance of the final rule, the Department intends to consult the Department of the Treasury and Federal financial regulatory agencies as part of issuing any guidance or advisory opinions regarding the application of the financial-services exemption.

4. Section 202.506—Corporate Group Transactions

As previewed in the ANPRM, the proposed rule exempts covered data transactions to the extent that they are (1) between a U.S. person and its

⁷² Cf., e.g., 31 CFR 560.405(c) (discussing OFAC exemption for transactions “ordinarily incident to a licensed transaction” as applied to scenarios involving the provision of transportation services to or from Iran), 515.533 n.1 (discussing OFAC exemption for transactions “ordinarily incident to” a licensed transaction as applied to scenarios involving the licensed export of items to any person in Cuba); Letter from R. Richard Newcomb, Director, U.S. Dep’t of Treas., Off. of Foreign Assets Control, *Re: Iran: Travel Exemption* (Nov. 25, 2003), <https://ofac.treasury.gov/media/7926/download?inline> [<https://perma.cc/3VRL-X886>] (discussing the OFAC exemption for transactions “ordinarily incident to” travel as applied to scenarios involving the use of airline-service providers from a sanctioned jurisdiction).

⁷³ 89 FR 15794.

⁷⁴ 89 FR 15789.

subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control of) a country of concern; and (2) ordinarily incident to and part of administrative or ancillary business operations (such as sharing employees' covered personal identifiers for human-resources purposes; payroll transactions like the payment of salaries and pensions to overseas employees or contractors; paying business taxes or fees; purchasing business permits or licenses; sharing data with auditors and law firms for regulatory compliance; and risk management). The ANPRM called this exemption "intra-entity transactions."⁷⁵ For greater clarity and accuracy, the proposed rule revises the name of this exemption to "corporate group transactions."

Some commenters requested that the Department broaden the corporate group transactions exemption to include routine business activities performed by third-party service providers. Similarly, commenters proposed augmenting the same exemption to include suppliers and other third-party vendors who are contractually bound to maintain privacy requirements and who engage in product and services development, research, and improvement activities for U.S. companies. The Department declines to incorporate these suggestions because they would not adequately mitigate the threats posed by access to government-related data or bulk U.S. sensitive personal data by a country of concern or covered person. Thus, the proposed rule adopts the approach described in the ANPRM without change, permitting restricted transactions involving vendor agreements to proceed as long as they comply with the proposed rule's security requirements designed to mitigate access to the sensitive personal data by countries of concern and covered persons.

One commenter requested clarification that it would not be a prohibited transaction for a U.S. company to provide access to a global company staff directory to its business office and employees located in a country of concern. Consistent with the approach contemplated in the ANPRM, this scenario would not be a prohibited or restricted transaction under the proposed rule for two independent reasons. First, a company directory containing only contact or demographic data linked to other contact or demographic data would not fall within the definition of "covered personal identifiers" and thus would not

constitute government-related data or bulk U.S. sensitive personal data. As a result, there would be no covered data transaction in providing such a directory. Second, the U.S. company's sharing of the directory would not be a prohibited or restricted transaction, regardless of whether the business office is a foreign branch or a subsidiary or affiliate: if the business office in the country of concern is a branch of the U.S. company, the branch is part of the same "U.S. person" as the U.S. company, and the U.S. company has not engaged in any transaction with a foreign person in the first place. If, by contrast, the business office is a subsidiary or affiliate of the U.S. company, the sharing is an exempt corporate group transaction because a transaction within a corporate group granting its employees access to a company directory is ordinarily incident to ancillary or administrative business operations. (In different circumstances where that exemption is not applicable, a transaction within a corporate group that gives an employee who is a covered person access to government-related data or bulk U.S. sensitive personal data would generally be a restricted employment agreement.)

5. Section 202.507—Transactions Required or Authorized by Federal Law or International Agreements, or Necessary for Compliance With Federal Law

As previewed in the ANPRM, the proposed rule exempts covered data transactions to the extent that they are required or authorized by Federal law, international agreements or specified global health and pandemic preparedness measures, or necessary for compliance with Federal law.

Some commenters requested clarity about whether the exemption for regulatory compliance (which the ANPRM contemplated as part of the financial-services exemption) applies to compliance with all Federal law, not just financial laws.⁷⁶ The Department acknowledges that this is a correct understanding of this exemption. To improve clarity and reflect this understanding, the proposed rule moves the exemption for compliance with Federal law from the financial-services exemption to a standalone subpart of the exemption for transactions required or authorized by Federal law or international agreements.

The proposed rule clarifies that, with respect to international agreements authorizing or requiring data transactions, the exemption applies only

to international agreements to which the United States is a party. Some commenters requested a non-exhaustive list of international agreements to which this exemption applies. The proposed rule adds an illustrative list of specific international agreements to which this exemption applies.

One commenter sought clarification on whether transactions required or authorized by international agreements include transactions in accordance with arrangements that facilitate international commercial data flows, such as the Global Cross-Border Privacy Rules ("G-CBPR") and Global Privacy Recognition for Processors ("G-PRP") Systems of the Global Cross-Border Privacy Rules Forum ("Global CBPR Forum") and the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("APEC CBPR") and APEC Privacy Recognition for Processors Systems. These arrangements are outside the scope of the exemption for international agreements. These arrangements consist of frameworks for coordinating national regulatory measures, and they do not facilitate the sharing of data between the U.S. and a country of concern. Thus, data transactions covered by this proposed rule would not be "pursuant to these arrangements as necessary to meet the definitional requirements of the exemption. The Department further declines to expand the scope of the exemption to incorporate these arrangements, which are designed to address general privacy concerns and other issues rather than the national security risks detailed in the Order. The same commenter also sought clarity as to whether the EU-U.S. Data Privacy Framework ("DPF") would be such an international agreement. The EU-U.S. DPF is similarly an arrangement that falls outside the scope of the exemption. The EU-U.S. DPF fulfills different objectives than the proposed rule and does not facilitate the sharing of information between a U.S. person and a country of concern or covered person. For example, under the EU-U.S. DPF and pursuant to Executive Order 14086 of October 7, 2022 (Enhancing Safeguards for United States Signals Intelligence Activities), the Attorney General determined that the laws of EU/ European Economic Area countries require appropriate safeguards for signals intelligence activities affecting U.S. persons' personal data.⁷⁷

⁷⁷ E. O. 14086, 87 FR 62283 (Oct. 7, 2022); Dep't of Just., Attorney General Designations of the European Union, Iceland, Liechtenstein, and Norway as "Qualifying States", 88 FR 44844 (July 13, 2023).

⁷⁵ 89 FR 15794.

⁷⁶ 89 FR 15794–95.

Furthermore, while DPF- and APEC CBPR-certified companies are subject to domestic law, including the Order, no DPF or APEC CBPR countries or jurisdictions are currently designated as countries of concern under this Executive Order. As such, the provisions of the Order would not apply to transfers conducted in reliance on the DPF or APEC CBPR, and any data transactions that the proposed rule does cover would not be “pursuant to” such arrangements as required for this exemption. Therefore, the proposed rule adopts the approach contemplated by the ANPRM without change.

6. Section 202.508—Investment Agreements Subject to a CFIUS Action

Adopting the approach contemplated by the ANPRM, the proposed rule exempts investment agreements to the extent that they are the subject of a “CFIUS action” as defined in section 202.207 (*i.e.*, CFIUS has suspended a proposed or pending transaction, or entered into or imposed mitigation measures to address a national security risk involving access to sensitive personal data by countries of concern or covered persons). The rationale for this approach is discussed separately in part IV.K of this preamble.

7. Section 202.509—Telecommunications Services

The proposed rule exempts transactions that are ordinarily incident to and part of telecommunications services.

Multiple commenters requested that the proposed rule include an additional exemption for data that is incidental to the provision and delivery of communications services. They asked that this kind of data be carved out from the scope of any restrictions on sensitive personal data for consumers, enterprises, and governments, including but not limited to international calling, mobile voice, and data roaming. Commenters also requested that communications service providers be able to use, disclose, or permit access to covered data obtained from their customers, either directly or indirectly through agents, to initiate, render, bill, and collect for communications services. These commenters assert that global commerce relies on effective and efficient global communications, that restrictions on such bulk U.S. sensitive personal data could hinder the ability of Americans to communicate globally, and that the United States Government has long held a policy of ensuring that communications are enabled even with countries subject to U.S. sanctions.

The Department appreciates the need to ensure Americans’ ability to communicate globally, including with and in countries of concern, and does not intend for these regulations to impede the ability of U.S. telecommunications service providers to operate. Accordingly, the Department has included in the proposed rule an exemption that seeks to address this concern. The proposed exemption is intended to be narrowly tailored to ensure that U.S. telecommunications service providers retain the ability to operate unimpeded while also continuing to mitigate the national security risk associated with data brokerage (*i.e.*, the sale of or leasing of access to customer data) to countries of concern and covered persons.

8. Section 202.510—Drug, Biological Product, and Medical Device Authorizations

Under the proposed rule, certain data transactions necessary to obtain and maintain regulatory approval to market a drug, biological product, medical device, or combination product in a country of concern would be exempt from the prohibitions in the proposed rule. This exemption balances the need to mitigate the risks to U.S. national security from the unrestricted transfer of bulk U.S. sensitive personal data to countries of concern against the scientific, humanitarian, and economic interests in enabling the sale of medicines in those countries. The proposed rule includes reporting requirements that will allow the Department to maintain visibility on the type and amount of data that is being transmitted to countries of concern under this exemption.

This exemption is limited to data that is de-identified; required by a regulatory entity to obtain or maintain authorization or approval to research or market a drug, biological product, device, or combination product (*i.e.*, covered product); and reasonably necessary to evaluate the safety and effectiveness of the covered product. For example, de-identified data that is gathered in the course of a clinical investigation and would typically be required for Food and Drug Administration (“FDA”) approval of a covered product would generally fall within the exemption. Conversely, clinical participants’ precise geolocation data, even if required by a country of concern’s regulations, would fall outside the scope of the exemption because such data is not reasonably necessary to evaluate safety or effectiveness.

The Department recognizes that data collection and submission continue beyond the initial regulatory approval process, and it intends the term “regulatory approval data” to include data from post-market clinical investigations (conducted under applicable FDA regulations, including 21 CFR parts 50 and 56), clinical care data, and post-marketing surveillance, including data on adverse events.⁷⁸ For example, where continued approval to market a drug in a country of concern is contingent on submission of data from ongoing product vigilance or other post-market requirements, the exemption applies.

The exemption applies even where FDA authorization for a product has not been sought or obtained. The Department does not, in these regulations, intend to require U.S. companies to first seek authorization to market a product in the United States before seeking regulatory approval from a country of concern.

The exemption is limited to transactions that are necessary to obtain or maintain regulatory approval in the country of concern. The Department specifically invites comments on the types of transactions that are necessary to that end. By way of illustration, Example 3 of § 202.510, as proposed, would not exempt a vendor or employment agreement with a covered person to prepare data for submission to a country of concern’s regulatory entity because the Department does not currently believe that such transactions are necessary to obtain regulatory approval. The Department seeks comments on whether, and why, such a vendor or employment agreement with a covered person to prepare data for submission is necessary and should be exempt.

As Example 3 reflects, the Department does not currently believe that it is reasonably necessary to use a covered person—as opposed to services provided by the U.S. company itself or by a non-covered person—to prepare data for regulatory submission. Although the marginal risk to national security from granting additional covered persons access to the submission data may be low, given that the submission data is ultimately being transferred directly to the government of

⁷⁸ See U.S. Food & Drug Admin., *What Is a Serious Adverse Event?* (May 18, 2023), <https://www.fda.gov/safety/reporting-serious-problems-fda/what-serious-adverse-event#:~:text=An%20adverse%20event%20is%20any,medical%20product%20in%20a%20patient> [https://perma.cc/9Q23-HRWY] (“An adverse event is any undesirable experience associated with the use of a medical product in a patient”).

a country of concern, the Department believes that a third-party vendor in this scenario may require access to a broader set of data than the regulatory body itself. At the same time, the Department recognizes that regulatory and legal expertise relevant to a country of concern is likely to be concentrated in the country of concern. Employment and vendor transactions in this context would be restricted, not prohibited, transactions, and generally could proceed if the requirements applicable to restricted transactions were followed. The Department welcomes comments that address this scenario and other similar transactions, including the potential impacts to clinical research, medical product development and authorizations, and companies' business practices and operations, as well as the feasibility of obtaining regulatory approval without engaging covered persons to access bulk U.S. sensitive personal data or if such engagements are subject to the security, recordkeeping, and reporting requirements applicable to restricted transactions.

The exemption requires that parties engaged in transactions involving regulatory approval data with countries of concern nonetheless comply with the recordkeeping and reporting requirements otherwise applicable to U.S. persons engaged in restricted transactions, because of the heightened national security risk that arises from transmitting U.S. sensitive personal data or government-related data directly to a government entity in a country of concern.

The Department seeks comment on the proposed scope of this exemption, including on the definition of regulatory approval data and the extent to which data submissions to regulatory entities in countries of concern may involve personally identifiable data.

9. Section 202.511—Other Clinical Investigations and Post-Marketing Surveillance Data

A few commenters expressed concerns that the proposed rule's inclusion of aggregated and anonymized data would prohibit companies from launching clinical investigations in countries of concern. Commenters also noted the possibility that overly restrictive prohibitions might harm biopharmaceutical innovation. The Department has considered these comments and agrees that some exemption or accommodation for clinical research may be appropriate. The Department proposed the exemption in § 202.511 for that purpose. To help inform the appropriate contours of the proposed provision, the

Department invites additional comments that illustrate the scope of transactions that might be subject to the proposed rule's restrictions and prohibitions and the consequences for clinical research if the proposed prohibitions and restrictions were applied to that context.

The United States has a national security interest in the development, authorization, and availability of medical products, including medical countermeasures to diagnose, treat, or prevent serious or life-threatening diseases or conditions that may be attributable to biological, chemical, radiological, or nuclear agents. The Department seeks to mitigate the national security risk described in the Order without unduly burdening the biomedical innovation that benefits U.S. persons. The Department is considering how to effectively strike that balance and how to scope an exemption for transactions related to or supporting FDA-regulated research to meet that goal.

The Department is considering the scope of a possible exemption along three axes. First, in terms of the types of data that would be within the exemption; second, in terms of the types of transactions involving that data that would be exempted; and third, in terms of the duration of any exemption.

On the first axis, the Department anticipates that any exemption would concern data obtained in the course of clinical investigations related to drugs, biological products, devices, and combination products, as those terms are defined in the Federal Food, Drug, and Cosmetic Act ("FD&C Act") and FDA regulations. The Department believes that these products raise the most significant countervailing economic, health, and scientific concerns that might outweigh the national security interests otherwise at stake. The Department seeks comment on whether the exemption should exempt clinical investigations data related to other products, such as foods (including dietary supplements) that bear a nutrient content claim or a health claim, food and color additives, and electronic products, as those terms are defined in the FD&C Act.

The Department also recognizes the existing regulatory framework in these contexts and is evaluating whether these provisions adequately reduce the national security risk associated with the transfer of bulk U.S. sensitive personal data to a country of concern or covered person. The FD&C Act and FDA regulations provide a robust framework to protect the confidentiality and privacy of data collected from subjects

in clinical investigations. This current framework of statutory and regulatory requirements protects the rights and safety of human subjects, ensuring that their private information is handled securely. For example, section 505(i) (21 U.S.C. 355(i)) and section 520(g) (21 U.S.C. 360j(g)) of the FD&C Act address the use of investigational new drugs and investigational devices, respectively, in clinical investigations and require that informed consent be obtained from subjects, with certain exceptions.

The implementing regulations established by the FDA in 21 CFR parts 50, 56, 312, and 812 include various requirements, including related to informed consent of human subjects and Institutional Review Boards ("IRBs"). For example, 21 CFR part 56 details requirements for IRB review, approval, and ethical oversight of FDA-regulated clinical investigations. Information about the confidentiality of records must be given to prospective subjects as part of informed consent (21 CFR 50.25(a)(5)), and to approve research, an IRB must determine that, where appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data (21 CFR 56.111(a)(7)). In addition, FDA regulations in 21 CFR part 11 establish requirements to ensure the authenticity, integrity, and, when appropriate, confidentiality of certain electronic records (21 CFR 11.10, 11.30). The FDA further issued a proposed rule in September 2022 proposing to require that certain information about future secondary use of subjects' information or biospecimens be provided to prospective subjects.⁷⁹

These regulations are principally focused on patient privacy, however, and do not directly address the national security concerns that animate the Order. As the Department has explained elsewhere in this preamble, privacy protections, in general, focus on addressing individual rights and preventing individual harm by protecting individuals' right to control the use of their own data and reducing the potential harm to individuals by minimizing the collection of data on the front end and limiting the permissible uses of that data on the back end. National security measures, by contrast, focus on collective risks and externalities that may result from how individuals and businesses choose to sell and use their data, including in lawful and legitimate ways. But the

⁷⁹Protection of Human Subjects and Institutional Review Boards, 87 FR 58733 (proposed Sept. 28, 2022).

Department is evaluating whether these existing regulations—for example, the requirements for informed consent under 21 CFR part 50—could offer sufficiently robust protection to also mitigate national security concerns.

The exemption would also apply to clinical care data indicating real-world performance or safety of products, or post-marketing surveillance data (including pharmacovigilance and post-marketing safety monitoring), where necessary to support or maintain authorization by the FDA. These submissions to FDA involve deidentified data and the exemption arising under proposed § 202.511(a)(2) would apply only to deidentified data.

On the second axis, the Department is considering what kinds of transactions to exempt when they involve data that implicates the exemption—such as, hypothetically, bulk U.S. sensitive personal data collected in the course of an FDA-regulated clinical investigation to develop a drug. One possibility would be to exempt all transactions that are part of the conduct of the investigation. Another possibility would be to limit an exemption to only certain types of transactions that are especially important to the conduct of a clinical investigation and that cannot feasibly be avoided without jeopardizing the clinical investigation.

The Department does not intend to categorically preclude clinical investigations from being conducted in a country of concern and does not believe that the proposed rule, even without a clinical investigation-focused exemption, does so. The proposed rule generally does not prohibit or restrict the flow of data from a country of concern to the United States and does not apply to data unrelated to U.S. persons. The Department seeks additional comments on whether, why, and to what extent it would be necessary for U.S. persons to transmit bulk U.S. sensitive personal data to a covered person in order to support a clinical investigation taking place in a country of concern.

For example, the Department has considered the following hypothetical:

- A U.S. sponsor conducts a clinical investigation to determine the safety and effectiveness of an investigational drug product. The clinical investigation involves a multinational trial with both U.S. citizens and non-U.S. citizens enrolled in the trial at different sites across the world, including in a country of concern, to support authorization of the product in the intended use populations. As part of the investigation, and pursuant to an employment or vendor agreement, the

sponsor transmits bulk U.S. sensitive personal data to covered persons in the country of concern to conduct a data analysis of the product's safety and effectiveness across different population groups. This clinical investigation supports an application for a marketing permit for a product regulated by the FDA (*i.e.*, a drug for human use). The trial in this example is subject to the FDA's regulatory framework for clinical investigations.

The Department believes that, absent an exemption, the employment or vendor agreement described in this hypothetical would be a restricted transaction (or a prohibited transaction, if it involves the transfer of bulk human genomic data or biospecimens from which such data could be derived). The Department seeks comments on whether such a vendor agreement should be considered to be “ordinarily incident to and part of” a clinical investigation; how prevalent and important the practice of sending bulk U.S. sensitive personal data to a covered person in a country of concern is; and the potential impacts to clinical research, medical product development and authorization, and industry if such transactions were restricted or prohibited.

The Department also seeks comments on how these concerns apply in post-marketing scenarios, such as pharmacovigilance and post-marketing safety monitoring necessary to support or maintain authorization. For example, the Department has considered the following hypothetical:

- A U.S. pharmaceutical company is required to submit reports to the FDA of adverse events related to its FDA-approved drug for human use, consistent with the requirements under 21 CFR 314.80.⁸⁰ The firm markets many other drug products; has a wide global distribution, including in a country of concern; and receives thousands of reports per year for its various marketed products. Under a vendor agreement, the firm may outsource processing of these reports to entities outside of the United States, including in a country of concern. The firm may also need to exchange adverse event information about its FDA-approved drug product with its distributors in a country of concern to pool the data and identify any adverse events trends across different population groups or conditions of use and submit those data to the FDA.

As in the context of the clinical investigation, the Department believes

that, absent an exemption, the vendor agreements described in this hypothetical would be restricted or prohibited. The Department seeks comments on how pervasive and important the practice of outsourcing the processing of adverse event reports to a covered person is, as well as on how pervasive and important it is to share adverse event information concerning U.S. persons with drug distributors in a country of concern. The Department seeks comments on the potential impacts to patient safety, industry, and the feasibility of obtaining or maintaining regulatory authorizations if such transactions were to be prohibited.

The Department is also aware that, as appropriate and required, certain data related to post-marketing surveillance are made available to global public health authorities, such as the World Health Organization Vigibase. Submissions by the United States Government itself, such as FDA submissions to Vigibase, would be exempt under proposed § 202.504. The Department expects that similar data transactions by U.S. persons, even if such data transactions were considered to be with a country of concern or a covered person so as to fall within the scope of the restrictions and prohibitions, would nonetheless be exempt under proposed § 202.507. The Department seeks specific comments on the nature and type of such submissions and a list of such global health authorities. The Department also notes that, if it is lawfully available to the public from a Federal, State, or local government record or in widely distributed media, such data would not meet the definition of sensitive personal data under § 202.249(b)(2).

FDA regulations include recordkeeping provisions such that FDA investigators can gather information about any data transactions, including to countries of concern. *See* 21 CFR part 312.62. However, in general, FDA's regulations related to clinical investigations do not require sponsors to report data transactions to the FDA in the manner proposed in the recordkeeping and reporting requirements set forth in §§ 202.1101(a) and 202.1102. The Department is considering requiring reporting even for transactions within any exemption to better evaluate the national security risks going forward and seeks comments on the cost and feasibility for industry of also complying with the recordkeeping and reporting requirements set forth in §§ 202.1101(a) and 202.1102 with respect to

⁸⁰ An adverse event report describes the experience of an individual who has experienced an adverse event associated with the use of a drug.

transactions related to clinical investigations.

The Department recognizes that U.S. companies employing covered persons—such as foreign persons primarily resident in a country of concern to support a clinical investigation there—may have to adjust data access policies or protocols to limit covered persons' access to bulk U.S. sensitive personal data. The Department seeks comment on this issue, including the costs and feasibility of adopting such policies or protocols and the likely effect of such policies on medical product research and development, as well as obtaining or maintaining regulatory authorization.

The Department also notes that, under § 202.504, covered data transactions that occur as part of federally funded research would be exempt from the proposed rule's prohibitions (although possibly subject to separate restrictions applicable to a Federal grantee, to include requirements established pursuant to section 3(b)(i) of the Order). The Department invites comment on the proportion of pharmaceutical research that would not be exempt under that exemption, the cost and feasibility of complying with different regulatory requirements depending on the source of funding, and the impact on medical product research and development.

If the Department were to implement an exemption for clinical investigations, clinical data, and post-marketing surveillance as described in this section, it could potentially do so through one or more general licenses as opposed to including the exemption in the final rule. General licenses may be a more flexible regulatory tool that can be adjusted to varying circumstances. Preliminarily, however, the Department believes that a codified exemption would provide more clarity and certainty for relevant entities. The Department also invites comments on the best mechanism to implement an exemption for such data transactions.

Finally, on the third axis, the Department is considering whether any exemption, or parts of it, could feasibly be time-limited to allow industry to shift existing processes and operations out of countries of concern over a transition period. The Department is cognizant of the long planning times and high costs associated with clinical research. If the Department does not broadly exempt clinical research from the scope of the prohibitions, it may consider delaying the effective date of the proposed rule with respect to such research to enable affected entities to complete ongoing or imminent trials without disruption or delay, while

transitioning planning and policies for future trials. The Department could potentially implement such a delay by general or specific licenses, and could use a set period of time or could limit the exemption to studies already past a certain stage, such as submission of an Investigational New Drug application to the FDA by a set date. The Department seeks comment—taking into account other exemptions, such as for federally funded research—on the number of clinical investigations that would be disrupted, and the extent of such disruption, if the prohibitions were immediately applicable; how long and how to structure any delay to minimize disruption without inviting misplaced reliance; and the best mechanism for implementing such a delay.

10. Other Exemptions

The Department is considering whether it is necessary or appropriate to adopt a tailored exemption that would permit covered data transactions involving the export to countries of concern or transfer or sale to covered persons of certain human biospecimens, like blood plasma, intended for direct medical use that the proposed rule would otherwise prohibit. The Department welcomes views about the specific types of biospecimens exported to countries of concern, or transferred or sold to covered persons for direct medical use that the Department should consider exempting from the prohibition on bulk transfers of human genomic data or biospecimens from which bulk human genomic data could be derived. Important considerations could include the importance of the biospecimens for direct medical use; the relative ease with which a country of concern or covered person could derive bulk human genomic data from the biospecimens; the economic and humanitarian value of permitting such transactions; and any other national security concerns the Department should consider.

A few commenters requested that the Department create a new exemption for data processed by a covered person on behalf of a U.S. person for product research, development, or improvement where the U.S. person directs the manner of data processing and contractually binds the covered person to maintain the privacy and security of the data. These comments were too vague to be addressed or implemented. For example, they did not identify the kinds of products that the U.S. person would seek to develop or the kinds of data that would be required for that development. In any case, as the Department discusses in part IV.D.1 of

this preamble, countries of concern have the legal authority and political systems to force, coerce, and influence entities in their jurisdictions to share their data and access with the government. Entities operating in these jurisdictions may be legally compelled to comply with these requests, regardless of their trustworthiness or contractual commitments. The Department assesses that the kind of contractual provisions contemplated by these commenters would not adequately mitigate the risk that countries of concern could compel these covered persons to provide them access to government-related data or Americans' bulk U.S. sensitive personal data. Further, other commenters expressed concern about relying on private parties to monitor and enforce contractual provisions on their own, as discussed in part IV.A.16 of this preamble.

D. Subpart F—Determination of Countries of Concern

1. Section 202.601—Determination of Countries of Concern

As explained in the ANPRM and above in part II of this preamble, countries of concern could exploit government-related data or bulk U.S. sensitive personal data for a range of activities detrimental to U.S. national security, including coercion, blackmail, surveillance, espionage, malicious cyber-enabled activities, malign foreign influence, curbing political dissent and opposition, and tracking and building profiles on potential targets.

The Order instructs the Attorney General to “identify, with the concurrence of the Secretary of State and the Secretary of Commerce, countries of concern.”⁸¹ In the proposed rule, the Attorney General has determined, with the concurrence of the Secretaries of State and Commerce, that the governments of six countries—the People's Republic of China (“China” or “PRC”), along with the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau; the Russian Federation (“Russia”); the Islamic Republic of Iran (“Iran”); the Democratic People's Republic of Korea (“North Korea”); the Republic of Cuba (“Cuba”); and the Bolivarian Republic of Venezuela (“Venezuela”)—have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of U.S. persons, and pose a significant risk of exploiting government-related data or bulk U.S.

⁸¹ 89 FR 15424.

sensitive personal data to the detriment of the national security of the United States or the security and safety of U.S. persons.

In determining that a country has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of U.S. persons, the proposed rule accounts for a range of conduct, including transnational repression; malicious cyber activities; sanctions evasion; theft of intellectual property, trade secrets, and technology; foreign malign influence;⁸² and human-rights abuses. Even where human-rights abuses do not directly involve U.S. persons, the Department considers human-rights abuses to be significantly adverse to national security because of their indirect effects. For example, by developing, testing, and using sophisticated surveillance technology on their own populations or conducting surveillance on their own populations, countries can expand the use of those methods and potentially deploy them directly against U.S. persons or U.S. interests in the future.⁸³ Furthermore, a country that commits human-rights violations shows its disregard for international norms and its intention to use the coercive power of the state to accomplish its policy goals. For example, countries that commit human-rights violations may also attempt to surveil or coerce their citizens in the United States, including through transnational repression.⁸⁴ Based on its experience, the Department believes that such factors demonstrate that a country presents a risk that, if provided access, it would exploit government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or the security and safety of U.S. persons.

During the ANPRM's comment period, commenters requested that the proposed rule include criteria and a transparent process for the Department of Justice to designate countries of concern, including by conducting robust interagency discussion and soliciting

public comment. The proposed rule makes no change in response to this comment. The Order already requires that prior to amending the list of countries of concern, the Department must obtain concurrence by the Secretary of State and the Secretary of Commerce and undertake a rulemaking that is subject to the ordinary process of robust interagency review and notice and public comment. In addition to the opportunity for notice and public comment on this proposed rule's identification of countries of concern, the Department took the optional step of issuing an ANPRM to permit an additional opportunity for public comment on the contemplated countries of concern.

One commenter supported aligning the list of countries of concern with the list established by the Department of Commerce in 15 CFR 791.4, which was adopted pursuant to Executive Order 13873. The ANPRM already contemplated identifying the same countries as countries of concern under the Order as the Department of Commerce identified as foreign adversaries under Executive Order 13873. The proposed rule adopts that approach and identifies those same countries for reasons explained further in this part.

Other commenters expressed concerns that the list of six countries of concern contemplated in the ANPRM is too narrow and does not adequately address entities based in third countries that engage in or facilitate surveillance on U.S. citizens. The proposed rule makes no change in response to this comment. As the ANPRM described, the Department intends to establish this program by issuing proposed rulemakings in tranches based on priority and effective administration of the program. The Department intends to continue working closely with the Department of State, Department of Commerce, and other agencies to monitor the effectiveness of the regulations and the need for any changes. Similarly, one commenter suggested that the Department consider designating a larger group of countries as countries of concern based upon those countries' lack of privacy laws or lack of enforcement of their privacy laws. The Department declines to adopt this approach at this time. The Order's focus is addressing the national security risk posed by country of concern access to government-related data or Americans' bulk U.S. sensitive personal data. The Order does not establish a general data privacy regime. The proposed rule thus maintains the

country of concern framework described in the ANPRM without change.

Informed by the ANPRM comments and the Department's independent research and analysis, which are summarized in part IV.D of this preamble, the Department proposes identifying the same countries of concern as those identified by the Department of Commerce in implementing Executive Order 13873. The proposed rule's definition of each of these countries includes political subdivisions, agencies, or instrumentalities of those countries. In addition, the Order specifically defines a "country of concern," and the Department has determined that every country included on the list of countries of concern meets that definition.

The Department seeks comment from the public on the proposed countries of concern. The proposed rule identifies these six countries as countries of concern for the following reasons.

a. China

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that China has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. Among other conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons, China engages in transnational repression;⁸⁵ steals trade secrets and intellectual property;⁸⁶ conducts foreign malign influence;⁸⁷ commits human rights abuses that could help it develop the capability to surveil, manipulate, or extort U.S. persons;⁸⁸ and conducts extensive malicious cyber activities.⁸⁹

⁸⁵ Press Release, U.S. Dep't of Just., *Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians* (Mar. 25, 2024), <https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived> [https://perma.cc/YQC7-JDCU].

⁸⁶ *Id.*; Off. of the Dir. of Nat'l Intel., *Annual Threat Assessment of the U.S. Intelligence Community*, at 12 (Feb. 5, 2024), <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf> [https://perma.cc/FX84-ZR7E].

⁸⁷ Off. of the Dir. of Nat'l Intel., *supra* note 86, at 12.

⁸⁸ Nat'l Counterintel. & Sec. Ctr., *supra* note 83, at 3–4.

⁸⁹ Off. of the U.S. Trade Rep., *Four-Year Review of Actions Taken in the Section 301 Investigation: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*, at 15–33 (May 14, 2024), <https://ustr.gov/sites/default/files/05.14.2024%20Four%20Year%20Review%20Report.pdf>.

⁸² See 50 U.S.C. 3059(f)(2).

⁸³ Nat'l Counterintel. & Sec. Ctr., *China's Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security* 3–4 (Feb. 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf [https://perma.cc/BL4H-WJSW].

⁸⁴ Press Release, U.S. Dep't of Just., *Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government* (Apr. 17, 2023), <https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government> [https://perma.cc/XM9B-2BU7].

According to the Office of the Director of National Intelligence (“ODNI”), China is “the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.”⁹⁰ China’s cyber espionage operations have included “compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.”⁹¹ China “conducts cyber intrusions that are targeted to affect U.S. and non-U.S. citizens beyond its borders—including journalists, dissidents, and individuals it views as threats—to counter views it considers critical of [Chinese Communist Party] narratives, policies and actions.”⁹² It also conducts malign influence operations to “sow doubts about U.S. leadership, undermine democracy, and extend [China’s] influence.”⁹³

Because China aggressively obtains and exploits data on U.S. persons through both commercial means and theft, and has growing artificial intelligence capabilities, it poses a significant risk of exploiting government-related data or Americans’ bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons.

China aggressively obtains and exploits data on U.S. persons via commercial and illicit means. The National Counterintelligence and Security Center (“NCSC”) has warned that China “views bulk personal data, including healthcare and genomic data, as a strategic commodity to be collected and used for its economic and national security priorities.”⁹⁴ As ODNI has also explained, China “has engaged in extensive and years-long efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations,”⁹⁵ and is “rapidly

expanding and improving its artificial intelligence and big data analytics capabilities for intelligence operations.”⁹⁶ China “uses a number of methods to obtain data.”⁹⁷ For example, China engages in the “wholesale theft” of sensitive personal data of U.S. persons.⁹⁸ The following are some examples of the PRC’s aggressive campaign to steal and exploit government-related data or bulk U.S. sensitive personal data:⁹⁹

- In 2024, a Federal grand jury returned an indictment against hackers working for Chinese intelligence services for, among other things, targeting high-ranking United States Government officials and staffers for a presidential campaign by sending thousands of malicious emails.¹⁰⁰ The hackers potentially compromised the email and cloud storage accounts and telephone records belonging to millions of Americans.¹⁰¹

- In 2020, a Federal grand jury returned an indictment against four members of the PRC’s People’s Liberation Army for hacking U.S. credit-reporting agency Equifax in 2017.¹⁰² The hackers stole the data of approximately 145 million victims, obtaining, “in a single breach, . . . the sensitive personally identifiable information for nearly half of all American citizens.”¹⁰³

(D.C. Cir. July 26, 2024) (publicly filed redacted version) (hereinafter “Blackburn Decl.”).

⁹⁶ *Id.* at Gov’t App. 10 ¶ 30.

⁹⁷ *Id.* at Gov’t App. 10 ¶ 32.

⁹⁸ *The Strategic Competition Between the U.S. and the Chinese Communist Party: Hearing Before the H. Select Comm.*, 108th Cong. (2024) (statement of Christopher Wray, Director, Fed. Bureau of Investig.), <https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party> [<https://perma.cc/89CA-DPHQ>]; see also Nat’l Intel. Council, *supra* note 5, at 3.

⁹⁹ Nat’l Intel. Council, *supra* note 5, at 3; Wray, *supra* note 98.

¹⁰⁰ Press Release, U.S. Dep’t of Just., *supra* note 85; Indictment, *United States v. Gaobin*, No. 24–cr–43 (E.D.N.Y. filed Jan. 30, 2024).

¹⁰¹ Indictment ¶ 15, *Gaobin*, 24–cr–43.

¹⁰² Indictment ¶¶ 2–3, *United States v. Zhiyong*, No. 20–cr–046 (N.D. Ga. filed Jan. 28, 2020); see also Press Release, U.S. Dep’t of Just., *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax* (Feb. 10, 2020), <https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking> [<https://perma.cc/2TW4-2HGP>].

¹⁰³ Indictment ¶ 3, *Zhiyong*, No. 20–cr–046; see also Nat’l Intel. Council, *supra* note 5, at 4; Christopher Wray, Dir., Fed. Bureau of Investig., *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Sec. of the United States*, Address at the Hudson Institute Event on China’s Attempt to Influence U.S. Institutions (July 7, 2020), <https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national>

- In 2015, PRC hackers stole the health records of 78.8 million persons from U.S. health insurance provider Anthem, Inc.,¹⁰⁴ and stole the background investigation records of 21.5 million prospective, current, and former Federal employees and contractors from the Office of Personnel Management.¹⁰⁵

- In 2021, a Federal grand jury returned an indictment against four Chinese nationals working for PRC intelligence services for hacking into the computer systems of dozens of companies, universities, and government entities between 2011 and 2018 to steal sensitive technical technology and data, including material related to genetic sequencing.¹⁰⁶

- In 2021, cyber actors linked to China’s intelligence services exploited previously undisclosed vulnerabilities in Microsoft Exchange Server, compromising tens of thousands of computers and networks, including those in the United States, in a massive operation.¹⁰⁷

- In 2018, a Federal grand jury returned an indictment against two PRC intelligence-affiliated officials for conducting a campaign targeting the computer networks and systems of technology and cloud-service companies in at least a dozen U.S. States, as well as United States Government agencies, to access their customers’ data.¹⁰⁸ At least eight major

security-of-the-united-states [<https://perma.cc/LMJ6-882S>].

¹⁰⁴ Nat’l Counterintel. & Sec. Ctr., *supra* note 83, at 3.

¹⁰⁵ U.S. Off. of Pers. Mgmt., *Cybersecurity Incidents*, <https://www.opm.gov/cybersecurity-resource-center/#url=Cybersecurity-Incidents> [<https://perma.cc/V87Q-2K6W>]; Nat’l Counterintel. & Sec. Ctr., *supra* note 83.

¹⁰⁶ See Press Release, U.S. Dep’t of Just., *Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research* (July 19, 2021), <https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion> [<https://perma.cc/KJ76-KRKS>]; Indictment ¶ 4, *United States v. Xiaoyang*, No. 21–cr–01622 (S.D. Cal. filed May 28, 2021).

¹⁰⁷ Press Release, The White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China* (July 19, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/> [<https://perma.cc/5ESU-43VY>].

¹⁰⁸ See Press Release, U.S. Dep’t of Just., *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information* (Dec. 20, 2018), <https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion> [<https://perma.cc/5M68->

20Year%20Review%20of%20China%20Tech%20Transfer%20Section%20301%20(Final).pdf [<https://perma.cc/W6FN-4C38>].

⁹⁰ Off. of the Dir. of Nat’l Intel., *supra* note 86, at 12.

⁹¹ Off. of the Dir. of Nat’l Intel., *Annual Threat Assessment of the U.S. Intelligence Community* 10 (Feb. 6, 2023), <https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf> [<https://perma.cc/4B2Y-7NVD>].

⁹² *Id.*

⁹³ *Id.*

⁹⁴ Nat’l Counterintel. & Sec. Ctr., *supra* note 83, at 1.

⁹⁵ *In Camera, Ex Parte Classified Decl.* of Casey Blackburn, Assistant Dir. of Nat’l Intel., Doc. No. 2066897 at Gov’t App. 10 ¶ 31, *TikTok Inc. v. Garland*, Case Nos. 24–1113, 24–1130, 24–1183

managed service providers were compromised, as well as the National Aeronautics and Space Administration and the Department of Energy.¹⁰⁹ Over 12 years, hackers stole hundreds of gigabytes of data, including the personally identifiable information of over 100,000 U.S. Navy personnel.¹¹⁰

As ODNI has explained, China “also tries to leverage access through its relationships with Chinese companies, strategic investments in foreign companies, and by purchasing large data sets.”¹¹¹ China and Chinese companies “have sought to acquire sensitive health and genomic data on U.S. persons through, for example, investment in U.S. firms that handle such data or by partnering with healthcare or research organizations in the United States to provide genomic sequencing services.”¹¹² China also strategically acquires sensitive personal data on U.S. persons through commercial means, such as by investing in U.S. firms through Chinese companies and engaging in partnerships with hospitals, universities, and research organizations.¹¹³ China employs a wide array of means to ensure that the Chinese government benefits from Chinese companies’ relationships with U.S. companies. Not only do direct investments by Chinese companies facilitate China’s strategic objectives,¹¹⁴ but those direct investments also promote a strategy of “military-civil fusion” that ensures that China’s military can “acquire advanced technologies and expertise developed by [Chinese] companies, universities, and research programs that appear to be civilian entities.”¹¹⁵

These commercial means of obtaining sensitive personal data on U.S. persons are paired with China’s national-

security laws that compel companies to share data they have collected on U.S. persons with the Chinese government.¹¹⁶ As the Department has explained, “China has enacted the world’s most comprehensive set of laws, regulations, and national plans to broadly define its national and public security interests in data and to govern data collection, sales, sharing, and storage.”¹¹⁷ Given “the authoritarian structures and laws of the PRC regime, Chinese companies lack meaningful independence from the PRC’s agenda and objectives,” and “even putatively ‘private’ companies based in China do not operate with independence from the government and cannot be analogized to private companies in the United States.”¹¹⁸ This regime includes “several laws that, in concert, allow the Chinese government to access sensitive personal data possessed by Chinese companies,”¹¹⁹ such as the following:

- The National Security Law of the People’s Republic of China (promulgated by the Standing Committee of the National People’s Congress, July 1, 2015, effective July 1, 2015), which “imposes broad obligations on corporations as well as citizens to assist and cooperate with the Chinese government in protecting what it defines as national security” and to “assist military agencies and relevant departments with national security efforts.”¹²⁰
- The Cybersecurity Law of the People’s Republic of China (promulgated by the Standing Committee of the National People’s Congress, Nov. 7, 2016, effective June 1, 2017), which “requires Chinese companies to store their data within China, to cooperate with crime and security investigations, and to allow full access to data to Chinese authorities.”¹²¹

- The Anti-Terrorism Law of the People’s Republic of China (promulgated by the Standing Committee of the National People’s Congress, Dec. 27, 2015, effective Jan. 1, 2016, amended Apr. 27, 2018), which authorizes the Chinese government to conduct “electronic monitoring,” “irregular inspections,” and “terrorism” investigations and requires individuals

and organizations to comply, in secret, with such investigations”; broadly “defines ‘terrorism’ as ‘propositions and actions that . . . create social panic, endanger public safety, infringe on personal and property rights, or coerce state organs or international organizations to achieve their political, ideological, and other objectives’”; and imposes on all organizations and individuals “the obligation to assist and cooperate with relevant departments in anti-terrorism work.”¹²²

- The Counter-Espionage Law of the People’s Republic of China (promulgated by the Standing Committee of the National People’s Congress, Nov. 1, 2014, amended Apr. 26, 2023, effective July 1, 2023), which authorizes “national security agency staff” to “enter restricted areas, locations, and units” and to “inspect the electronic devices, facilities, and relevant procedures and tools of concerned individuals and organizations,” and also requires “citizens and organizations” to “support and assist” such efforts.¹²³

These laws all “contain provisions that prohibit individuals and organizations from revealing when and if the Chinese government has requested any assistance or information from them.”¹²⁴ As a result, China can covertly obtain data on U.S. persons in the possession of Chinese companies without meaningful due process and independent judicial oversight. China’s commercial acquisitions of data also contribute to the government’s growing repository of data on U.S. persons.¹²⁵

China’s access to bulk U.S. sensitive personal data—whether via commercial means or outright theft—fuels its development of artificial intelligence capabilities, which China believes will drive the next revolution in military affairs.¹²⁶ The Office of the Director of National Intelligence assesses that China is “rapidly expanding and improving its

677]]]; see also Indictment ¶¶ 3–5, *United States v. Zhu*, No. 18–cr–891 (S.D.N.Y. filed Dec. 17, 2018).

¹⁰⁹ Indictment ¶¶ 5–6, *Zhu*, No. 18–cr–891.

¹¹⁰ Indictment ¶ 10, *Zhu*, No. 18–cr–891.

¹¹¹ Blackburn Decl., *supra* note 95, at Gov’t App. 11 ¶ 33.

¹¹² *Id.* at Gov’t App. 11 ¶ 33(a).

¹¹³ Nat’l Counterintel. & Sec. Ctr., *supra* note 83, at 2.

¹¹⁴ Off. of the U.S. Trade Representative, Exec. Off. of the Pres., *Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974* 63 (Mar. 22, 2018), <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF> [<https://perma.cc/SAS4-JSNK>].

¹¹⁵ Press Release, U.S. Dep’t of Def., *DOD Releases List of People’s Republic of China (PRC) Military Companies in Accordance with Section 1260H of the National Defense Authorization Act for Fiscal Year 2021* (Jan. 31, 2024), <https://www.defense.gov/News/Releases/Release/Article/3661985/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/> [<https://perma.cc/S7HA-384R>].

¹¹⁶ Nat’l Counterintel. & Sec. Ctr., *supra* note 83, at 4.

¹¹⁷ Newman Decl., *supra* note 40, at Gov’t App. 49 ¶ 16.

¹¹⁸ *Id.* at Gov’t App. 49 ¶ 17.

¹¹⁹ *Id.* at Gov’t App. 19 ¶ 18.

¹²⁰ *Id.* at Gov’t App. 49–50 ¶ 19; see Exh. A to Newman Decl., *supra* note 40.

¹²¹ Newman Decl., *supra* note 40, at Gov’t App. 50–51 ¶ 20; see Exh. B to Newman Decl., *supra* note 40.

¹²² Newman Decl., *supra* note 40, at Gov’t App. 51 ¶ 21; see Exh. C to Newman Decl., *supra* note 40.

¹²³ Newman Decl., *supra* note 40, at Gov’t App. 51–52 ¶ 23; see Exh. E to Newman Decl., *supra* note 40.

¹²⁴ Newman Decl., *supra* note 40, at Gov’t App. 52 ¶ 24.

¹²⁵ Lisa Monaco, Deputy Att’y Gen., U.S. Dep’t of Just., Remarks on Disruptive Technologies at Chatham House (Feb. 16, 2023), <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-remarks-disruptive-technologies-chatham> [<https://perma.cc/NW6D-HM6Q>] (“So if a company operating in China collects your data, it is a good bet that the Chinese government is accessing it.”).

¹²⁶ Elsa B. Kania, “AI Weapons” in *China’s Military Innovation*, Brookings Inst. (Apr. 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf [<https://perma.cc/JPM7-YHV5>].

AI and big data analytics capabilities for intelligence operations”¹²⁷ and “increasing [its] ability to analyze and manipulate large quantities of personal information in ways that will allow [it] to more effectively target and influence, or coerce, individuals and groups in the United States.”¹²⁸ In turn, China’s advances in artificial intelligence “deepen[] the threats posed by cyberattacks and disinformation campaigns” that China is using “to infiltrate [U.S.] society, steal [U.S.] data and interfere in [U.S.] democracy.”¹²⁹

b. Cuba

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that Cuba has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. The United States has long recognized that the Cuban government presents a national security threat to the United States. Among other conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons, Cuba conducts intelligence operations against the United States; commits human-rights abuses that, among other effects, contribute to a significant increase in migration into the United States and its neighbors;¹³⁰ and sponsors terrorism.¹³¹ Because of the Cuban government’s actions, the United States has imposed some form of economic sanctions on Cuba since the early 1960s, including under the Trading with the Enemy Act of 1917. The United States currently maintains a

comprehensive economic embargo on Cuba.¹³²

Because Cuba has engaged in long-standing efforts to target the United States Government and United States Government personnel for intelligence purposes, Cuba poses a significant risk of exploiting government-related data or Americans’ bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons. According to ODN, Cuba’s intelligence capabilities pose a “significant threat[]” to the United States.¹³³ For decades, Cuban intelligence services have sought to obtain information about the United States Government and to target U.S. persons to pursue Cuba’s interests, including espionage. For example, in 2024, a former U.S. Department of State employee who served as U.S. Ambassador to Bolivia admitted to secretly acting as an agent of Cuba for decades and received a 15-year prison sentence.¹³⁴ In another example, in 2010, a U.S. Department of State official and his wife were sentenced to lengthy prison sentences for participating in a “nearly 30-year conspiracy to provide highly classified U.S. national defense information” to Cuba.¹³⁵ In 2004, a Federal grand jury returned an indictment against an individual for conspiring to share information related to U.S. national defense with Cuba, including helping Cuban intelligence services “spot, assess, and recruit U.S. citizens who occupied sensitive national security positions or had the potential of occupying such positions in the future to serve as Cuban agents.”¹³⁶

In 2002, an employee at the Defense Intelligence Agency was sentenced to 25 years in prison for spying on behalf of Cuba, including sharing the identities of American undercover intelligence officers working in Cuba with the Cuban government.¹³⁷ In 2022, Team Telecom recommended that the Federal Communications Commission (“FCC”) deny an application for a license for a subsea telecommunications cable that would have directly connected the United States to Cuba.¹³⁸ Team Telecom highlighted Cuba’s history of espionage and intelligence activities targeting the United States.¹³⁹ Because Cuba’s state-owned telecommunications monopoly would control the cable, Team Telecom concluded that the cable would give the Cuban government the ability and opportunity to access U.S. persons’ internet traffic, data, and communications transiting the cable, and make the Cuban government an even greater counterintelligence threat to the United States.¹⁴⁰

Cuba also has strong ties to both China and Russia and might share any information it obtains on U.S. persons with either of those countries.¹⁴¹ For example, in 2018, *The Diplomat* noted that the Cuban government “has been reported to sell its intercept data from U.S. communications to third-party buyers, particularly military adversaries of the [United States],” including China.¹⁴² Team Telecom has also found that Cuba’s relationships with China and Russia—which include extensive economic, military and intelligence cooperation—heighten the risk that Cuba could share U.S. sensitive

¹²⁷ Off. of the Dir. of Nat’l Intel., *supra* note 86, at 12.

¹²⁸ Nat’l Intel. Council, *supra* note 5, at 3.

¹²⁹ Nat’l Counterintel. & Sec. Ctr., *supra* note 48, at 4; Wray, *supra* note 98.

¹³⁰ Press Release, U.S. Dep’t of Treas., *Treasury Sanctions Senior Cuban Officials in Response to Violence Against Peaceful Demonstrators* (Aug. 19, 2021), <https://home.treasury.gov/news/press-releases/jy0327> [<https://perma.cc/TQP2-U79G>]; Press Statement, The White House, *Fact Sheet: Biden Harris Administration Measures on Cuba* (July 22, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/22/fact-sheet-biden-harris-administration-measures-on-cuba/> [<https://perma.cc/7H7-BAA8>]; Eric Bazail-Eimil, *Record-Breaking Numbers of Cuban Migrants Entered the U.S. in 2022–23*, *Politico* (Oct. 24, 2023), <https://www.politico.com/news/2023/10/24/record-breaking-numbers-of-cuban-migrants-entered-the-u-s-in-2022-23-00123346> [<https://perma.cc/ZQ6C-KCC4>].

¹³¹ Press Release, U.S. Embassy in Cuba, *U.S. Announces Designation of Cuba as a State Sponsor of Terrorism* (Jan. 11, 2021), <https://cu.usembassy.gov/u-s-announces-designation-of-cuba-as-a-state-sponsor-of-terrorism/> [<https://perma.cc/6GE4-5JJS>].

¹³² *Cuba Sanctions*, U.S. Dep’t of State, <https://www.state.gov/cuba-sanctions/> [<https://perma.cc/Q759-9XA6>].

¹³³ Nat’l Counterintel. & Sec. Ctr., *National Counterintelligence Strategy of the United States 2020–2022*, at 2 (Jan. 7, 2020), https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf [<https://perma.cc/V8NU-PN23>].

¹³⁴ Press Release, U.S. Dep’t of Just., *Former U.S. Ambassador and National Security Council Official Admits to Secretly Acting as Agent of the Cuban Government and Receives 15-Year Sentence* (Apr. 12, 2024), <https://www.justice.gov/opa/pr/former-us-ambassador-and-national-security-council-official-admits-secretly-acting-agent> [<https://perma.cc/NU9F-6NUS>]; Complaint, *United States v. Rocha*, No. 23–mj–04368 (S.D. Fla. filed Dec. 4, 2023).

¹³⁵ Press Release, U.S. Dep’t of Just., *Former State Department Official Sentenced to Life in Prison for Nearly 30-Year Espionage Conspiracy* (July 16, 2010), <https://www.justice.gov/opa/pr/former-state-department-official-sentenced-life-prison-nearly-30-year-espionage-conspiracy> [<https://perma.cc/622F-Y6NR>].

¹³⁶ Press Release, U.S. Dep’t of Just., *Unsealed Indictment Charges Former U.S. Federal Employee with Conspiracy to Commit Espionage for Cuba* (Apr. 25, 2013), <https://www.justice.gov/opa/pr/unsealed-indictment-charges-former-us-federal>

employee-conspiracy-commit-espionage-cuba [<https://perma.cc/ZSW8-7A4R>]; Indictment ¶¶ 14–34, *United States v. Velazquez*, No. 04–cr–044 (D.D.C. filed Feb. 5, 2004), ECF No. 1.

¹³⁷ Ana Montes: Cuban Spy, *Famous Cases and Criminals*, Fed. Bureau of Invest., <https://www.fbi.gov/history/famous-cases/ana-montes-cuba-spy> [<https://perma.cc/MJf5-WG9X>].

¹³⁸ Press Release, U.S. Dep’t of Just., *Team Telecom Recommends the FCC Deny Application to Directly Connect the United States to Cuba Through Subsea Cable* (Nov. 30, 2022), <https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-application-directly-connect-united-states-cuba-through> [<https://perma.cc/77RF-HM6U>]; see generally *ARCOS–1 USA, Inc.*, File No. SCL–MOD–202100928–0039 (Fed. Comm’n Nov. 29, 2022) (committee recommendation to deny application), <https://www.justice.gov/opa/file/1555196/dl?inline> [<https://perma.cc/F9SV-7U98>].

¹³⁹ *ARCOS–1 USA, Inc.*, *supra* note 138, at 11–12.

¹⁴⁰ *ARCOS–1 USA, Inc.*, *supra* note 138, at 14–15.

¹⁴¹ *Id.* at 17–25.

¹⁴² Victor Robert Lee, *Satellite Images: A (Worrying) Cuban Mystery*, *Diplomat* (June 8, 2018), <https://thediplomat.com/2018/06/satellite-images-a-worrying-cuban-mystery> [<https://perma.cc/H6ZF-P3QU>].

personal data that it obtains with China or Russia.¹⁴³

c. Iran

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that Iran has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. Iran engages in transnational repression;¹⁴⁴ commits human-rights abuses, including against U.S. persons;¹⁴⁵ smuggles U.S. technology;¹⁴⁶ evades U.S. sanctions;¹⁴⁷ sponsors terrorism;¹⁴⁸ and conducts malicious cyber activities, among other conduct.

Because Iran has growing cyber expertise and aggressively seeks to obtain and exploit data on U.S. persons, it poses a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons. According to ODNI, "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied . . . networks and data."¹⁴⁹ Individuals linked to the

Iranian government engage in advanced cyber activities that target U.S. infrastructure,¹⁵⁰ conduct cyber espionage,¹⁵¹ and steal data from U.S. persons, companies, and government agencies. For example, in 2018, a Federal grand jury returned an indictment against nine Iranians for stealing "more than 31 terabytes of documents and data from more than 140 American universities, 30 American companies, [and] five American government agencies," in part at the behest of the Iranian government.¹⁵²

In particular, Iranian hackers "have engaged in widespread theft of personal information . . . to track targets of interest to the Iranian regime"¹⁵³ and influence U.S. persons. During the 2020 U.S. elections, "Iranian cyber actors obtained or attempted to obtain U.S. voter information, sent threatening emails to voters, and disseminated disinformation about the election."¹⁵⁴ According to ODNI, those same Iranian actors have developed new cyber and influence techniques that Iran could deploy during the 2024 election cycle.¹⁵⁵ Iran-associated individuals also target U.S. persons for assassinations. For example, in 2023, a Federal grand jury returned an indictment against three individuals for plotting the murder of a U.S. citizen targeted by Iran for speaking out against the regime's human-rights abuses.¹⁵⁶ In

another example of Iran's exploitation of sensitive personal data, Iranian cyber threat actors engaged in "widespread theft" of personal information, "probably to support surveillance operations that enable Iran's human-rights abuses."¹⁵⁷ Iranian threat actors also "employed a years-long malware campaign" that targeted Iranian citizens, dissidents, journalists, and foreign organizations, including U.S.-based travel services companies that possess personal information on millions of travelers.¹⁵⁸

d. North Korea

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that North Korea has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. Among other conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons, it develops weapons of mass destruction;¹⁵⁹ commits human-rights abuses, including against U.S. persons;¹⁶⁰ evades U.S. sanctions;¹⁶¹ and conducts malicious cyber activities.

canadian-nationals-indicted-murder-hire-scheme [https://perma.cc/2DDC-Q7VQ]; Press Release, U.S. Dep't of Treas., *The United States and United Kingdom Target Iranian Transnational Assassinations Network* (Jan. 29, 2024), https://home.treasury.gov/news/press-releases/jy2052 [https://perma.cc/SE4A-7G4U].

¹⁵⁷ Press Release, U.S. Dep't of Treas., *Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities* (Sept. 9, 2022), https://home.treasury.gov/news/press-releases/jy0941 [https://perma.cc/98LB-5XYJ].

¹⁵⁸ Press Release, Fed. Bureau of Investg., *FBI Releases Cybersecurity Advisory on Previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies* (Sept. 17, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-releases-cybersecurity-advisory-on-previously-undisclosed-iranian-malware-used-to-monitor-dissidents-and-travel-and-telecommunications-companies [https://perma.cc/K8V5-LA6U].

¹⁵⁹ Press Statement, Antony J. Blinken, Sec'y, Dep't of State, *Designation of Two DPRK Individuals Supporting the DPRK's Unlawful Weapons of Mass Destruction and Missile Programs* (June 15, 2023), https://www.state.gov/designation-of-two-dprk-individuals-supporting-the-dprks-unlawful-weapons-of-mass-destruction-and-missile-programs/ [https://perma.cc/EV6L-3TCL].

¹⁶⁰ Press Release, U.S. Dep't of Treas., *Treasury Sanctions Over 40 Individuals and Entities Across Nine Countries Connected to Corruption and Human Rights Abuse* (Dec. 9, 2022), https://home.treasury.gov/news/press-releases/jy1155 [https://perma.cc/Y6ST-UVSP]; Bernd Debusmann Jr., *What Happened to US Citizens Like Otto Warmbier Detained in North Korea*, BBC News (July 18, 2023), https://www.bbc.com/news/world-us-canada-66236989 [https://perma.cc/MTL8-D425].

¹⁶¹ Press Statement, Antony J. Blinken, Sec'y, Dep't of State, *The Democratic People's Republic of Korea's Illicit Activities and Sanctions Evasion*

¹⁴³ ARCOS-1 USA, Inc., *supra* note 138, at 17–25.

¹⁴⁴ Press Statement, Matthew Miller, Spokesperson, Dep't of State, *Taking Actions to Combat the Iranian Regime's Transnational Repression* (Jan. 29, 2024), https://www.state.gov/taking-actions-to-combat-the-iranian-regimes-transnational-repression/ [https://perma.cc/VS2Z-VA32].

¹⁴⁵ Press Statement, Antony J. Blinken, Sec'y, Dep't of State, *Designating Iranian Persons Connected to Wrongful Detentions* (Sept. 18, 2023), https://www.state.gov/designating-iranian-persons-connected-to-wrongful-detentions/ [https://perma.cc/2CFT-YQWB].

¹⁴⁶ Press Statement, Matthew Miller, Spokesperson, Dep't of State, *Designating Persons Tied to Network Smuggling U.S. Technology to Central Bank of Iran* (Feb. 14, 2024), https://www.state.gov/designating-persons-tied-to-network-smuggling-u-s-technology-to-central-bank-of-iran/ [https://perma.cc/XD7P-JKNU].

¹⁴⁷ Press Release, U.S. Dep't of Treas., *Treasury Targets Sanctions Evasion Network Moving Billions for Iranian Regime* (Mar. 9, 2023), https://home.treasury.gov/news/press-releases/jy1330 [https://perma.cc/U8f2-NZ5Y]; Press Release, U.S. Dep't of Just., *Justice Department Announces Terrorism and Sanctions-Evasion Charges and Seizures Linked to Illicit, Billion-Dollar Global Oil Trafficking Network that Finances Iran's Islamic Revolutionary Guard Corps and Its Malign Activities* (Feb. 2, 2024), https://www.justice.gov/opa/pr/justice-department-announces-terrorism-and-sanctions-evasion-charges-and-seizures-linked [https://perma.cc/AXS4-63QM]; Indictment ¶ 2, *United States v. Shahriyari*, No. 24–cr–44 (S.D.N.Y. filed Jan. 25, 2024), ECF No. 1, https://www.justice.gov/opa/media/1336966/dl?inline [https://perma.cc/T664-3F6U].

¹⁴⁸ U.S. Dep't of Just., *supra* note 147.

¹⁴⁹ Off. of the Dir. of Nat'l Intel., *supra* note 86, at 20.

¹⁵⁰ Cybersec. & Infrastructure Sec. Agency, AA21–321A, *Cybersecurity Advisory: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities* (Nov. 19, 2021), https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-321a [https://perma.cc/9F3H-KY7F].

¹⁵¹ Cybersec. & Infrastructure Sec. Agency, *Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks* (Feb. 24, 2022), https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-055a [https://perma.cc/46ZR-MDVN].

¹⁵² Press Release, U.S. Dep't of Just., *Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps* (Mar. 23, 2018), https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary [https://perma.cc/F3BP-GJP7].

¹⁵³ Nat'l Intel. Council, *supra* note 5, at 4.

¹⁵⁴ Off. of the Dir. of Nat'l Intel., *supra* note 86, at 20.

¹⁵⁵ *Id.* at 20.

¹⁵⁶ Press Release, U.S. Dep't of Just., *Justice Department Announces Charges and New Arrest in Connection with Assassination Plot Directed from Iran* (Jan. 27, 2023), https://www.justice.gov/opa/pr/justice-department-announces-charges-and-new-arrest-connection-assassination-plot-directed [https://perma.cc/WW34-K9AH]; *Iran Sanctions*, U.S. Dep't State, https://www.state.gov/iran-sanctions/ [https://perma.cc/MH6Z-EFV7]; see also Press Release, U.S. Dep't of Just., *One Iranian and Two Canadian Nationals Indicted in Murder-for-Hire Scheme* (Jan. 29, 2024), https://www.justice.gov/opa/pr/one-iranian-and-two-

Regarding North Korea's malicious cyber activities, ODNI has concluded that North Korea's cyber program poses a "sophisticated and agile espionage, cybercrime, and attack threat," and that North Korea's cyber forces are "fully capable of achieving a variety of strategic objectives against diverse targets" in the United States.¹⁶²

Because North Korea has sophisticated cyber capabilities and attempts to obtain and exploit data on U.S. persons, it poses a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons. North Korea conducts cyber-enabled attacks and steals personal information to influence and target U.S. persons. For example, in 2014, North Korea-affiliated hackers attacked U.S. company Sony Pictures Entertainment in retaliation for an American film depicting the North Korean leader.¹⁶³ They stole proprietary information, personally identifiable information, and confidential communications; rendered Sony Pictures Entertainment's computers inoperable; and threatened the company's executives and employees.¹⁶⁴ North Korea and North Korea-affiliated hacker groups have repeatedly targeted military networks, critical infrastructure, and other corporate networks to "steal data and conduct disruptive and destructive cyber activities."¹⁶⁵ For example, in 2017, North Korea was responsible for a massive ransomware attack that infected hundreds of thousands of computers in more than 150 countries.¹⁶⁶ North Korea also "uses cyber capabilities to steal from financial institutions" and "generate revenue for its weapons of mass destruction and ballistic missile

programs."¹⁶⁷ North Korea's cyber actors use a range of tactics "to further their larger espionage and financial goals," including conducting spear phishing, abusing privileged access to networks while working as information technology contractors, exploiting software vulnerabilities, and attacking supply chains.¹⁶⁸ North Korea is also trying to use AI to further its offensive cyber capabilities.¹⁶⁹

e. Russia

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that Russia has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. According to ODNI, Russia poses "an enduring global cyber threat" and views "cyber disruptions as a foreign policy lever to shape other countries' decisions."¹⁷⁰ Russia has launched a "full-scale war against Ukraine;"¹⁷¹ commits human-rights abuses, including against U.S. persons;¹⁷² conducts malign influence

campaigns;¹⁷³ evades U.S. sanctions;¹⁷⁴ and conducts malicious cyber activities.¹⁷⁵ Russia "continuously refines and employs its espionage, influence, and attack capabilities" against a variety of targets, including critical infrastructure in the United States.¹⁷⁶ For example, in 2019, Russian intelligence services perpetrated a "broad-scope cyber espionage campaign" that exploited the SolarWinds Orion platform and compromised both United States Government agencies and private-sector organizations.¹⁷⁷ The campaign gave Russian intelligence "the ability to spy on or potentially disrupt more than 16,000 computer systems worldwide."¹⁷⁸ Russian intelligence ultimately used the attack to target United States Government agencies and employees for espionage.¹⁷⁹

Because Russia has advanced cyber capabilities and aggressively seeks to obtain and exploit data on U.S. persons, including to conduct influence campaigns in the United States, it poses a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons. Russia engages in the large-scale theft of sensitive personal data and is "increasing [its] ability to analyze and manipulate large quantities of personal information," enabling it "to more effectively target and influence, or coerce, individuals and groups in the

(May 6, 2022), <https://www.state.gov/the-democratic-peoples-republic-of-koreas-illicit-activities-and-sanctions-evasion/> [https://perma.cc/LQ9B-9Z22].

¹⁶² Off. of the Dir. of Nat'l Intel., *supra* note 86, at 22.

¹⁶³ Press Release, U.S. Dep't of Just., *North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions* (Sept. 6, 2018), <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and> [https://perma.cc/WXQ3-YMQA].

¹⁶⁴ Press Release, Fed. Bureau of Investig., *Update on Sony Investigation* (Dec. 19, 2014), <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation> [https://perma.cc/5H4K-5E5F].

¹⁶⁵ Cybersec. & Infrastructure Sec. Agency, *Guidance on the North Korean Cyber Threat* (June 23, 2020), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a> [https://perma.cc/X8CJ-TAYV].

¹⁶⁶ U.S. Dep't of Just., *supra* note 163.

¹⁶⁷ Cybersec. & Infrastructure Sec. Agency, *supra* note 165.

¹⁶⁸ Off. of the Dir. of Nat'l Intel., *North Korean Tactics, Techniques and Procedures for Revenue Generation* (July 2023), <https://www.dni.gov/files/CTIC/documents/products/North-Korean-TTPs-for-Revenue-Generation.pdf> [https://perma.cc/Y949-JJW4]; Press Release, U.S. Dep't of Just., *Justice Department Announces Court-Authorized Action to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea Information Technology Workers* (Oct. 18, 2023), <https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation> [https://perma.cc/3JHY-UH5K].

¹⁶⁹ Anne Neuberger, Deputy Nat'l Sec. Advisor for Cyber & Emerging Tech., Nat'l Sec. Council, U.S. Dep't of State, *Digital Press Briefing* (Oct. 18, 2023), <https://www.state.gov/digital-press-briefing-with-anne-neuberger-deputy-national-security-advisor-for-cyber-and-emerging-technologies/> [https://perma.cc/GK88-FW8H].

¹⁷⁰ Off. of the Dir. of Nat'l Intel., *supra* note 86, at 16; see also Press Statement, The White House, *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government* (Apr. 15, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/> [https://perma.cc/MD56-GD27]; Nat'l Counterintel. & Sec. Ctr., *SolarWinds Orion Software Supply Chain Attack* (Aug. 19, 2021), <https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf> [https://perma.cc/TS3M-MQQ7].

¹⁷¹ Press Statement, Antony J. Blinken, Sec'y, Dep't of State, *Responding to Two Years of Russia's Full-Scale War Against Ukraine and Aleksey Navalny's Death* (Feb. 23, 2024), <https://www.state.gov/responding-to-two-years-of-russias-full-scale-war-against-ukraine-and-aleksey-navalny-death/> [https://perma.cc/K3SL-LHFF].

¹⁷² Press Statement, Vedant Patel, Principal Deputy Spokesperson, Dep't of State, *Russia's Wrongful Detention of Journalist Evan Gershkovich* (Apr. 10, 2023), <https://www.state.gov/russias>

wrongful-detention-of-journalist-evan-gershkovich/ [https://perma.cc/XE2R-93RE].

¹⁷³ Press Release, U.S. Dep't of Treas., *Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts* (Mar. 20, 2024), <https://home.treasury.gov/news/press-releases/jy2195> [https://perma.cc/TB2X-YRPN]; Press Release, U.S. Dep't of Treas., *Treasury Targets the Kremlin's Continued Malign Political Influence Operations in the U.S. and Globally* (July 29, 2022), <https://home.treasury.gov/news/press-releases/jy0899> [https://perma.cc/FXN8-J748].

¹⁷⁴ Press Release, U.S. Dep't of Treas., *Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War* (Mar. 31, 2022), <https://home.treasury.gov/news/press-releases/jy0692> [https://perma.cc/ERD6-ARTE].

¹⁷⁵ Press Statement, Matthew Miller, Spokesperson, Dep't of State, *U.S. Takes Action to Further Disrupt Russian Cyber Activities* (Dec. 7, 2023), <https://www.state.gov/u-s-takes-action-to-further-disrupt-russian-cyber-activities/> [https://perma.cc/AW9F-E8BP].

¹⁷⁶ Off. of the Dir. of Nat'l Intel., *supra* note 86, at 16.

¹⁷⁷ White House, *supra* note 170.

¹⁷⁸ *Id.*

¹⁷⁹ *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response* (infographic), U.S. Gov't Accountability Off. (Apr. 22, 2021), <https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic> [https://perma.cc/3A2V-6S59].

United States.”¹⁸⁰ For example, in 2013, Russian intelligence services sponsored the theft of information associated with at least 500 million accounts from U.S. web services company Yahoo!¹⁸¹ and used some of that stolen information to obtain unauthorized access to the email accounts of United States Government officials, among others.¹⁸² In 2020, Russian cyber operations targeted and compromised U.S. State and local government networks and exfiltrated some voter data.¹⁸³ In another example, in 2023, a Federal grand jury returned an indictment against two Russian individuals for obtaining unauthorized access to the computers and email accounts of current and former United States Government employees and stealing intelligence related to defense, security policies, and nuclear energy technology from the victims’ accounts.¹⁸⁴ In 2024, Russian intelligence services used compromised routers to conduct “spearphishing and similar credential harvesting campaigns against targets of intelligence interest to the Russian government, such as U.S. and foreign governments and military, security, and corporate organizations.”¹⁸⁵

Russia also has a legal regime that gives it the capability to covertly access and exploit data through companies subject to its jurisdiction. As the Department of Commerce has explained, “Russian laws compel companies subject to Russian jurisdiction to cooperate with Russian intelligence and law enforcement efforts, to include requests from the Russian Federal

Security Service (“FSB”).”¹⁸⁶ These laws include the following:

- Federal Law No. 40–FZ of April 3, 1995, “On the Federal Security Service,” “requires FSB bodies to carry out their activities in collaboration with various entities in Russia” and places private enterprises “under a legal obligation to assist FSB bodies in the execution of the duties assigned to FSB bodies,” including intelligence and counterintelligence activities.¹⁸⁷

- Federal Law No. 144–EZ of August 12, 1995 (as amended), “On Operational-Investigative Activity,” requires persons subject to Russian jurisdiction to “assist the FSB with operational-investigative activities undertaken in the performance of FSB duties, such as by installing equipment supplied by the FSB for use in obtaining information stored on computers.”¹⁸⁸ This law “makes it clear that, as a general rule, operational-investigative activities may be carried out against anyone anywhere” and “makes it clear that operational-search activities include obtaining computer information.”¹⁸⁹

- Federal Law No. 149–FZ of July 27, 2006, “On Information, Information Technologies, and Protection of Information,” imposes several “obligations on any entity that qualifies as ‘an organizer of the dissemination of information on the internet,’” which is broadly defined to include any “person who carries out activities to ensure the operation of information systems and/or programs for electronic computers that are designed and/or used to receive, transmit, deliver and/or process electronic messages of users of the internet.”¹⁹⁰ These obligations include giving the FSB and other Russian agencies in the field of security “the information necessary to decode” encrypted data.¹⁹¹

In short, persons subject to Russia’s jurisdiction must “assist the FSB in its counterintelligence and intelligence functions,” which “includes a duty to assist the FSB in operational-

investigative activity, in support of FSB counterintelligence and intelligence functions” such as “collecting information from U.S. computers,” “with no need for the FSB to have obtained a court order.”¹⁹²

Finally, Russia also poses a “serious foreign influence threat because of its wide-ranging efforts to . . . sow domestic discord, including among voters inside the United States.”¹⁹³ In July 2018, a Federal grand jury returned an indictment against Russian intelligence officers after they conducted a spear phishing campaign against volunteers and employees of a presidential campaign and political committees.¹⁹⁴ The actors hacked into computers, stole emails, covertly monitored the computer activity of campaign employees, and released the hacked information to the public in an attempt to interfere with the 2016 U.S. presidential election.¹⁹⁵

f. Venezuela

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that Venezuela has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. Among other conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons, Venezuela commits human-rights abuses, including against U.S. persons;¹⁹⁶ evades U.S. sanctions;¹⁹⁷ has concerning relationships with other

¹⁹² *Id.* ¶ 30.

¹⁹³ Off. of the Dir. of Nat’l Intel., *supra* note 86, at 17.

¹⁹⁴ Press Release, U.S. Dep’t of Just., *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election* (July 13, 2018), <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-to-2016-election> [https://perma.cc/RG2P-SJLQ]; Indictment ¶¶ 2–5, *United States v. Netyksho*, No. 18–cr–215 (D.D.C. filed July 13, 2018).

¹⁹⁵ U.S. Dep’t of Just., *supra* note 194; Indictment ¶¶ 2–5, *Netyksho*, No. 8–cr–215.

¹⁹⁶ U.S. Dep’t of State, *2022 Country Reports on Human Rights Practices: Venezuela* (2022), https://www.state.gov/wp-content/uploads/2023/02/415610_VENEZUELA-2022-HUMAN-RIGHTS-REPORT.pdf [https://perma.cc/7TM9-P87S]; see also, e.g., E.O. 13692, 80 FR 12747 (Mar. 8, 2015).

¹⁹⁷ Press Release, U.S. Att’y’s Off. DC, U.S. Dep’t of Just., *Largest U.S. Seizure of Iranian Fuel from Four Tankers* (Aug. 14, 2020), <https://www.justice.gov/usao-dc/pr/largest-us-seizure-iranian-fuel-four-tankers> [https://perma.cc/66EF-42CD]; Fin. Crimes Enft Network, U.S. Dep’t of Treas., FIN–2019–A002, *Updated Advisory on Widespread Public Corruption in Venezuela*, 8 (May 3, 2019), <https://www.fincen.gov/sites/default/files/advisory/2019-05-03/Venezuela%20Advisory%20FINAL%20508.pdf> [https://perma.cc/X5VL-HH69].

¹⁸⁰ Nat’l Intel. Council, *supra* note 5, at 3.

¹⁸¹ Press Release, U.S. Dep’t of Just., *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts* (Mar. 15, 2017), <https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions> [https://perma.cc/44UK-XM7P].

¹⁸² U.S. Dep’t of Just., *supra* note 181; Indictment ¶ 34, *United States v. Dokuchaev*, No. 17–cr–103 (N.D. Cal. filed Feb. 28, 2017).

¹⁸³ Nat’l Intel. Council, ICA 2020–00078D, *Intelligence Community Assessment on Foreign Threats to the 2020 US Federal Elections* 3 (Mar. 10, 2021), <https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf> [https://perma.cc/R8LM-KEUX].

¹⁸⁴ Indictment ¶¶ 3–5, *United States v. Aleksandrovic*, No. 23–cr–447 (N.D. Cal. filed Dec. 5, 2023).

¹⁸⁵ Press Release, U.S. Dep’t of Just., *Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate of the General Staff (GRU)* (Feb. 15, 2024), <https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian> [https://perma.cc/8M8Z-C3SM].

¹⁸⁶ Kaspersky Lab, Inc., *supra* note 20, 89 FR 52435.

¹⁸⁷ Report of Peter B. Maggs to the U.S. Dep’t of Homeland Sec. ¶¶ 14–18 (Dec. 2, 2017), <https://www.internetgovernance.org/wp-content/uploads/12-7-Exhibit-AR-Part-6-Maggs-report.pdf> [https://perma.cc/US4P-VMCP] (hereinafter “Maggs Report”) (supporting the Department of Homeland Security’s Dec. 4, 2017 Final Decision on Binding Operational Directive 17–01, Removal of Kaspersky-Branded Products).

¹⁸⁸ Kaspersky Lab, Inc., *supra* note 20, 89 FR 52435 n.13; Maggs Report, *supra* note 187, ¶¶ 24–25.

¹⁸⁹ Maggs Report, *supra* note 187, ¶¶ 24–29.

¹⁹⁰ *Id.* ¶ 21.

¹⁹¹ *Id.* ¶¶ 13(f), 31.

countries of concern;¹⁹⁸ and fosters widespread corruption.¹⁹⁹

Because Venezuela exploits its demonstrated and systematic relationships with other countries of concern to degrade U.S. national security; aggressively surveils its own population to target perceived government critiques, including with the help of other countries of concern; and, according to credible reports, commits human-rights abuses, including against U.S. citizens, Venezuela's access to government-related data or Americans' bulk U.S. sensitive personal data poses a significant risk to the national security of the United States and the security and safety of U.S. persons. Regarding Venezuela's human-rights abuses, Venezuela surveils its domestic population through telecommunications providers to target perceived opponents, including with the help of other countries of concern.²⁰⁰ Venezuela's misuse of private telecommunications capabilities for expansive surveillance poses risks to U.S. persons, as the regime has the capability to access data on U.S. persons in Venezuela. For example, in 2021, a report by Spanish telecommunications company Telefonica revealed that Venezuela monitored the communications of nearly 1.5 million of its users, which represents over 20 percent of Telefonica's Venezuela-based customers.²⁰¹ In addition to surveillance, there are credible reports that Venezuela perpetrates extensive human-rights abuses, such as torture, extrajudicial killings, and enforced disappearances. Venezuelan security forces detain individuals, including U.S. citizens, for long periods without due process.²⁰² According to the State

Department, the United States Government is not generally notified of the detention of U.S. citizens in Venezuela or granted access to U.S. citizen prisoners in Venezuela.²⁰³

Venezuela maintains close relationships with other countries of concern that, as described in part IV.D of this preamble, possess sophisticated surveillance capabilities and pose a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data. Given the nature of these relationships, Venezuela might use technology provided by these countries of concern to obtain access to government-related data or bulk U.S. sensitive personal data, or share any access to government-related data or bulk U.S. sensitive personal data with these countries of concern. For example, Venezuela uses equipment provided by Chinese technology company Zhongxing Telecommunication Equipment ("ZTE") Corporation, which the FCC has designated a national security threat to the U.S. communications network and supply chain, to monitor Venezuelan citizens' social, political, and economic activities.²⁰⁴ The company has provided Venezuela with identity cards, referred to as "carnet de la patria" or "fatherland cards," that the regime can use to track citizen behavior.²⁰⁵ Additionally, Venezuelan and Russian state-owned companies jointly own Evrofinance Mosnarbank, a bank that has financed Venezuela's efforts to use digital currencies to circumvent U.S. financial sanctions.²⁰⁶ Evrofinance Mosnarbank also provides financial support to Petroleos de Venezuela, a Venezuelan state-owned oil company that has been used to embezzle and launder billions of dollars.²⁰⁷ Venezuela also has concerning military and intelligence ties with other countries of concern. For example, Russia provides military

support to Venezuela.²⁰⁸ Cuba provides training to Venezuelan intelligence and military personnel, and the two nations support each other's intelligence operations.²⁰⁹

E. Subpart G—Covered Persons

1. Section 202.211—Covered Person

The proposed rule identifies a "covered person" as an individual or entity that falls into one of the classes of covered persons or that the Attorney General has designated as a covered person. An entity is a covered person if it is a foreign person that: (1) is 50 percent or more owned, directly or indirectly, by a country of concern; (2) is organized or chartered under the laws of a country of concern; or (3) has its principal place of business in a country of concern. An entity is also a covered person if it is a foreign person that is 50-percent or more owned, directly or indirectly, by a covered person. Any foreign individual who is an employee or a contractor of such an entity or of the country of concern itself is also a covered person. Any foreign person who is primarily a resident in the territorial jurisdiction of a country of concern is also a covered person.

The proposed rule would not categorically treat citizens of countries of concern located in third countries (*i.e.*, not located in the United States and not primarily resident in a country of concern) as covered persons. Instead, it treats only a subset of country of concern citizens in third countries categorically as covered persons: those working for the government of a country of concern or for an entity that is a covered person. All other country of concern citizens located in third countries would not qualify as covered persons except to the extent that the Attorney General designates them.

Some commenters believed that it would be difficult for U.S. persons

¹⁹⁸ U.S. Dep't of Just., *supra* note 197; Off. of the Dir. of Nat'l Intel., *supra* note 86, at 29.

¹⁹⁹ Press Release, U.S. Dep't of Just., *Former Venezuelan National Treasurer and Her Husband Sentenced in Money Laundering and International Bribery Scheme* (Apr. 19, 2023), <https://www.justice.gov/opa/pr/former-venezuelan-national-treasurer-and-her-husband-sentenced-money-laundering-and> [https://perma.cc/AU8N-C9UD]; Fin. Crimes Enf't Network, *supra* note 197, at 7.

²⁰⁰ U.S. Dep't of State, *supra* note 196, at 19; Maria Luisa Paul, *Venezuela Tapped 1.5 Million Phone Lines. It's Just the Start, Experts Warn.*, Wash. Post (June 28, 2022), <https://www.washingtonpost.com/nation/2022/06/28/telefonica-wiretapping-venezuela-phone/> [https://perma.cc/T8YV-A9TW].

²⁰¹ U.S. Dep't of State, *supra* note 196, at 19; Paul, *supra* note 200.

²⁰² U.S. Dep't of State, *Venezuela Travel Advisory* (May 13, 2024), <https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories/venezuela-travel-advisory.html> [https://perma.cc/5F26-GNRM]; Clare Ribando Seelke et al., Cong. Rsch. Serv., R44841, *Venezuela: Background and*

U.S. Relations 7 (Dec. 6, 2022), <https://crsreports.congress.gov/product/pdf/R/R44841> [https://perma.cc/T8ZW-4RRA].

²⁰³ U.S. Dep't of State, *supra* note 196.

²⁰⁴ FCC, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs—ZTE Designation, 35 FCC Rcd. 6633 (2020), <https://docs.fcc.gov/public/attachments/DA-20-691A1.pdf> [https://perma.cc/MK3W-SYEN].

²⁰⁵ Angus Berwick, *How ZTE Helps Venezuela Create China-Style Social Control*, Reuters (Nov. 14, 2018), <https://www.reuters.com/investigates/special-report/venezuela-zte/> [https://perma.cc/66X9-FBWD]; see also U.S. Dep't of State, *supra* note 196.

²⁰⁶ Fin. Crimes Enf't Network, *supra* note 197, at 4–5.

²⁰⁷ *Id.*; Press Release, U.S. Dep't of Treas., *Treasury Sanctions Venezuela's State-Owned Oil Company Petroleos de Venezuela, S.A.* (Jan. 28, 2019), <https://home.treasury.gov/news/press-releases/sm594> [https://perma.cc/375J-DR47].

²⁰⁸ Regina Garcia Cano, *Venezuela's Leader Pledges Military Cooperation with Russia*, AP News (Feb. 16, 2022), <https://apnews.com/article/europe-russia-venezuela-vladimir-putin-south-america-fc9e01895f52f8d9f52e501a93b2f089> [https://perma.cc/M59U-SRUU]; Russia in the Western Hemisphere: Assessing Putin's Malign Influence in Latin America and the Caribbean: Hearing Before the H. Foreign Affs. Subcomm. on W. Hemisphere, Civilian Sec., Migration, & Int'l Econ. Pol'y, 117th Cong. 1–3 (2022) (statement of Evan Ellis, Senior Associate, Ctr. for Strategic & Int'l Stud.), https://csis-website-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/ts202072_Ellis.pdf [https://perma.cc/K9VG-ZFW2].

²⁰⁹ Moises Rendon & Claudia Fernandez, Ctr. for Strategic & Int'l Stud., *The Fabulous Five: How Foreign Actors Prop Up the Maduro Regime in Venezuela* 7 (2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201019_Rendon_Venezuela_Foreign_Actors.pdf [https://perma.cc/39AG-LAXX].

subject to the proposed rule to determine whether entities are 50 percent or more owned by countries of concern, particularly where the foreign companies are publicly traded companies. However, this provision is not unique to the proposed rule. It is similar to sanctions regulations issued by the Office of Foreign Assets Control (“OFAC”) within the Department of the Treasury. Such regulations treat any entity owned in the aggregate, directly or indirectly, 50-percent or more by one or more blocked persons as itself a blocked person, regardless of whether the entity itself is designated pursuant to an Executive Order or otherwise identified on OFAC’s Specially Designated Nationals and Blocked Persons List.²¹⁰ The proposed rule also uses higher ownership thresholds than some regulatory regimes, such as those related to anti-money laundering, which generally require certain companies to identify beneficial owners with 25 percent or more (and, in some cases, 10 percent or more) direct or indirect legal interest in an entity and to collect, verify, and report specific information about them.²¹¹ As other commenters pointed out, businesses and third-party service providers have developed tools and services to assist with screening and due diligence based on corporate ownership in the sanctions, anti-money laundering, and other regulatory contexts. Consequently, the proposed rule adopts the approach described in the ANPRM without change.

One commenter recommended that the Department clarify how the proposed rule would apply to companies headquartered outside a country of concern but with business operations in a country of concern. The proposed rule maintains the framework described in the ANPRM without change, and the Department has provided some additional examples in the proposed rule to demonstrate how the proposed rule treats foreign branches and subsidiaries located in countries of concern. See § 202.256(b)(5)(8). The proposed rule also exempts corporate group transactions that are ordinarily incident to and part of administrative or ancillary business operations, such as human resources, including between U.S.

entities and their foreign subsidiaries or affiliates.

Several commenters suggested that the Department rely solely on designations and adopt an exclusively list-based approach to the identification of covered persons (similar to OFAC’s Specially Designated Nationals and Blocked Persons List or the Bureau of Industry and Security’s (“BIS”) Entity List) rather than applying the prohibitions and restrictions to categories of covered persons supplemented by a non-exhaustive list. The Department declines to adopt the exclusively list-based approach. Such an approach would be inconsistent with the Order, as well as with the national security risk associated with country of concern access to government-related data or bulk U.S. sensitive personal data. Specifically, the national security risk identified in the Order exists with respect to any entity that is subject to the ownership, direction, jurisdiction, or control of a country of concern due to the fact that each of the listed countries of concern in the proposed rule have legal or political systems that allow the countries to obtain sensitive personal data (and access to such data) from persons subject to their ownership, direction, jurisdiction, or control without due process or judicial redress.²¹² That risk exists with respect

to any person that is meaningfully subject to their ownership, direction, jurisdiction, or control—not only to specific entities designated on a case-by-case basis. Entities that are meaningfully subject to the ownership, direction, jurisdiction, or control of a country of concern are, as the FBI has described, hybrid commercial threats. As the FBI has explained, “[h]ybrid [c]ommercial [t]hreats are businesses whose legitimate commercial activity can facilitate foreign government access to U.S. data, critical infrastructure, and emerging technologies that enable adversaries to conduct espionage, technology transfer, data collection, and other disruptive activities under the guise of an otherwise legitimate commercial activity.”²¹³

As such, trying to apply a list-based approach would be insufficient to mitigate the national security risk identified in the Order and the proposed rule. The categories of covered persons defined in the Order and defined further in the proposed rule identify categories of persons that are meaningfully subject to the ownership, direction, jurisdiction of a country of concern, or control of a country of concern or covered person, and thus present this risk. Processes like those used by OFAC to add blocked persons to the Specially Designated Nationals and Blocked Persons List or by BIS to add entities to the Entity List, which are generally based on a particularized inquiry into whether the target meets the applicable legal criteria for designation,²¹⁴ would thus be

²¹⁰ Nat’l Counterintel. & Sec. Ctr., *supra* note 83, at 1; Justin Sherman, *Russia Is Weaponizing Its Data Laws Against Foreign Organizations*, Brookings Inst. (Sept. 27, 2022), <https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/> [<https://perma.cc/ATU2-SU3G>]; U.S. Dep’t of State, *supra* note 196, at 19; see generally *Freedom in the World 2024: North Korea*, Freedom House, <https://freedomhouse.org/country/north-korea/freedom-world/2024> [<https://perma.cc/5PAA-YMQ4>]; *Freedom on the Net 2022: Cuba*, Freedom House, <https://freedomhouse.org/country/cuba/freedom-net/2022> [<https://perma.cc/FFF6-ALCB>]; Data Security Business Advisory, *Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People’s Republic of China*, U.S. Dep’t of Homeland Sec. (Dec. 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf [<https://perma.cc/B6XM-8G9V>]; Anna Borshchevskaya, ‘Brave New World’: Russia’s New Anti-Terrorism Legislation, Wash. Inst. (July 8, 2016), <https://www.washingtoninstitute.org/policy-analysis/brave-new-world-russias-new-anti-terrorism-legislation> [<https://perma.cc/2XXZ-UTC7>]; *Combating the Iranian Cyber Threat: Republic at the Center of Cyber Crime Charges in Three Cases*, Fed. Bureau of Investig. (Sept. 18, 2020), <https://www.fbi.gov/news/stories/iran-at-center-of-cyber-crime-charges-in-three-cases-091820> [<https://perma.cc/DYL5-WXUC>]; Amelia Williams, *Cuba: New data protection law—what you need to know*, Data Guidance (Sept. 2022), <https://www.dataguidance.com/opinion/cuba-new-data-protection-law-what-you-need-know> [<https://perma.cc/JH83-6P7S>]; Joanna Robin, *Maduro regime doubles down on censorship and repression in lead-up to Venezuelan election*, ICIJ (July 24, 2024), <https://www.icij.org/inside-icij/2024/07/maduro-regime-doubles-down-on-censorship-and-repression-in-lead-up-to-venezuelan-election/>

repression-in-lead-up-to-venezuelan-election/ [<https://perma.cc/6TBD-4J28>]; U.S. Dep’t of State, Bureau of Democracy, H.R. and Lab., 2021 Country Reports on Human Rights Practices: North Korea (2021), https://www.state.gov/wp-content/uploads/2022/03/313615_KOREA-DEM-REP-2021-HUMAN-RIGHTS-REPORT.pdf [<https://perma.cc/GF5Z-25UG>]; *Freedom on the Net 2024: Iran*, Freedom House, at C4 and C6, <https://freedomhouse.org/country/iran/freedom-net/2024> [<https://perma.cc/2QKR-9E7C>].

²¹³ *In Camera*, *Ex Parte* Classified Decl. of Kevin Vorndran, Assistant Dir., Counterintel. Div., Fed. Bureau of Invest., Doc. No. 2066897 at Gov’t App. 33 ¶ 6, *TikTok Inc. v. Garland*, Case Nos. 24–1113, 24–1130, 24–1183 (D.C. Cir. July 26, 2024) (publicly filed redacted version).

²¹⁴ See 15 CFR 744.16 (1996) (“The Entity List (supplement No. 4 to [part 744]) identifies persons . . . reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States.”); see also, 31 CFR 589.201(a) (2022) (blocking the property of “any person determined by the Secretary of the Treasury” to, among other things, “be responsible for or complicit in, or to have engaged in, directly or indirectly,” actions or policies “that undermine democratic processes or institutions in Ukraine” or “that threaten the peace, security, stability, sovereignty, or territorial integrity of Ukraine” or “[m]isappropriation of state assets of Ukraine or of an economically significant entity in Ukraine”).

²¹⁰ See generally OFAC, U.S. Dep’t of Treas., *Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked* (Aug. 13, 2014), <https://ofac.treasury.gov/media/6186/download?inline> [<https://perma.cc/Q87V-VZJQ>].

²¹¹ See generally *Beneficial Ownership Information: Frequently Asked Questions*, Fin. Crimes Enf’t Network, <https://www.fincen.gov/boi-faqs> [<https://perma.cc/Z7KQ-PN79>].

insufficient by themselves to address the national security risk identified in the Order. An exclusively list-based approach could present considerable compliance and enforcement challenges. It also poses potential evasion risks, similar to those encountered by OFAC, and circumvention threats that could compromise national security. The Department has determined not to exclusively implement a list-based program to mitigate the risk that listed entities, such as corporations, would rename or reorganize themselves in a manner that avoids being subject to the framework. Therefore, the proposed rule adopts the approach described in the ANPRM without change.

One commenter suggested that the Department should not treat trustworthy entities located in countries of concern as covered persons. The Department declines to do so, and the proposed rule retains the framework described in the ANPRM without change. Regardless of the trustworthiness of entities, as explained in part IV.E.1 of this preamble, countries of concern have the legal authority or political systems to force, coerce, or influence entities in their jurisdictions to share their data and access with the government.²¹⁵

One commenter urged the Department to narrow the definition of “covered persons” to exclude individuals who are temporarily in the United States but are otherwise residents of a country of concern. The proposed rule adopts the approach described in the ANPRM without change. As described in the ANPRM, including its Example 33, anyone in the United States (including temporarily in the United States) would be considered a U.S. person, and no U.S. persons (including those temporarily in the United States) would be categorically treated as covered persons.²¹⁶ A U.S. person (including a temporary traveler to the United States) would be a covered person only if they had been designated by the Department. The proposed rule adopts this proposal unchanged from the ANPRM.

Two related commenters expressed identical concerns that the definition of “covered persons” would require companies to discriminate based on nationality or race, particularly with respect to employees who are primarily resident in countries of concern. No change was made in response to these comments. As the Order makes clear, status as a covered person does not depend on the nationality or race of an individual, and the Order and proposed

rule are directed at persons of any nationality or race who are subject to the ownership, direction, jurisdiction, or control of a country of concern. The definition of “covered person” categorically includes any foreign person that is primarily resident in a country of concern, regardless of their nationality or race. Likewise, the definition of “covered person” categorically includes any foreign person abroad who is an employee or contractor of a country of concern or a covered person that is an entity, regardless of their nationality or race. Similarly, the Department’s authority to designate a specific individual as a “covered person” turns on a determination that the individual is subject to the control, jurisdiction, or direction of a country of concern, or is acting on behalf of or purporting to act on behalf of a country of concern or covered person, or has knowingly caused or directed a violation of the proposed rule. The definition of “U.S. person” is also not dependent on a person’s nationality or race; it includes, for example, any person in the United States and any U.S. citizen or lawful permanent resident. For example, under the proposed rule, a country of concern citizen located in the United States is a U.S. person (unless individually designated). As a result, a U.S. person of any particular race or nationality would not be categorically treated as a covered person, and the only circumstance in which a U.S. person would be treated as a covered person is by individual designation. Consequently, the proposed rule adopts the approach described in the ANPRM without change.

Several commenters sought clarification that any U.S. subsidiary of a covered person is considered a U.S. person for purposes of these regulations. The proposed rule would not treat any U.S. person, including a U.S. subsidiary of a covered person, as a covered person unless the Department has designated the U.S. subsidiary as a covered person pursuant to the process described in the proposed rule. No U.S. person, including the U.S. subsidiary of a covered person, would be categorically treated as a covered person under the proposed rule. The proposed rule includes additional examples highlighting the differences in treatment between a U.S. subsidiary and its foreign owner, as well as between U.S. companies and their foreign branches.

2. Section 202.701—Designation of Covered Persons

The proposed rule provides for the Attorney General to publicly designate a

person, whether an individual or entity, as a covered person with whom U.S. persons may not knowingly engage in a prohibited transaction, or a restricted transaction that fails to comply with the requirements of subpart D of the proposed rule, except as otherwise authorized under the proposed rule. The Department intends generally to model this process on the processes for designation under the various sanctions lists maintained by OFAC. Inclusion on the Department’s Covered Persons List would have no effect on a person’s inclusion on other United States Government designation lists, including lists maintained by OFAC.

The Department expects that, in many cases, designation will be unnecessary because a person will be automatically deemed a covered person by operation of the definition of “covered person” discussed in part IV.E.1 of this preamble. For example, an entity that is majority-owned by a country of concern would be a covered person by definition, regardless of whether the entity itself is designated by the Attorney General and included on the Department’s Covered Persons List. Designation is not necessary in that circumstance and, except as otherwise authorized under the proposed rule, a U.S. person would be prohibited from knowingly engaging in a prohibited transaction, or a restricted transaction that fails to comply with the requirements of subpart D, with such an entity.

Even in these circumstances, however, the Attorney General may nonetheless designate such an entity and identify that entity as a covered person in the **Federal Register** and on a Department website. Such designation may serve to provide broader notice to U.S. persons that the entity is a covered person under the Order and the regulations. For example, the definition of “covered person” includes entities that are majority-owned directly or indirectly by a country of concern. In some circumstances, indirect ownership may not be readily apparent, and Attorney General designation, published in the **Federal Register**, will provide notice that the entity is a covered person. Even in the case of instances in which the covered person status of an entity is clear—such as companies that are openly organized or chartered under the laws of a country of concern or that have their principal place of business in a country of concern—designation and publication in the **Federal Register** may facilitate compliance with the prohibitions and restrictions under the Order and the regulations. Importantly, however, the public list would not

²¹⁵ See sources cited *infra* note 212.

²¹⁶ 89 FR 15790–91.

exhaustively include all covered persons, as any person that satisfies the criteria of the relevant definitions will be considered a covered person under the proposed rule, regardless of whether the person is also specifically identified on the public list. Under the proposed rule, for example, every company with its principal place of business in any country of concern is a “covered person”; the Department does not intend to individually designate all such companies.

The proposed rule also authorizes the Department to designate as covered persons other individuals or entities that are not already captured by other elements of the definition. This process is modeled after other IEEPA-related designation processes and contemplates designation based on interagency consultation and consideration of any relevant sources of information (which may include classified information). Under the proposed rule, and consistent with the Order, the Department could designate as a covered person any person that is owned or controlled by or subject to the jurisdiction or direction of a country of concern, is acting on behalf of or purporting to act on behalf of a country of concern or other covered person, or is knowingly causing or directing a violation of these regulations. For example, individual citizens of a country of concern primarily residing in a third country are not generally considered to be covered persons. In specific cases, however, covered data transactions with such individuals may present an unacceptable national security risk because, for example, the individual may be subject to the direction of a country of concern. The proposed rule provides for the Attorney General to designate such an individual—or any other individual or entity that satisfies the substantive criteria in the proposed rule—as a covered person.

Under the proposed rule, designation as a covered person is effective upon the Department’s announcement; a U.S. person with actual knowledge of the designated person’s status would be prohibited from knowingly engaging in a covered data transaction with that person (except as otherwise authorized under the proposed rule). After publication in the **Federal Register**, the Department would infer knowledge of the designated person’s status on the part of any U.S. person engaging in a covered data transaction with that person. As in the context of asset flight, designations must be immediately effective to prohibit the irreversible transfer of regulated data—and the attendant risk to national security—once

a designation is announced. If there were delay, unscrupulous actors could rush to complete transactions that would soon become prohibited, thus inviting precisely the national security risk that the Order, and the designation, is intended to mitigate. Like the OFAC processes on which it is modeled, the proposed rule includes a mechanism for a person designated as a covered person to seek administrative reconsideration of the designation or removal from the list of designated covered persons on the basis of changed circumstances.

Designation as a covered person reflects the risk to national security that attaches to the designated person’s relationship—whether voluntary or involuntary—with a country of concern. The definition of “covered person,” for example, includes any foreign person who is primarily resident in the territorial jurisdiction of a country of concern or any person who is an employee or contractor of an entity with its principal place of business in a country of concern. As a general matter, the national security risk from concluding a covered data transaction with such persons arises primarily from the potential actions of the government of the country of concern in relation to that person, not from the intent or personal characteristics of the individual.

A few commenters expressed concern that it will be difficult for businesses subject to the proposed rule to identify entities controlled by or subject to the jurisdiction of countries of concern. However, neither the ANPRM nor the proposed rule would require companies to determine whether entities are subject to the control or jurisdiction of a country of concern. Whether an entity is controlled by or subject to the jurisdiction or direction of a country of concern is part of the criteria applied by the Attorney General in designating individuals and entities as covered persons; it is not a standard to be applied by the private sector. If the Attorney General determines that an individual or entity meets the criteria for designation, the Attorney General will specifically and publicly designate that person, as addressed in the foregoing discussion, and the private sector can screen counterparties against that public list. For entities not so designated, the private sector need only consult the four other categories of covered persons discussed in part IV.E.1 of this preamble; the private sector need not conduct any inquiry into whether such an entity is controlled by or subject to the jurisdiction or direction of a country of concern. Therefore, the proposed rule adopts the approach

described in the ANPRM without change.

F. Subpart H—Licensing

The Order authorizes the Attorney General, in concurrence with the Departments of State, Commerce, and Homeland Security and in consultation with other relevant agencies, to issue (including to modify or rescind) licenses authorizing a transaction that would otherwise be a prohibited transaction or a restricted transaction. The proposed rule implements this provision of the Order by providing processes for regulated parties to seek, and for the Attorney General to issue, general and specific licenses. The Department anticipates that licenses will be issued only in rare circumstances as the Attorney General deems appropriate.

1. Section 202.801—General Licenses

General licenses would be published in the **Federal Register** and could be relied upon by all relevant parties affected by a particular element of these regulations. As deemed appropriate, the Attorney General, in concurrence and consultation with other departments as required by the Order, may issue a general license permitting otherwise prohibited transactions, including pursuant to conditions specified in the license. In those instances, otherwise prohibited transactions that satisfy any applicable conditions would be permitted; there would be no requirement for a party to seek further authorization prior to concluding a transaction covered by such a license. General licenses could be issued to ease industry’s transition once the proposed rules become effective by potentially, for example, authorizing orderly wind-down conditions for covered data transactions that would otherwise be prohibited by the proposed rules.

2. Section 202.802—Specific Licenses

Specific licenses, on the other hand, would cover only parties who apply to the Department for such a license and disclose the facts and circumstances of the covered data transaction they seek to engage in. Specific licenses would authorize only the transactions described in the license; a specific license might authorize one or more transactions that would otherwise be prohibited.

3. Conditions on General and Specific Licenses

Both general licenses and specific licenses could include a range of requirements or obligations as the Department deems appropriate. For example, a license might be conditioned

on additional disclosure requirements, ongoing reporting obligations, recordkeeping obligations, due diligence requirements, certification requirements, cybersecurity requirements, or inclusion of certain contractual terms. The Department believes, as a general matter, that imposing uniform requirements across licenses to the greatest extent possible will encourage adoption of those practices as a matter of course and will facilitate compliance for parties operating under more than one license. For example, recordkeeping requirements for one license might be identical to those of another license. Nonetheless, the Department believes that it is important to retain flexibility in crafting applicable requirements—especially in the context of specific licenses—to account for varying contexts of the contemplated transactions and other aspects of the license at issue. The proposed rule reflects that flexibility.

The authorization provided by a license is contingent on satisfying all conditions of the license. Transactions not conducted in compliance with a license's conditions would be subject to the regulation's restrictions and prohibitions and may result in violations of the proposed rule and subject the transacting parties to enforcement action. Misrepresentations in the application process may render the license void from the date of issuance and may subject parties to enforcement action. The proposed rule contains provisions authorizing the Department to require applicants for specific licenses to use specific forms and procedures published by the Department. The proposed rule also establishes a process to allow applicants and other parties-in-interest to request reconsideration of the denial of a license based on new facts or changed circumstances.

Under subpart D of the proposed rule, governing restricted transactions, parties may engage in certain otherwise-prohibited transactions if they satisfy the specified security requirements. These provisions operate functionally as a general license to engage in certain prohibited transactions when specific conditions—the security requirements—are met. The Department does not anticipate issuing licenses in the ordinary course to relieve parties from complying with the security requirements for restricted transactions but may do so in unusual or unique circumstances as necessary or appropriate. The Department retains the discretion, however, to issue general or

specific licenses that would apply to otherwise restricted transactions.

G. Subpart I—Advisory Opinions

1. Section 202.901—Inquiries Concerning Application of This Part

The proposed rule creates a system for the Attorney General to provide guidance on this part in the form of official guidance or written advisory opinions. The Department may issue official guidance at any time, including to address recurring or novel issues. The Department may also issue guidance in response to specific inquiries received through advisory opinion procedures.

Under the proposed rule, the Department may publish general forms of interpretive guidance, such as Frequently Asked Questions posted online. The Department plans to make any official guidance publicly available to help potentially regulated parties better understand the regulations and the Department's interpretation of the regulations and the Order.

The proposed rule also creates a mechanism for potentially regulated parties to seek opinions about the application of the regulations or the Order to specific transactions. The proposed rule would permit a U.S. person engaging in a transaction potentially regulated by the program to request an interpretation of any provision of this part. Advisory opinions could cover, for example: (1) whether a particular transaction is a prohibited transaction or restricted transaction; and (2) whether a person is a U.S. person, foreign person, or covered person. The proposed rule requires that advisory opinions only be requested regarding actual—not hypothetical—transactions.

The proposed rule sets out procedural and administrative requirements for submitting a request for any advisory opinion, including: (1) that the request be made in writing, *see* § 202.1201; (2) that the request identify all participants in the transaction for which the opinion is being sought (*i.e.*, anonymous requests will not be accepted); and (3) that the request describe the actual, not hypothetical, conduct giving rise to the request for an advisory opinion. Advisory opinions issued in response to a party's request may be published as appropriate. A determination regarding whether an advisory opinion or portions of that opinion are appropriate for publication will include consideration of whether publication complies with applicable laws and regulations (*e.g.*, regarding the protection of confidential business information). In addition, the proposed rule makes clear that each

advisory opinion can be relied upon only to the extent that the disclosures made in obtaining the advisory opinion were accurate and complete, and to the extent that those disclosures continue to accurately and completely reflect the circumstances after the advisory opinion is issued. Advisory opinions will reflect the view of the Department of Justice and will not bind any other agency; an advisory opinion does not affect obligations under provisions not specifically discussed in the opinion.

Commenters supported the Department's proposal to provide interpretive guidance to the public. They also requested that the Department publish the decisions for the public's benefit. As stated above, advisory opinions may be published as appropriate in compliance with applicable laws and regulations. One commenter requested that trade associations be allowed to request interpretive guidance on behalf of their members. The proposed rule would allow trade associations to seek guidance on behalf of their members, so long as the guidance sought relates to a specific transaction and identifies the parties to the transaction. Although one commenter requested the ability to seek guidance related to hypothetical transactions, the Department declines to extend the interpretive guidance provision to such transactions to ensure that any such guidance is based on specific, factual circumstances so that it is as helpful to the public as possible. Consequently, the proposed rule adopts the approach described in the ANPRM without change.

H. Subpart J—Due Diligence and Audit Requirements

The Order delegates to the Attorney General, in consultation with relevant agencies, the full extent of the authority granted to the President by IEEPA as may be necessary or appropriate to carry out the purposes of the Order,²¹⁷ and it expressly states that the proposed rules will “address the need for, as appropriate, recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts.”²¹⁸ The Department of Justice wishes to achieve widespread compliance with the proposed rule, and to gather the information necessary to administer and enforce the program, without unduly burdening U.S. persons or discouraging data transactions that the program is not intended to address.

The Department will encourage U.S. persons subject to the proposed rule to

²¹⁷ E.O. 14117 sec. 2(b), 89 FR 15423.

²¹⁸ *Id.* sec. 2(c)(viii), 89 FR 15424.

develop, implement, and update compliance programs as appropriate. The compliance program suitable for a particular U.S. person would be based on that person's individualized risk profile and would vary depending on a variety of factors, including the U.S. person's size and sophistication, products and services, customers and counterparties, and geographic locations. The Department may issue guidance on this topic to assist U.S. persons to develop and implement compliance programs. The Department may also consider the adequacy of a compliance program in any enforcement action.

The proposed rule does not impose affirmative due diligence and recordkeeping requirements on every U.S. person engaging in a covered data transaction with a covered person or country of concern. As discussed in part IV.H.1 of this preamble, the proposed rule only imposes affirmative due diligence and recordkeeping requirements as a condition of engaging in a restricted transaction.

Two related commenters expressed concerns that the proposed rule would require U.S. companies to surveil their employees' communications to comply with the prohibitions and restrictions. No changes have been made in response to this comment. The proposed rule does not, on its face or in practice, require surveillance of employees to achieve compliance. Any U.S. person engaging in activities relevant to the proposed rule should take a risk-based approach to their compliance program and ensure that it aligns with their business profile. Like sanctions, export controls, and other national security regulations, any compliance program may include a mix of policies, processes, resources, and technologies to ensure compliance. Important aspects of an effective compliance program may include, for example, senior management support and buy-in (including adequate resources); a routine and ongoing assessment of the business' risk profile to identify potential issues under the regulations that the business is likely to encounter; internal controls informed by that risk assessment, including policies and procedures to identify and address data transactions that may trigger obligations under the regulations, appointing and empowering responsible compliance personnel, integrating these controls into the company's daily operations, and ensuring that employees have adequate training and job-specific knowledge regarding the proposed rule and internal controls; and testing these controls and remediating any

weaknesses or gaps.²¹⁹ The Department is considering providing separate guidance on implementing effective risk-based compliance programs.

1. Section 202.1001—Due Diligence for Restricted Transactions

As discussed in part IV.H of this preamble, the Order delegates to the Attorney General, in consultation with relevant agencies, the full extent of the authority granted to the President by IEEPA as may be necessary or appropriate to carry out the purposes of the Order.²²⁰ In accordance with that delegation, and adopting the approach contemplated in the ANPRM, the proposed rule imposes and details affirmative due diligence requirements as a condition of engaging in a restricted transaction. The proposed rule imposes know-your-data requirements, which specifically require that U.S. persons engaging in restricted transactions develop and implement data compliance programs with risk-based procedures for verifying data flows, including the types and volumes of data involved in the transactions, the identity of the transaction parties, and the end-use of the data. The Order also requires that the proposed rule address the need for recordkeeping, as appropriate.²²¹ The proposed rule imposes affirmative recordkeeping requirements as a condition of engaging in a restricted transaction, and requires U.S. persons subject to these affirmative requirements to maintain documentation of their due diligence to assist in inspections and enforcement, and to maintain the results of annual audits that verify their compliance with the security requirements and, where relevant, the license conditions to which the U.S. persons may be subject.

2. Section 202.1002—Audits for Restricted Transactions

Adopting the approach contemplated in the ANPRM, the proposed rule would impose and details an annual audit requirement as a condition of engaging in a restricted transaction to verify and improve compliance with the security requirements.

²¹⁹ See generally OFAC, U.S. Dep't of Treas., *A Framework for OFAC Compliance Commitments* (May 2, 2019), <https://ofac.treasury.gov/media/16331/download?inline> [<https://perma.cc/6EQY-MD3L>]; Bureau of Indus. & Sec., U.S. Dep't of Com., *Export Compliance Guidelines: The Elements of an Effective Export Compliance Program* (2017), <https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file> [<https://perma.cc/KXT2-TMQ5>].

²²⁰ E.O. 14117 sec. 2(b), 89 FR 15424.

²²¹ E.O. 14117 sec. 2(c)(viii), 89 FR 15423.

I. Subpart K—Reporting and Recordkeeping Requirements

1. Section 202.1101—Records and Recordkeeping Requirements

Adopting the approach contemplated in the ANPRM, the proposed rule would require any U.S. person engaging in a restricted transaction to keep full and accurate records of each restricted transaction and to keep the records available for examination for at least 10 years after the date of such transaction (the length of the statute of limitations for violations of IEEPA). The proposed rule describes the required records in detail, which include a written policy describing the compliance program, a written policy documenting implementation of the security measures for restricted transactions, the results of any audits to evaluate compliance with the security measures, documentation of the due diligence conducted to verify the data flow involved in any restricted transaction, and other pertinent information regarding each transaction.

2. Section 202.1102—Reports To Be Furnished on Demand

Adopting the approach contemplated in the ANPRM, the proposed rule includes provisions to assist the Department in investigating potential noncompliance with the proposed rules of this program. These include requiring any U.S. person to furnish under oath, from time to time and at any time as may be required by the Attorney General, complete information relative to any covered data transaction subject to a prohibition or restriction.

3. Section 202.1103—Annual Reports

Adopting the approach contemplated in the ANPRM, the proposed rule would require reporting by U.S. persons who engage in certain restricted transactions or, in certain narrow circumstances, to identify attempts to engage in prohibited transactions. Specifically, the proposed rule requires annual reports from U.S. persons engaged in restricted transactions involving cloud-computing services where 25 percent or more of that U.S. person's equity interests are owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a country of concern or covered person.

The Department may impose similar reporting requirements on U.S. persons engaging in licensed transactions as conditions of specific or general licenses. Those requirements may vary depending on the nature of the licenses, will be set forth in the licenses

themselves, and are not part of the proposed rule.

4. Section 202.1104—Reports on Rejected Prohibited Transactions

Adopting the approach contemplated in the ANPRM, the proposed rule also requires that any U.S. person that has received and affirmatively rejected an offer from another person to engage in a prohibited transaction must submit a report to the Department within 14 business days of rejecting it. These reports will help the Department identify instances in which potential countries of concern or covered persons seek to enter into prohibited transactions with U.S. persons in contravention of the proposed rule, including through evasion. The information submitted by these reports will thus assist the Department in monitoring U.S. persons' compliance with the proposed rule, identifying matters for potential investigation, undertaking enforcement actions, and identifying ways in which to refine the proposed rule in the future.

J. Subpart M—Penalties and Finding of Violation

1. Section 202.1301—Penalties for Violations

Adopting the approach contemplated in the ANPRM, the proposed rule also includes a process for imposing civil monetary penalties similar to those used in other IEEPA-based regimes. See 31 CFR part 501, Appendix A; 15 CFR part 764. The proposed rule includes mechanisms for pre-penalty notice, an opportunity to respond, and a final decision. Under the proposed rule, penalties may be based on noncompliance with the proposed rules of this program, material misstatements or omissions in connection with this program, false certifications or submissions pursuant to the proposed rules of this program, or other actions and factors. The proposed rule stipulates that, consistent with due process requirements, the Department of Justice will give the alleged violator any relevant non-classified information that forms the basis of any enforcement action and a meaningful opportunity to respond.

As part of this proposed rulemaking, the Department is adjusting for inflation the civil monetary penalty that can be imposed under IEEPA in accordance with section four of the Federal Civil Penalties Inflation Adjustment Act of 1990 (Pub. L. 101–410, 104 Stat. 890; 28 U.S.C. 2461 note), as amended by the Federal Civil Penalties Inflation Adjustment Act Improvements Act of

2015 (Pub. L. 114–74, tit. VII, sec. 701, 129 Stat. 584, 599, 28 U.S.C. 2461 note) (“FCPIA Act”), for penalties assessed after the effective date of this proposed part with respect to violations occurring after November 2, 2015.

For consistency with the civil monetary penalties imposed in other, more widely known IEEPA-based regimes administered by the Department of the Treasury’s OFAC, the Department of Justice proposes incorporating OFAC’s prior annual adjustments to IEEPA’s maximum civil monetary penalty as an initial catch-up adjustment applicable to this part. Those adjustments by OFAC occurred on August 1, 2016 (Implementation of the Federal Civil Penalties Inflation Adjustment Act, 81 FR 43070 (July 1, 2016)); February 10, 2017 (Inflation Adjustment of Civil Monetary Penalties, 82 FR 10434 (Feb. 10, 2017)); March 19, 2018 (Inflation Adjustment of Civil Monetary Penalties, 83 FR 11876 (Mar. 19, 2018)); June 14, 2019 (Inflation Adjustment of Civil Monetary Penalties, 84 FR 27714 (June 14, 2019)); April 9, 2020 (Inflation Adjustment of Civil Monetary Penalties, 85 FR 19884 (Apr. 9, 2020)); March 17, 2021 (Inflation Adjustment of Civil Monetary Penalties, 86 FR 14534 (Mar. 17, 2021)); February 9, 2022 (Inflation Adjustment of Civil Monetary Penalties, 87 FR 7369 (Feb. 9, 2022)); January 13, 2023 (Inflation Adjustment of Civil Monetary Penalties, 88 FR 2229 (Jan. 13, 2023)); and January 12, 2024 (Inflation Adjustment of Civil Monetary Penalties, 89 FR 2139 (Jan. 12, 2024)).

The proposed maximum civil monetary penalty for violations of this part after its effective date would therefore be the greater of \$368,136 or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed.²²² The Department of Justice proposes making annual adjustments to the civil monetary penalty on an annual basis after the effective date of this part consistent with the FCPIA Act.

2. Section 202.1305—Finding of Violation

The proposed rule also provides a process in which the Department might issue a finding of violation where the Department determines that a party has violated the regulations and that an administrative response short of a civil monetary penalty is warranted. As with civil penalties, the proposed rule also

provides that, consistent with due process requirements, the Department will give the alleged violator any relevant non-classified information that forms the basis of any finding of violation and a meaningful opportunity to respond.

K. Coordination With Other Regulatory Regimes

The Order requires the Department of Justice to address, as appropriate, coordination with other United States Government entities, such as CFIUS, OFAC, agencies that operate export-control programs, and other entities implementing relevant programs, including those implementing Executive Order 13873; Executive Order 14034 of June 9, 2021 (Protecting Americans’ Sensitive Data from Foreign Adversaries); and Executive Order 13913 of April 4, 2020 (Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector).²²³ The Department does not currently intend or anticipate that this new program will significantly overlap with existing programs. As explained in the ANPRM, existing programs do not provide prospective, categorical rules to address the national security risks posed by transactions between U.S. persons and countries of concern (or persons subject to their ownership, direction, jurisdiction, or control) that pose an unacceptable risk of providing those countries with access to government-related data or bulk U.S. sensitive personal data.

The Department has identified and considered three potential areas of overlap between this proposed rule and existing regulatory regimes.

First, the Department has considered the potential interaction between this proposed rule’s application to investment agreements and CFIUS’s authority to review “covered transactions,” see generally 50 U.S.C. 4565. Some “investment agreements,” as defined in the proposed rule, would also be covered transactions or covered real estate transactions subject to CFIUS’s jurisdiction. See § 202.228; 50 U.S.C. 4565(a)(4). The ANPRM contemplated an approach in which the proposed rule would independently regulate, as a restricted transaction, an investment agreement that is also a covered transaction or covered real estate transaction subject to review by CFIUS unless and until a “CFIUS action” occurs in which CFIUS imposes an order or condition or enters into a mitigation agreement to resolve the

²²² See 50 U.S.C. 1705(b); Inflation Adjustment of Civil Monetary Penalties, 89 FR 2139 (Jan. 12, 2024).

²²³ E.O. 14117, sec. 2(c)(vii), 89 FR 15424.

national security risk arising from the transaction.²²⁴ As explained in the ANPRM, this approach would preserve CFIUS's authority to develop bespoke protections to mitigate risks arising from covered transactions or covered real estate transactions—or recommend that the President prohibit a transaction—where CFIUS concludes that such action is necessary to address the national security risk arising from the transaction. To implement this approach, the ANPRM contemplated an exemption in the proposed rule that would apply categorically for all covered transactions that are subject to CFIUS actions, rather than requiring the Department to issue a specific license for each investment agreement subject to a CFIUS action.

The proposed rule adopts the approach described in the ANPRM and implements that approach by adding a corresponding exemption for any investment agreement that is subject to a “CFIUS action,” defining that term, and providing examples. *See* § 202.508. Under the proposed rule, if a CFIUS action occurs with respect to an investment agreement, that investment agreement would become exempt from the proposed rule and would be subject only to CFIUS's authority going forward. The Department, in close coordination with the Department of the Treasury, as chair of CFIUS, would retain enforcement authority with respect to any violations of the proposed rule before the effective date of the CFIUS action. Alternatively, in some instances, CFIUS may not review a particular transaction at all or may conclude its review or assessment of a transaction without taking a CFIUS action. Because CFIUS's authority to mitigate transactions is limited to risks that “arise[s] as a result” of the particular transaction, *see* 50 U.S.C. 4565(l)(3)(A)(i), the fact that CFIUS takes no action does not mean that the transaction poses no national security risk. For example, the transaction may implicate pre-existing national security risks that do not arise from the particular transaction CFIUS can review.” In those scenarios, any obligations under the proposed rule would continue to apply with respect to the transaction. Similarly, if CFIUS requests information from parties about a transaction for which no filing has been submitted to CFIUS under 31 CFR 800.504(b) or 31 CFR 802.501(b), the Department will closely coordinate with the Department of the Treasury with respect to any enforcement action under the proposed rule with respect to that

investment agreement. CFIUS may also refer a covered transaction or covered real estate transaction to the President, in which case any obligations under the proposed rule would continue to apply and the Department would closely coordinate with the Department of the Treasury on any enforcement actions under the proposed rule. The same would be true after any Presidential order under 50 U.S.C. 4565(d) following a referral from CFIUS, absent any accompanying CFIUS action. The Department, in consultation with CFIUS member agencies, continues to evaluate alternative approaches, such as regulating investment agreements as restricted transactions regardless of whether they are “covered transactions” subject to a CFIUS action. The Department welcomes comments on this potential alternative approach, as well as any other proposed alternatives.

Second, the Department has considered, in consultation with the Federal Trade Commission (“FTC”) and other agencies, the potential interaction between this proposed rule's application to data-brokerage transactions and the Protecting Americans' Data from Foreign Adversaries Act of 2024 (“PADFAA”). *See* Public Law 118–50, div. I 138 Stat. 895, 960 (2024). The PADFAA generally makes it unlawful for a “data broker to sell” or “otherwise make available personally identifiable sensitive data of a United States individual” to any foreign adversary country or any entity that is controlled by a foreign adversary and authorizes the FTC to bring civil enforcement actions for any violations. The proposed rule would generally prohibit U.S. persons from engaging in covered data transactions involving data brokerage with countries of concern or covered persons.

Following consultation with the FTC, the Department does not believe that it would be appropriate to alter the proposed rule's scope in light of the PADFAA for several reasons. There are significant differences in scope between the PADFAA and the proposed rule. The PADFAA's prohibition applies to entities that meet the statutory definition of “data broker.”²²⁵ By contrast, the proposed rule would regulate certain transactions involving “data brokerage,” a term that is broader and covers activities that present the national security risk of allowing countries of concern access to sensitive personal data, regardless of the kinds of entities that engage in that activity. In

addition, the proposed rule would reach any U.S. persons—including individuals, not just entities—who engage in the regulated categories of activities. Similarly, the PADFAA applies to a narrower category of activities than the proposed rule. Unlike the PADFAA, the proposed rule expressly addresses the re-export or resale of data by third parties and indirect sales through intermediaries. The PADFAA excludes from the definition of “data broker” any entity that transmits a U.S. individual's data at that individual's request or direction, whereas the proposed rule would not contain any such exception in light of the national security threat posed even in such instances. In addition, the PADFAA does not provide any mechanisms for affected parties to seek clarification or redress, such as the advisory opinions, general licenses, and specific licenses available to parties under the proposed rule. Similarly, the PADFAA provides general contours for entities and businesses to determine whether a counterparty is “subject to the direction or control” of either: (1) a person that is domiciled in, headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country; or (2) an entity that is 20-percent or more owned by such a person.²²⁶ The proposed rule provides different criteria for determining whether a person is “covered” under the regulatory program, and it contemplates a designation process, which the PADFAA lacks.

Given the PADFAA's structure and the significant differences in scope, the Department declines to alter the proposed rule's scope in light of the PADFAA. The Department and the FTC intend to coordinate closely to ensure that these authorities are exercised in a harmonized way to minimize any conflicting obligations or duplicative enforcement. For example, the Department and the FTC intend to coordinate, as appropriate, on licensing decisions and on any potential enforcement actions under the PADFAA with respect to activities that may be authorized, exempt, or licensed under the proposed rule. Thus, the proposed rule adopts the approach described in the ANPRM without change.

Third, the Department has considered the potential interaction between this proposed rule's application to vendor agreements and any actions taken by the Secretary of Commerce under Executive Orders 13873 and 14034. Some vendor agreements, as defined in this proposed

²²⁵ Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. 118–50, div. I, sec. 2(c)(3) 138 Stat. 895, 960 (2024).

²²⁶ *Id.* at sec. 2(c)(2).

rule, could also be the subject of an action by the Secretary of Commerce regarding an information and communications technology and services (“ICTS”) transaction that involves ICTS that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary and presents the types of unacceptable national security risks described in Executive Orders 13873 and 14034. Even so, the Department does not believe that it would be appropriate to alter the scope of this proposed rule for several reasons. While these two authorities could potentially address some of the same national security risks related to vendor agreements, they would do so in different ways and by focusing on different vectors of risk. Executive Order 14117 and this proposed rule seek to address this risk by addressing transactions involving the export of U.S. sensitive personal data, such as restricting a U.S. person’s ability to enter into a vendor agreement that grants access to government-related data or bulk U.S. sensitive personal data to a country of concern or covered person. Executive Orders 13873 and 14034, on the other hand, seek to address transactions involving the acquisition, import, or use, among other actions, of technology or services developed or otherwise sourced from a foreign adversary by U.S. persons or in the United States. For that reason, the ICTS authority addresses a broader range of potential national security risks than access to Americans’ bulk sensitive personal data.

In addition, this proposed rule (through the incorporation by reference of the CISA security requirements for restricted transactions, including vendor agreements) creates a floor for the security of all government-related data or Americans’ bulk U.S. sensitive personal data involved in a restricted transaction. Only by complying with these requirements (or operating under an applicable license) could a U.S. person engage in a proposed restricted transaction. Executive Order 13873 and its implementing regulations do not establish a baseline set of mitigation measures to protect this data across all of types of vendors that could be subject to prohibition or restriction. Rather, the Department of Commerce will exercise that authority by taking an action with respect to transactions involving a specific vendor²²⁷ or proposing regulation of a sector-specific set of

ICTS.²²⁸ Nothing in this proposed rule would prevent the Department of Commerce from exercising its ICTS authorities to take vendor-specific actions or promulgate sector-specific rules. At this time, any overlap between these two authorities is hypothetical, and the Department does not believe that there will be any substantial impact. The Department is, however, considering approaches to address any potential overlap that might arise between the requirements of this proposed rule and any ICTS actions undertaken by the Department of Commerce, whether through an understanding between the Department of Commerce and Department of Justice or a more formal licensing process that could apply where the Department of Commerce has taken action under its ICTS authorities. The Department welcomes comments on the identified approaches, or any others, to address any potential overlap that might arise.

L. Severability

The Department intends for the provisions of this proposed rule to be severable from each other. In short, if a court holds that any provision in a final 28 CFR part 202 is invalid or unenforceable, the Department intends that the remaining provisions of a final 28 CFR part 202, as relevant, would continue in effect to the greatest extent possible. In addition, if a court holds that any such provision is invalid or unenforceable as to a particular person or circumstance, the Department intends that the provision would remain in effect as to any other person or circumstance. Depending on the circumstances and the scope of the court’s order, remaining provisions of a final rule likely could continue to function sensibly independent of any provision or application held invalid or unenforceable. For example, the prohibitions and restrictions related to transactions involving access to personal health data could continue to apply even if a court finds that the restrictions or prohibitions on transactions involving access to biometric data are invalid. Similarly, the proposed rule could be applied with respect to North Korea even if a court finds its application with respect to Russia is invalid.

²²⁸ See *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, 89 FR 15066 (Mar. 1, 2024) (to be codified at 15 CFR pt. 7), <https://www.federalregister.gov/documents/2024/03/01/2024-04382/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles> [<https://perma.cc/PV7Y-998V>].

V. Analysis for Proposed Bulk Thresholds

The Department of Justice proposes volume-based thresholds for each category of sensitive personal data and for combined datasets. The bulk thresholds are based on a risk-based assessment that accounts for the characteristics of datasets that affect the data’s vulnerability to exploitation by countries of concern and that affect the consequences of exploitation. In conducting this assessment, the Department considered numerous ways that a country of concern might exploit each category of sensitive personal data. In general, bulk U.S. sensitive personal data is useful for deriving additional information about individuals or subpopulations, such as demography, geography, and interests, that can be used to identify vulnerabilities.²²⁹ The advertising industry has long recognized that such data is useful for predicting and influencing behavior.²³⁰ Influencing behavior is similarly at the root of intelligence recruitment.²³¹ The Department assessed how a foreign intelligence service might use bulk U.S. sensitive personal data as part of the agent recruitment cycle—a “systematic method for finding agents who will meet national intelligence information needs”—among other potential malign uses.²³² While the categories of sensitive personal data may have a variety of applications for foreign intelligence services or foreign governments, they may be especially useful to parts of the first three steps of agent recruitment:

- “spotting (or identifying) individuals who can meet intelligence needs”;
- “assessing whether the spotted individuals have the placement and access to provide desired information”; and

²²⁹ *What Is Targeted Advertising, and How Does It Work?*, RTB House (May 13, 2024), <https://blog.rtbhouse.com/what-is-targeted-advertising-and-how-does-it-work/> [<https://perma.cc/EQ5Q-M6KD>].

²³⁰ See *The Role of Data in the Targeted Advertising Industry*, New Am., <https://www.newamerica.org/oti/reports/special-delivery/the-role-of-data-in-the-targeted-advertising-industry/> [<https://perma.cc/LMX7-B93Q>]; Ben Collier, *Targeted Social Media Ads Are Influencing Our Behaviour—and the Government Uses Them Too*, Conversation (Feb. 27, 2024), <https://theconversation.com/targeted-social-media-ads-are-influencing-our-behaviour-and-the-government-uses-them-too-223576> [<https://perma.cc/YGA8-YKF9>].

²³¹ See *id.*; Randy Burkett, *An Alternative Framework for Agent Recruitment: From MICE to RASCLS*, 57 Stud. Intel. 7, 13 (2013), <https://www.cia.gov/resources/csi/static/9ccc45dc156271d11769e5205ec49c29/Alt-Framework-Agent-Recruitment-1.pdf> [<https://perma.cc/9GQU-UTET>]; Collier, *supra* note 230.

²³² Burkett, *supra* note 231, at 13.

²²⁷ See *Kaspersky Lab, Inc.*, 89 FR 52435 n.13; Maggs Report, *supra* note 187.

• “developing a relationship with the individual to . . . explore whether they will be responsive to . . . tasking for intelligence information.”²³³

The Department’s subject-matter experts identified seven characteristics relevant to the exploitability and national security harm posed by any particular type of data: purpose (*i.e.*, how the data can be used), changeability (*i.e.*, how easy it would be for an individual to deliberately change or falsify the data in question), control (*i.e.*, who tracks and manages the data), availability (*i.e.*, how easily the data can be obtained), volume (*i.e.*, the number of data points in a dataset), velocity (*i.e.*, how quickly the dataset evolves), and quality (*i.e.*, how much processing is required to use the data). These characteristics help describe the national security risk of each type of sensitive personal data by providing a methodology for analyzing their value to an adversary. For example, availability and control focuses on the ease with which an adversary may be able to acquire this data using licit or illicit means. Quality and changeability examine the ease and speed with which an adversary can use the data. Volume, velocity, and purpose are other important attributes of these datasets that focus on how valuable a particular data may be to an adversary and how long it is likely to remain valuable.

Using this framework of characteristics, the Department evaluated the relative sensitivity of each of the seven categories of bulk U.S. sensitive personal data and ranked them based on their potential value to enable foreign governments and foreign intelligence services engaged in agent recruitment to: (1) identify or spot individuals within bulk datasets for intelligence needs; (2) group individuals into specific categories to assess their value for intelligence purposes; and (3) characterize the behaviors and vulnerabilities of individuals to identify ways to develop and exploit relationships. The Department then considered how close in sensitivity each category was to the other, grouped them into tiers of similar sensitivity (resulting in four tiers), and then set proposed numerical thresholds for each tier.

To conduct the analysis, the Department considered use cases from each category of bulk U.S. sensitive personal data based on widely available information about commercial practices around data,²³⁴ news reports of past

incidents involving data with national security implications,²³⁵ and a survey of covered transactions reviewed by CFIUS that implicated sensitive personal data. The Department also considered how future changes in technology could affect the utility and value of each category of data.²³⁶

A. Analysis of Sensitivity of Each Category of Sensitive Personal Data

1. Human Genomic Data

The Department of Justice assesses that human genomic data is the most sensitive category of sensitive personal data. To conduct the analysis, the Department considered human genetic testing data, which sequences only specific portions of the human genome for a specific purpose (*e.g.*, identifying ancestry, diagnosing a specific disease); and sequencing of a complete human genome, a still-emerging capability with a wide variety of potential applications.²³⁷ Based on the multiple characteristics that were considered of high sensitivity, and especially noting that the velocity of this data has very high sensitivity, human genomic data is highly sensitive:

- **Purpose:** High sensitivity. Human genomic data has unique purposes among the categories of bulk U.S. sensitive personal data. It is not only useful for identifying traits such as health, emotional stability, mental capacity, appearance, and physical abilities that might be useful in intelligence recruitment; countries of concern may also use this data to

develop military capabilities such as bioweapons.²³⁸ Because human genomic data includes the unique genetic code of an individual, it is exceptionally useful in identifying individuals.²³⁹ For example, an adversary with access to an individual’s genomic data may be able to predict physical features, such as eye, hair, and skin color, and vocal and facial characteristics.²⁴⁰ As technology develops further, analysts may also be able to use such genomic data to determine an individual’s propensity toward certain behaviors, such as aggression or risky activities.²⁴¹ Finally, foreign adversaries could potentially use human genomic data to conduct or support surveillance, oppression, extortion, and influence operations; and could potentially use this data to inform biological weapons development.²⁴²

- **Changeability:** High sensitivity. Human genomic data is difficult to deliberately alter. While certain technologies, such as Clustered Regularly Interspaced Short Palindromic Repeats (“CRISPR”), can alter or edit the human genome in extremely targeted, localized ways, larger-scale alterations remain technologically impossible.²⁴³ As a result, human genomic data is largely immutable over an individual’s lifetime.

- **Control:** High sensitivity. Corporate entities such as healthcare laboratories usually process and control human

www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/944W-ZC4M].

²³⁵ See, *e.g.*, Hsu, *supra* note 43; Garrett M. Graff, *China’s Hacking Spree Will Have a Decades-Long Fallout*, *Wired* (Feb. 11, 2020), <https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/> [https://perma.cc/48WK-M9AM]; Press Release, U.S. Dep’t of Just., *Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People* (May 9, 2019), <https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including> [https://perma.cc/84YH-CVA5].

²³⁶ See, *e.g.*, Steve Van Kuiken, *Tech at the Edge: Trends Reshaping the Future of IT and Business*, *McKinsey Digital* (Oct. 21, 2022), <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-at-the-edge-trends-reshaping-the-future-of-it-and-business> [https://perma.cc/HW2S-N464]; Adam D. Nahari & Dimitris Bertsimas, *External Data and AI Are Making Each Other More Valuable*, *Harv. Bus. Rev.* (Feb. 26, 2024), <https://hbr.org/2024/02/external-data-and-ai-are-making-each-other-more-valuable> [https://perma.cc/2ZAS-8VBB].

²³⁷ Luca Bonomi et al., *Privacy Challenges and Research Opportunities for Genomic Data Sharing*, *52 Nature Genetics* 646 (2020), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7761157/> [https://perma.cc/2J8T-BLLF].

²³⁸ Ken Dilanian, *Congress Wants to Ban China’s Largest Genomics Firm from Doing Business in the U.S. Here’s Why*, *NBC News* (Jan. 25, 2024), <https://www.nbcnews.com/politics/nationalsecurity/congress-wants-ban-china-genomics-firm-bgi-from-us-rcna135698> [https://perma.cc/T2Y2-R7RZ]; Ron Pulivarti et al., *Nat’l Inst. of Standards & Tech., NIST IR 8432, Cybersecurity of Genomic Data 9* (2023), <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8432.pdf> [https://perma.cc/5D3G-BEEZ].

²³⁹ Bonomi et al., *supra* note 237.

²⁴⁰ Christopher Lippert et al., *Identification of Individuals by Trait Prediction Using Whole-Genome Sequencing Data*, *114 PNAS* 10166 (Sept. 5, 2017), <https://www.pnas.org/doi/full/10.1073/pnas.1711125114> [https://perma.cc/CM4L-GPE4].

²⁴¹ J.C. Barnes et al., *The Propensity for Aggressive Behavior and Lifetime Incarceration Risk: A Test for Gene-Environment Interaction (G x E) Using Whole-Genome Data*, *49 Aggr. & Violent Behav.* (Nov.–Dec. 2019), <https://www.sciencedirect.com/science/article/abs/pii/S1359178919300631> [https://perma.cc/3GVF-MPKF]; Heather Buschman, *Large Study Identifies Genetic Variants Linked to Risk Tolerance and Risky Behaviors*, *UC San Diego Health* (Jan. 2019), <https://health.ucsd.edu/news/press-releases/2019-01-14-large-study-identifies-genetic-variants-linked-to-risk-tolerance-risky-behaviors/> [https://perma.cc/FMV2-GKYE].

²⁴² Pulivarti et al., *supra* note 238, at 9.

²⁴³ *What Are Genome Editing and CRISPR-Cas9?*, *MedlinePlus* (updated Mar. 22, 2022), <https://medlineplus.gov/genetics/understanding/genomicresearch/genomeediting/> [https://perma.cc/42K9-765F].

²³³ *Id.*

²³⁴ See, *e.g.*, Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)*, *Bus. News Daily* (Oct. 20, 2023), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

genomic data.²⁴⁴ Because human genomic data is tied to an individual at a biological level, it is basically immutable. Additionally, biological residue such as saliva, blood, and hair can contain human genomic data, and this residue is difficult for an individual to completely control.²⁴⁵

- **Availability:** High sensitivity. Bulk human genomic data is difficult to obtain in the commercial marketplace, as it remains an emerging capability. For example, the crucial technologies that formed the foundation for scaled commercial applications of genomic sequencing are still less than 20 years old.²⁴⁶ In addition, medical systems tightly control access to and distribution of this information through privacy regulations and general scientific ethics.²⁴⁷ Because this data is currently hard to acquire but has myriad potential applications, it is highly valued.

- **Volume:** Varied sensitivity. A complete human nuclear genome contains about 3.2 billion base pairs, with each base pair representing a unique data point.²⁴⁸ This human genome can be divided into codons of three base pairs each, each of which codes for a unique amino acid.²⁴⁹ This human genome can also be divided into tens of thousands of genes, each of which code for the production of specific proteins and other cellular activity and each of which can have multiple variants.²⁵⁰ Data sets

containing human genomic data will be of different sizes—for example, a data set including the complete genome of an individual will be much larger than the data set just identifying specific genes present that may affect the chances of a specific cancer. A larger data set is more sensitive. Thus, the volume sensitivity of genomic information may vary because the datasets containing human genomic data are likely to vary widely in size.

- **Velocity:** Very high sensitivity. Human genomic data remains largely stable over an individual's lifetime, and while the ability to interpret that data may evolve over time, the underlying information will not change.²⁵¹ Furthermore, the value of human genomic data will likely increase significantly in the future as technology develops.²⁵² It requires protection now to prevent future exploitation.²⁵³

- **Quality:** Varied sensitivity. Processing a single sample of human genomic data can take as long as 48 hours. As a result, computing power continues to limit analysts' ability to use fully sequenced but unevaluated human genomic data.²⁵⁴ However, analysts will be increasingly able to take advantage of public databases and open-source tools to evaluate sequenced and analyzed data, reducing the computational power required to evaluate such processed datasets.²⁵⁵

2. Biometric Identifiers

The Department of Justice assesses that biometric identifiers are the second most sensitive category of sensitive personal data. To conduct the analysis, the Department considered physical biometrics measurements (e.g., eye patterns, fingerprints, facial features) as well as behavioral biometrics measurements (e.g., gait, keystroke recognition, signature).²⁵⁶ Biometric

data is moderately to highly sensitive overall based primarily on the purpose, changeability, and control characteristics below:

- **Purpose:** High sensitivity. Biometric data is specifically intended to identify specific individuals based on distinguishing biological or behavioral characteristics.²⁵⁷ In addition, analysts can identify certain categorizing characteristics from this data—for example, inferring gender from facial features.²⁵⁸ Finally, biometric information can be used to authenticate users, either alone or as part of a multi-factor authentication protocol. Fingerprints, voiceprints, and facial scans provide useful reference points for identifying individuals for intelligence recruitment, espionage, and influence based on their patterns of life. Searches through video footage, police records, and intelligence databases using biometrics could provide points of leverage for coercion, blackmail, and influence.

- **Changeability:** Moderate-to-high sensitivity. Biometric data is generally difficult to deliberately change or falsify because it is linked to the physical characteristics of an individual. However, it can evolve as individuals age or be altered through activities such as limb loss or amputation, long-term manual labor, or physical retraining.²⁵⁹

- **Control:** Moderate-to-high sensitivity. Physical biometric information is largely beyond the ability of an individual to control or conceal. If an individual's fingerprint or other

²⁴⁴ Bonomi et al., *supra* note 237, at Table 2; *Genomic & Infrastructure Services*, Quest Diagnostics, <https://www.questdiagnostics.com/business-solutions/life-sciences/biotech/genomic-infrastructure-services> [<https://perma.cc/WD2E-2YXA>].

²⁴⁵ Am. Bar Ass'n, *ABA Standards for Criminal Justice: DNA Evidence* at 25 (3d ed. 2007), https://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/dna_evidence.pdf [<https://perma.cc/3CSA-Q6J9>]; Alexia Ramirez, *Police Need a Warrant to Collect DNA We Inevitably Leave Behind*, ACLU (Mar. 10, 2020), <https://www.aclu.org/news/privacy-technology/police-need-a-warrant-to-collect-dna-we-inevitably-leave-behind> [<https://perma.cc/9MGJ-LDZP>].

²⁴⁶ Joseph Wilson, *Sequencing—The Next Generation*, *Nature* (Feb. 10, 2021), <https://www.nature.com/articles/d42859-020-00103-7> [<https://perma.cc/PY2Q-GKNY>].

²⁴⁷ *Privacy in Genomics*, Nat'l Hum. Genome Rsch Inst. (Feb. 6, 2024), <https://www.genome.gov/about-genomics/policy-issues/Privacy> [<https://perma.cc/2YU5-GBRZ>].

²⁴⁸ Terence A. Brown, *The Human Genome*, in *Genomes* (2d ed. 2002), <https://www.ncbi.nlm.nih.gov/books/NBK21134/> [<https://perma.cc/Q9EW-FB7E>].

²⁴⁹ *Codon*, Nat'l Cancer Inst., <https://www.cancer.gov/publications/dictionaries/genetics-dictionary/def/codon> [<https://perma.cc/GDB6-T32U>].

²⁵⁰ See Steven L. Salzberg, *Open Questions: How Many Genes Do We Have?*, 16 *BMC Biology* (Aug. 20, 2018), <https://bmcbiol.biomedcentral.com/articles/10.1186/s12915-018-0564-x> [<https://perma.cc/89MV-J6HU>].

²⁵¹ Kate Lyle et al., *Immortal Data: A Qualitative Exploration of Patients' Understandings of Genomic Data*, 31 *Eur. J. Hum. Genetics* 681 (Mar. 31, 2023), <https://doi.org/10.1038/s41431-023-01325-9> [<https://perma.cc/V6BM-NEE8>].

²⁵² *Genomic Data Science*, Nat'l Hum. Genome Rsch Inst. (Apr. 5, 2022), <https://www.genome.gov/about-genomics/fact-sheets/Genomic-Data-Science> [<https://perma.cc/8YD2-MQZJ>]; Nat'l Counterintel. & Sec. Ctr., *supra* note 83.

²⁵³ Pulivarti et al., *supra* note 238, at 7–10.

²⁵⁴ See Nathan Eddy, *High-Performance Computing Breaks the Genomics Bottleneck*, *HealthTech* (Feb. 13, 2023), <https://healthtechmagazine.net/article/2023/02/high-performance-computing-breaks-genomics-bottleneck> [<https://perma.cc/LCD5-X3K2>].

²⁵⁵ See, e.g., *Genome*, Nat'l Lib. Med., <https://www.ncbi.nlm.nih.gov/genome/> [<https://perma.cc/XEV9-FRYH>].

²⁵⁶ Sterling Miller, *The Basics, Usage, and Privacy Concerns of Biometric Data*, *Thomson Reuters* (July 20, 2022), <https://legal.thomsonreuters.com/en/insights/articles/the->

basics-usage-and-privacy-concerns-of-biometric-data [<https://perma.cc/92HR-4YMX>]; *Types of Biometrics*, Biometrics Inst., <https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/> [<https://perma.cc/W7FD-5P6B>].

²⁵⁷ Int'l Org. for Standardization, ISO/IEC TR 24741:2018, *Information Technology—Biometrics—Overview and Application* (2018), <https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en> [<https://perma.cc/P3RB-56RM>]; see *What Is Biometrics?*, Biometrics Inst., <https://www.biometricsinstitute.org/what-is-biometrics/> [<https://perma.cc/2APY-5WBM>].

²⁵⁸ D. Gowtami Annapurna et al., *Gender Identification from Facial Features*, 15 *Int'l J. Innovations Eng'g & Tech.* 5 (2020), <https://ijiet.com/wp-content/uploads/2020/03/21.pdf> [<https://perma.cc/9M69-GXZ8>].

²⁵⁹ See, e.g., Jesse M. Charlton et al., *Learning Gait Modifications for Musculoskeletal Rehabilitation: Applying Motor Learning Principles to Improve Research and Clinical Implementation*, 101 *Physical Therapy*, Feb. 2021, at 2, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7899063/> [<https://perma.cc/Jf9W-CKDA>]; Javier Galbally et al., *A Study of Age and Ageing in Fingerprint Biometrics*, 14 *IEEE Transactions on Info. Forensics & Sec.* 1351 (2019), <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=8509614> [<https://perma.cc/FK88-THWY>]; *Physiological and Behavioural Biometrics*, Biometrics Inst., <https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/> [<https://perma.cc/8QE4-LW74>].

physiological biometric measurement is compromised, it can be impossible to change.²⁶⁰ Additionally, covert or passive measures such as surveillance cameras or latent fingerprints can capture biometric data without the targeted individual's knowledge.²⁶¹ However, certain types of behavioral biometric information, such as gait and voice, may be possible to change, though it may be difficult.

- **Availability:** Moderate sensitivity. Certain types of biometric data could be widely available in certain records, such as facial features derived from photographs on the internet.²⁶² Others, such as gait, are not widely available. Reliable bulk biometric databases remain difficult enough to assemble that they are seen as important national security assets.²⁶³

- **Volume:** Varied sensitivity. Video surveillance footage, which could be used to derive biometric information from tens or hundreds of individuals walking by the camera, collects up to 30 frames of potentially high-definition photo images per second.²⁶⁴ In contrast, a single human face can be represented by approximately 80 distinct nodal points, each of which could be represented as a single number.²⁶⁵

- **Velocity:** Moderate sensitivity. Certain types of biometric information can change, for example as individuals age or change weight.²⁶⁶ However,

because biometrics are physical, many will remain substantially the same over a person's lifetime. For example, fingerprints are constant over a lifetime, and iris patterns remain largely stable even as children grow.²⁶⁷

- **Quality:** Varied sensitivity. Factors including the quality of sensors and environmental conditions can affect the reliability of readings stored in databases.²⁶⁸ The complex nature of most biometric data systems means data quality can be further affected by obscured or degraded characteristics, subject behavior, data collection, compression and sampling efforts, feature extraction issues, matching errors, and administrative and database problems.²⁶⁹ As a result, the value of a bulk biometric data source to an analyst will depend on the quality of the underlying dataset.

3. Precise Geolocation Data

The Department of Justice assesses that precise geolocation data is the third most sensitive category of sensitive personal data. To conduct the analysis, the Department considered geolocation measurements obtained by a variety of means, including Global Positioning Systems ("GPS"), cell tower proximity, Wi-Fi networks, Bluetooth signals, and IP geolocation.²⁷⁰ It considered use cases where sets of geolocation points were linked to a specific device and included timestamps; were linked to a specific device but did not include timestamps; and were not linked to either specific devices or timestamps but instead represented an aggregate picture of where individuals were taking devices. In many—but not all—instances across these use cases, precise

geolocation data is moderately to highly sensitive based primarily on the purpose, changeability, volume, and quality characteristics below:

- **Purpose:** High sensitivity. Analysts can use geolocation data to derive detailed information about patterns of life, as well as other types of sensitive personal data such as home address and place of work.²⁷¹ They may use it to identify influential individuals for blackmail and coercion, physically map and target sensitive sites and high-risk personnel, create near-real-time situational awareness, and target offensive cyber operations.²⁷² They may also use it to identify a specific person, such as who goes to a residence, as well as large numbers of people, such as everyone who goes to the Pentagon.²⁷³

- **Changeability:** Moderate sensitivity. Geolocation data is technically collected (*i.e.*, derived from signals and electronic devices). As a result, individuals can spoof or alter this data with some effort. One common way to affect the apparent location of a device is through a Virtual Private Network ("VPN"), which can affect the apparent location of a device based on its IP address, while connected applications that can spoof a GPS location on a cellphone are readily available online.²⁷⁴ More complicated spoofing techniques require transmission of a false radio signal to override a legitimate GPS signal.²⁷⁵

- **Control:** Moderate sensitivity. Precise geolocation data is collected from electronic devices, which an individual can typically leave behind or be separated from. However, these devices usually collect geolocation data in the background, often beyond the control or visibility of the individual, using software services built into device operating systems.²⁷⁶ These sensors are

²⁶⁰ See Off. of the Victorian Info. Comm'r, *Biometrics and Privacy—Issues and Challenges* (July 2019), <https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/> [<https://perma.cc/ME8R-XWJU>]; Is Biometric Information Protected by Privacy Laws?, Bloomberg L. (June 20, 2024), <https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/> [<https://perma.cc/56EZ-69HK>].

²⁶¹ *Id.*

²⁶² Katherine Tangelakis-Lippert, *Clearview AI Scraped 30 Billion Images from Facebook and Other Social Media Sites and Gave Them to Cops: It Puts Everyone into a 'Perpetual Police Line-Up'*, Bus. Insider (Apr. 2, 2023), <https://www.businessinsider.com/clearview-scraped-30-billion-images-facebook-police-facial-recognition-database-2023-4> [<https://perma.cc/6LZG-NBUT>].

²⁶³ Kelsey Atherton, *The Enduring Risks Posed by Biometric Identification Systems*, Brookings Inst. (Feb. 9, 2022), <https://www.brookings.edu/articles/the-enduring-risks-posed-by-biometric-identification-systems/> [<https://perma.cc/65DW-832R>].

²⁶⁴ Optiview, *A Practical Guide to CCTV Video Resolutions*, <https://optiviewusa.com/cctv-video-resolutions/> [<https://perma.cc/K24Y-MJA5>].

²⁶⁵ Chris De Silva et al., NEC Corp., *It's All About the Face: Face Recognition* (2013), https://www.nec.com/en/global/solutions/safety/pdf/NEC-FR_white-paper.pdf [<https://perma.cc/P5PJ-8LQ2>].

²⁶⁶ Joel R. McConvey, *How Aging, Injury and Capture Impact the Challenge of Change in Biometric Identifiers*, Biometric Update (Dec. 25, 2023), <https://www.biometricupdate.com/202312/how-aging-injury-and-capture-impact-the-challenge-of-change-in-biometric-identifiers> [<https://perma.cc/285T-5L2E>].

²⁶⁷ Justin Lee, *New Research Proves that Fingerprint Accuracy Remains Unchanged Over Time*, Biometric Update (June 30, 2015), <https://www.biometricupdate.com/201506/new-research-proves-that-fingerprint-accuracy-remains-unchanged-over-time> [<https://perma.cc/C95U-DSSS>]; Priyanka Das et al., *Iris Recognition Performance in Children: A Longitudinal Study*, 3 IEEE Transactions on Biometrics, Behav. & Identity Sci. 138 (Jan. 13, 2021), <https://ieeexplore.ieee.org/document/9321488> [<https://perma.cc/X2KJ-G4EE>].

²⁶⁸ Off. of the Victorian Info. Comm'r, *supra* note 260.

²⁶⁹ Austin Hicklin & Rajiv Khanna, Mitretek Sys., *The Role of Data Quality in Biometric Systems* (Feb. 9, 2006), <https://citeserx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a892c6e2cf2fdd94bab672a987940f2bb6996119> [<https://perma.cc/4YWP-KDWH>].

²⁷⁰ Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, Bus. L. Today (Mar. 25, 2019), <https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/> [<https://perma.cc/MWB2-7BWN>]; Daniel Ionescu, *Geolocation 101: How It Works, the Apps, and Your Privacy*, PCWorld (Mar. 29, 2010), <https://www.pcworld.com/article/511772/geolo.html> [<https://perma.cc/C28D-XYXU>].

²⁷¹ Hsu, *supra* note 43.

²⁷² Hazelrig, *supra* note 4.

²⁷³ Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases*, The Guardian (Jan. 28, 2018), <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases> [<https://perma.cc/J7N3-BHKU>]; Hsu, *supra* note 43.

²⁷⁴ See, e.g., Shweta, *What a VPN Hides (And What It Doesn't)*, Forbes Advisor (June 5, 2024), <https://www.forbes.com/advisor/business/software/what-does-vpn-hide/> [<https://perma.cc/MF23-SYK7>]; Tim Fisher, *How to Fake a GPS Location on Your Phone*, Lifewire (June 18, 2024), <https://www.lifewire.com/fake-gps-location-4165524> [<https://perma.cc/ZB8S-X3ZB>].

²⁷⁵ *What Is GPS Spoofing and How Do You Defend Against It?*, Okta (Aug. 16, 2023), <https://www.okta.com/identity-101/gps-spoofing/> [<https://perma.cc/ZM7K-4349>].

²⁷⁶ See, e.g., *Build Location-Aware Apps*, Google for Developers (July 1, 2024), <https://developer.android.com/develop/sensors-and-location/location> [<https://perma.cc/LVM6-TZGK>].

present in an increasing number of devices, including phones, cars, and smartwatches.²⁷⁷

- **Availability:** Moderate sensitivity. Commercial companies collect geolocation data in large volumes and consider it valuable for identifying consumers and evaluating their behavior.²⁷⁸ It is subject to increasing regulatory protection, with laws passed in California and Virginia to regulate precise geolocation data, and Massachusetts considering a law that would ban the sale of user location data as of the date of the proposed rule.²⁷⁹ These restrictions make the data more sensitive because it is less generally available.

- **Volume:** High sensitivity. Technically, geolocation is often a combination of latitude and longitude, along with related fields such as timestamps, accuracy measurements, device identifiers, and IP addresses.²⁸⁰ This string of information requires relatively little space to store and is simple, and geolocation information is often collected in very large quantities to be meaningful for commercial or research purposes at scale. For example, one provider of geolocation data advertised a dataset covering 1 year with 214 million daily data points, suggesting the relatively small amount of information contained in each data point.²⁸¹ In general, geolocation data is sold in many differently sized sets and different ways, ranging from small,

precisely targeted geofenced areas using ads to global datasets containing records on billions of devices.²⁸²

- **Velocity:** Low sensitivity. Commercially available geolocation datasets typically offer 1 to 5 years of data.²⁸³ This indicates a relatively limited lifespan and may vary. Compared to other types of data under consideration, this data is less valuable and useful over long time periods due to other factors such as volume.

- **Quality:** Moderate sensitivity. Analysts can purchase geolocation data in a variety of formats, including real-time and historical data, over a variety of geographic locations.²⁸⁴ Analysts can determine valuable information about patterns of life from this information.²⁸⁵ However, this data is generally provided as raw, unprocessed “pings,” which require machine analysis to derive useful insights.

4. Personal Health Data

The Department of Justice assesses that personal health data is the fourth most sensitive category of sensitive personal data. In conducting the analysis, the Department considered personal health records as well as claims and billing information. Unlike the three categories discussed in parts V.A.1, V.A.2, and V.A.3 of this preamble, personal health data contains a much more heterogeneous set of data, with sensitivity varying across the evaluated characteristics. Based primarily on the purpose, control, and availability characteristics described below, the Department assesses personal health data to be moderately sensitive overall:

- **Purpose:** Moderate sensitivity. Personal health records contain a variety of information, including information on medical history, medications, treatments, tests, immunizations, implanted devices, and associated data.²⁸⁶ They may also

contain financial information (where related to billing), and covered personal identifiers.²⁸⁷ As a result, analysts could use them for a variety of identifying, characterizing, and categorizing activities, including identifying vulnerabilities in an individual's background that could be leveraged to coerce that individual into recruitment by a foreign intelligence service. For example, healthcare records can reveal healthcare providers and embarrassing or expensive medical conditions that help our adversaries target individuals and groups for intelligence recruitment, espionage, and influence. Severe injuries, chronic medical conditions, and mental health information provide points of leverage for coercion, blackmail, and influence. In extreme circumstances, countries of concern could even exploit information gathered from personal health records to target individuals using certain medical devices or taking certain prescriptions.²⁸⁸

- **Changeability:** Moderate sensitivity. Many medical records contain objective information, such as laboratory test results and physical measurements. They also contain information that an individual could falsify by providing an inaccurate medical history, describing false symptoms, and hiding certain behaviors or habits to avoid negative consequences, get access to medication or insurance, or for simple emotional reasons such as guilt or shame.²⁸⁹

- **Control:** Moderate sensitivity. Personal health records are often based on information provided by an individual and subject to strict privacy laws that help ensure individual control of this data.²⁹⁰ As a result, this data may not be available without an individual's permission. However, it is typically maintained by third parties, such as doctors, hospitals, and insurance systems, placing it in record systems outside an individual's direct control.²⁹¹

²⁷⁷ Rob Gabriele, *170 Million Americans Own GPS Tracking Devices; Market to Grow Over Next Six Months*, SafeHome.org (July 15, 2024), <https://www.safehome.org/gps-industry-outlook-statistics/> [<https://perma.cc/C3ZY-2WCA>]; Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, *supra* note 228.

²⁷⁸ Robert Archacki et al., *Unlocking Value with Location Intelligence*, Bos. Consulting Grp. (Feb. 4, 2021), <https://www.bcg.com/publications/2021/leveraging-location-intelligence-across-industries> [<https://perma.cc/XM6A-NQRG>].

²⁷⁹ BCLP, *Precise Geolocation: Recent Trends and Enforcement*, JD Supra (Mar. 30, 2023), <https://www.jdsupra.com/legalnews/precise-geolocation-recent-trends-and-8834493/> [<https://perma.cc/4YMR-J8NE>]; Will Shanklin, *Massachusetts Weighs Outright Ban on Selling User Location Data*, Engadget (July 10, 2023), <https://www.engadget.com/massachusetts-weighs-outright-ban-on-selling-user-location-data-191637974.html> [<https://perma.cc/X43U-Q35P>].

²⁸⁰ *Geolocation Data 101: A Guide to Powerful Place-Based Insights*, Zartico, <https://www.zartico.com/blog/guide-to-using-geolocation-data#where-does-geolocation-come-from> [<https://perma.cc/M6SG-5PRF>]; see Amended Complaint ¶¶ 27–28, *Fed. Trade Comm'n v. Kochava, Inc.*, No. 22-cv-00377 (D. Idaho 2023), ECF No. 26, https://www.ftc.gov/system/files/ftc_gov/pdf/26AmendedComplaint%28unsealed%29.pdf [<https://perma.cc/4KWL-ZEJE>].

²⁸¹ *Factori Products*, Datarade, <https://datarade.ai/data-providers/lifesight/data-products> [<https://perma.cc/3XEP-9BVH>].

²⁸² See Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, Markup (Sept. 30, 2021), <https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data> [<https://perma.cc/3TUV-HHGV>].

²⁸³ See, e.g., *What Is Mobile Location Data? Definition, Uses, Datasets, & Providers*, Datarade (Sept. 23, 2024), <https://datarade.ai/data-categories/mobile-location-data> [<https://perma.cc/X8FH-GY9Y>].

²⁸⁴ Sherman et al., *supra* note 6.

²⁸⁵ See, e.g., Thompson & Warzel, *supra* note 44.

²⁸⁶ See, e.g., *The Guide to Getting & Using Your Health Records*, Off. Nat'l Coordinator for Health Info. Tech., <https://www.healthit.gov/how-to-get-your-health-record/> [<https://perma.cc/K2ZH-7VTW>]; *Dick Cheney Feared Assassination Via Medical Device Hacking: 'I Was Aware of the Danger'*, ABC News (Oct. 19, 2023), [https://abcnews.go.com/US/vice-president-dick-cheney-](https://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434)

[feared-pacemaker-hacking/story?id=20621434](https://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434) [<https://perma.cc/Q779-MESR>].

²⁸⁷ See Trisha Torrey, *How to Get Your Medical Records*, Verywell Health (May 11, 2023), <https://www.verywellhealth.com/how-to-get-copies-of-your-medical-records-2615505> [<https://perma.cc/2VY5-PXJA>].

²⁸⁸ See, e.g., *Dick Cheney Feared Assassination Via Medical Device Hacking*, *supra* note 286.

²⁸⁹ John J. Palmieri & Theodore A. Stern, *Lies in the Doctor-Patient Relationship*, 11 Prim. Care Companion J. Clinical Psychiatry 163, 165 (2009), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2736034/> [<https://perma.cc/AH9L-FD5K>].

²⁹⁰ *Health Information Privacy Law and Policy*, Off. Nat'l Coordinator for Health Info. Tech., <https://www.healthit.gov/topic/health-information-privacy-law-and-policy> [<https://perma.cc/2XHZ-UPFE>].

²⁹¹ Trisha Torrey, *Who Can Access Your Medical Records?* VeryWell Health (Mar. 11, 2022), <https://www.verywellhealth.com/who-can-access-your-medical-records/>

- **Availability:** High sensitivity. Personal health data is considered highly private and is well protected by privacy legislation. Data is shared as part of clinical trials, but access to such data is recognized as a continuing challenge within the healthcare community.²⁹² Furthermore, health data remains highly valuable to cyber criminals on the dark web, as compared to data such as credit card numbers and Social Security numbers, pointing to the general difficulty in obtaining this information in bulk quantities.²⁹³

- **Volume:** Varied sensitivity. As discussed, personal health data generally contains large amounts of data of varying formats and structures, ranging from the highly structured and technical information in lab results, to the more unstructured data, such as x-ray images and magnetic resonance imaging scans. Such variation means the amount of information may range from very small, such as the results of a single test, to very voluminous, such as a complete medical history. The volume of elements such as progress notes is also increasing, further expanding variability.²⁹⁴

- **Velocity:** Moderate-to-low sensitivity. As discussed, personal health data contains a variety of different types of information, but many of these records are lab tests, diagnostics, and other treatment information that may be less useful to analysts. However, certain pieces of information of enduring value—such as information on chronic disease and hereditary conditions—may be mixed in with other pieces of information, somewhat raising the overall sensitivity.

- **Quality:** Low sensitivity. Personal health records vary widely in terms of data type, quantity, precision, and consistency,²⁹⁵ making personal health

data less suitable for automated machine analysis than other types of data. Analysts or automated systems may not be able to draw useful conclusions without a great deal of context surrounding highly technical diagnostic data. “Note bloat”—unnecessarily lengthy information—is a recognized issue within the medical community, indicating the ongoing challenge of obtaining quality, valuable information.²⁹⁶ Much of the useful information may be contained in generalized diagnostics, particularized forms, and images that analysts may not be able to easily transform into useful conclusions, particularly if patients are not being truthful.²⁹⁷

5. Personal Financial Data

The Department of Justice assesses that personal financial data is the fifth most sensitive category of sensitive personal data. To conduct the analysis, the Department considered data linked directly with personal financial accounts (e.g., records with account numbers and names), data included in financial applications such as data used to apply for mortgages or loans (e.g., credit history), and related data routinely exchanged during a transaction (e.g., account numbers, routing numbers). Personal financial data includes records that are confidential (e.g., complete bank account information, including name). Personal financial data includes a variety of data types with varying sensitivity and moderate sensitivity overall based primarily on the purpose, changeability, availability, and quality characteristics below:

- **Purpose:** Moderate sensitivity. Financial institutions must uniquely identify and verify the identity of individuals both to track financial flows and to comply with regulations such as anti-money laundering.²⁹⁸ In order to do this, they store a mix of data that is useful for identifying individuals. Other categories of financial data, such as credit or consumer reports, provide data that can be useful for characterizing behavior or grouping individuals into categories.²⁹⁹ Today, most individuals leave a digital trail through their

purchases and other financial activities, revealing behaviors, activities, and patterns of life.³⁰⁰ They provide insight into their financial condition, personal preferences, habits, and concerns through brokerage activity, savings account information, and insurance records. Foreign intelligence services could derive other sensitive personal data, such as workplace and daily life habits, including vulnerabilities in an individual’s personal life that may be leveraged to coerce that individual into recruitment by a foreign intelligence service, from financial transaction data.³⁰¹ Use of a financial instrument to purchase products or services reveals spending habits and patterns of life that help our adversaries target individuals and groups for intelligence recruitment, espionage, and influence. Debt, creditworthiness, and financial troubles provide points of leverage for coercion, blackmail, and influence.

- **Changeability:** Moderate-to-high sensitivity. Financial information on an individual is recorded and maintained by financial institutions, which depend on possessing reliable and accurate information. However, individuals do have some ability to change their financial identifiers by, for example, closing one account and opening another. Additionally, the continued existence of money laundering as a law enforcement issue demonstrates that financial information can be, to some extent, controlled or manipulated by an individual.³⁰²

- **Control:** Moderate sensitivity. Financial information and records are managed and maintained by centralized financial institutions. Credit cards and checks leave a history with the financial institution, but individuals have the power to pay in cash or other anonymized methods and not reveal transactions to these financial institutions.³⁰³ Ultimately, this

²⁹² www.verywellhealth.com/who-has-access-to-your-medical-records-2615502 [https://perma.cc/BX52-5URC].

²⁹³ Sonali Kochhar et al., *Clinical Trial Data Sharing: Here’s the Challenge*, 9 *BMJ Open* (2019), <https://bmjopen.bmj.com/content/9/8/e032334> [https://perma.cc/392P-PVKN].

²⁹⁴ Sanjay Cherian, *Healthcare Data: The Perfect Storm*, *Forbes* (Jan. 14, 2022), <https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm> [https://perma.cc/DR6V-D7QY].

²⁹⁵ Adam Rule et al., *Length and Redundancy of Outpatient Progress Notes Across a Decade at an Academic Medical Center*, 4 *JAMA Network Open* (July 19, 2021), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8290305/> [https://perma.cc/7NA8-7Y9N].

²⁹⁶ See, e.g., Alex Roehrs et al., *Personal Health Records: A Systematic Literature Review*, 19 *J. Med. Internet Res.* under sections titled Overview, Electronic Health Records, and Personal Health Records (Jan. 6, 2017), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5251169/> [https://perma.cc/T6MA-29VB].

²⁹⁷ See *Cures for Note Bloat*, ForeSee Medical (June 9, 2023), <https://www.foreseemed.com/blog/note-bloat-cures> [https://perma.cc/AB34-CYGL].

²⁹⁸ Palmieri & Stern, *supra* note 289.

²⁹⁹ Frequently Asked Questions (FAQ) Regarding Anti-Money Laundering (AML), FINRA, <https://www.finra.org/rules-guidance/key-topics/aml/fq> [https://perma.cc/Z9TK-WBRW].

³⁰⁰ Barry Paperno, *How Credit Scores Predict Your Behavior*, *Yahoo! Finance* (May 24, 2013), <https://finance.yahoo.com/news/credit-scores-predict-behavior-113006994.html> [https://perma.cc/GC4S-6H67].

³⁰¹ Nicholas Anthony, Policy Analysis No. 945, *The Right to Financial Privacy*, CATO Inst. (May 2, 2023), <https://www.cato.org/policy-analysis/right-financial-privacy#conclusion> [https://perma.cc/5K3E-BUPF] (“Today, technology is an integral part of modern life: Americans use credit or debit cards for nearly all purchases, acquire loans directly on their phones, and leave a digital trail nearly everywhere they go.”).

³⁰² Carola Westermeier, *Money Is Data—The Platformization of Financial Transactions*, 23 *Info., Comm’n & Soc’y* 2047, 2050–52 (2020), <https://www.tandfonline.com/doi/full/10.1080/1369118X.2020.1770833> [https://perma.cc/TD9J-UF9U].

³⁰³ Examples of Money Laundering Techniques, LexisNexis (May 4, 2023), <https://www.lexisnexis.com/blogs/gb/b/compliance-risk-due-diligence/posts/examples-money-laundering> [https://perma.cc/6MHE-U83S].

³⁰⁴ See, e.g., Edvardas Mikalauskas, *The Ultimate Guide to Safe and Anonymous Online Payment*

information reflects the activity of individuals, leaving it partly in their control.

- **Availability:** Moderate sensitivity. The sharing of certain types of information maintained by financial institutions is controlled by privacy regulations.³⁰⁴ However, credit card, debit card, and bank account numbers, and other financial identifiers and information, are routinely exchanged as a matter of course in commercial transactions; credit reports are regularly used by financial institutions and businesses as part of background checks; and transaction data is provided to marketing and third-party data analytics organizations.³⁰⁵ Credit cards and online financial account credentials can command between \$15 and \$200 on the dark web, as compared with Social Security numbers, which command less than \$10.³⁰⁶

- **Volume:** Moderate-to-low sensitivity. Over 100 million credit card transactions occur in the United States each day.³⁰⁷ While each transaction contains a small amount of information, this total transaction volume represents a massive dataset that analysts must mine to achieve useful results. Other types of information, such as data in credit reports, can contain information in a wide variety of formats that may be bulkier to manage and store.

- **Velocity:** Varied sensitivity. Analysts can use certain pieces of data, such as long-term loans, for a very long time. However, other pieces of information, such as information on individual transactions, may lose their value to an analyst over a short period of time.

- **Quality:** Moderate sensitivity. Analysts usually value personal financial data not for the information

itself, but for what it can reveal about an individual's behavior.³⁰⁸ As a result, some analysis is usually required to make it useful. Additionally, financial records such as credit reports can contain inaccurate information or make erroneous connections between individuals and assets.³⁰⁹

6. Covered Personal Identifiers

The Department of Justice assesses that covered personal identifiers are the sixth most sensitive category of sensitive personal data. Covered personal identifiers come from a variety of contexts and are of varying quality. For example, people have used certain types of covered personal identifiers (e.g., Social Security numbers) for decades, and numerous entities collect them, making them more available than other categories of data. Other types of covered personal identifiers (e.g., advertising IDs) are distributed widely and only useful when collected in very large volumes and linked to other pieces of data.³¹⁰ The variety and variability of this category makes it inherently more difficult to characterize across the board than other categories. Based primarily on the purpose, changeability, and velocity characteristics below, the Department assesses covered personal identifiers to have low sensitivity relative to the other categories of sensitive personal data:

- **Purpose:** Moderate sensitivity. As stated in the proposed rule, covered personal identifiers are pieces of data that can be useful for identifying individuals, making them inherently sensitive. However, covered personal identifiers include pieces of information that are uniquely identifying (e.g., Social Security numbers) as well as those that are deliberately designed to be anonymous (e.g., advertising identifiers).³¹¹ Covered personal

identifiers and unique IDs can be used to link other datasets containing more directly exploitable information.³¹² For example, they can help link databases of habitual visitors to gambling sites with debt collection records or a database of government records. They could link advertising IDs, IP addresses, and SIM card numbers to personal mobile devices, home addresses, and government mobile devices. However, in general, covered personal identifiers are primarily useful as identifiers, reducing their overall sensitivity because they themselves reveal little information.

- **Changeability:** Moderate-to-low sensitivity. As a category, they cover a range of data points that differ in terms of ease of change. For example, Social Security numbers are difficult to change, requiring evidence that an individual is in danger from domestic violence, other abuse, or identity theft.³¹³ In contrast, account identifiers and passwords can be changed at a user's discretion. Many covered personal identifiers, including passport numbers, device IMEIs, and addresses, do change on a semi-regular basis as passports are reissued, devices are replaced, and individuals move.

- **Control:** Moderate-to-low sensitivity. Some covered personal identifiers—particularly government-issued identifiers such as Alien Registration Numbers and Social Security numbers or financial identifiers such as account information—are fully outside the control of an individual. Others are fully controlled by an individual, including email addresses and account identifiers. Still other covered personal identifiers such as phone numbers may be issued by a third party, but an individual can change them at will.

- **Availability:** Low sensitivity. Covered personal identifiers such as phone numbers and home addresses have been used as unique identifiers in a variety of systems, ranging from customer loyalty trackers to tax records. Many are available as part of the public record.³¹⁴ Technical covered personal

Methods in 2024, Cybernews (Dec. 12, 2023), <https://cybernews.com/resources/the-ultimate-guide-to-safe-and-anonymous-online-payment-methods/> [<https://perma.cc/5EX5-8YFC>].

³⁰⁴ See, e.g., Gramm-Leach-Bliley Act tit. V, 15 U.S.C. 6801–09; *Privacy Rule Handbook*, Fed. Deposit Ins. Corp. (Aug. 11, 2023), <https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/index.html> [<https://perma.cc/NK9U-MVFF>].

³⁰⁵ See, e.g., R.J. Cross, *How Mastercard Sells Its 'Gold Mine' of Transaction Data*, U.S. PIRG (June 17, 2024), <https://pirg.org/edfund/resources/how-mastercard-sells-data/> [<https://perma.cc/N4T8-P3ZG>].

³⁰⁶ Paul Bischoff, *Dark Web Prices for Stolen PayPal Accounts Up, Credit Cards Down: Report*, Comparitech (Aug. 12, 2023), <https://www.comparitech.com/blog/vpn-privacy/dark-web-prices/> [<https://perma.cc/88HM-2VZK>].

³⁰⁷ Erica Sandberg, *The Average Number of Credit Card Transactions per Day & Year*, iMerchant Direct (Nov. 5, 2020), <https://www.imerchantdirect.com/news/number-of-credit-card-transactions-per-day-year> [<https://perma.cc/NVZ8-M3PR>].

³⁰⁸ Alessio Balduini et al., *Combining Financial and Behavioral Information to Predict Defaults for Small and Medium-Sized Enterprises: A Dynamic Weighting Approach*, Moody's Analytics (Sept. 2017), <https://www.moodyanalytics.com/articles/2017/combining-financial-and-behavioral-information> [<https://perma.cc/X8DS-WPZB>]; Luke Goldsten, *Rollups: The Big Data Machine Driving Online Sports Betting*, Am. Prospect (Apr. 4, 2022), <https://prospect.org/power/rollups-big-data-machine-driving-online-sports-betting/> [<https://perma.cc/AZ97-H4TW>].

³⁰⁹ *Is My Credit Report Accurate? For Over 40 Million Americans, the Answer Is No*, Am. Bankr. Inst., <https://www.abi.org/feed-item/is-my-credit-report-accurate-for-over-40-million-americans-the-answer-is-no> [<https://perma.cc/462F-UMEN>].

³¹⁰ Priv. Int'l, *Examples of Data Points Used in Profiling*, 3–12 (2018), https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf [<https://perma.cc/LF63-XUDT>].

³¹¹ *Are Advertising Unique IDs Anonymous?*, Panda Sec. (July 21, 2021), <https://>

www.pandasecurity.com/en/mediacenter/advertising-ids/ [<https://perma.cc/ANA8-JE2H>].

³¹² Priv. Int'l, *supra* note 310.

³¹³ *Is It Possible to Get a New Social Security Number?*, AARP (Apr. 8, 2022), <https://www.aarp.org/retirement/social-security/questions-answers/new-number.html> [<https://perma.cc/X759-P6LF>].

³¹⁴ See, e.g., Brian Fung, *DC Makes It Shockingly Easy to Snoop on Your Fellow Voters*, Wash. Post (June 14, 2016), <https://www.washingtonpost.com/news/the-switch/wp/2016/06/14/d-c-s-board-of-elections-makes-it-shockingly-easy-to-snoop-on-your-fellow-voters/> [<https://perma.cc/5A2F-VNAZ>]; How Your Phone Number is Exposed: Phone

identifiers such as IP addresses are necessarily widely available as a matter of technical necessity.

- **Volume:** Low sensitivity. Online data-brokerage firms advertise datasets of mobile advertising IDs containing hundreds of millions to billions of records.³¹⁵ Tens of millions of Social Security numbers are routinely found on the dark web, suggesting the large volumes in which these data points are stored and shared by companies.³¹⁶ Companies such as Twitter (now X) hold the phone numbers and email addresses of more than 100 million individuals.³¹⁷ As these examples demonstrate, covered personal identifiers are routinely held and used in massive volumes. At such large volumes, this type of data tends to be less sensitive because it reduces the ability of an adversary to identify a specific individual (such as distinguishing between people who have the same name, have lived at the same address, etc.), absent other data that can be used to narrow down and link the identifiers to individuals.

- **Velocity:** Moderate-to-low sensitivity. Covered personal identifiers such as Social Security numbers and names can be quite persistent, changing infrequently or not at all over an individual's lifetime. Covered personal identifiers like mobile advertising IDs cease to be useful in as little as 7 to 8 months.³¹⁸ In general, the useful lifespan of many covered personal identifiers is limited. Only a few covered personal identifiers follow an individual over a lifetime, while many have lifespans measured in weeks to months, reducing the overall sensitivity of the category.

- **Quality:** Low sensitivity. For example, an individual user may have multiple mobile advertising IDs across multiple devices. Advertising specialists assert that 91 percent of companies have data quality issues, including from

outdated data and user-error mistakes.³¹⁹ Individuals may also make and use throwaway email accounts to avoid spam.³²⁰ Major technology companies, such as Apple, offer the ability to create relay emails specifically to obfuscate certain underlying covered personal identifiers.³²¹

B. Grouping the Categories Into Tiers by Similar Sensitivity

Based on this ranking, the Department grouped the categories of sensitive personal data into four tiers based on how similar or dissimilar, in terms of sensitivity, each category is compared to the other. Human genomic data, the most sensitive category, is unique and substantially more sensitive than biometric data due to its lower changeability and velocity. As a result, the Department placed human genomic data on its own in the first tier. While not as sensitive as human genomic data, biometric identifiers and precise geolocation data are generally more sensitive than either personal health or personal financial data because the data is more structured, making it more useful for machine-based analysis. Biometric identifiers and precise geolocation data also identify individuals with more precision than personal health data or personal financial data, making the results of machine-based analysis more valuable to human analysts. As a result, the Department grouped biometric identifiers and precise geolocation data together into the second tier and grouped personal financial data and personal health data together into the third tier. Finally, compared to personal financial data or personal health data, covered personal identifiers are more varied in terms of use, making them less useful to foreign intelligence services. As a result, the Department grouped covered personal identifiers into the fourth tier.

To help verify the relative sensitivities and tiered groupings yielded by the seven-factor analysis, the Department compared the results of this analysis to other circumstances in

which the Federal Government or state governments have treated these categories of data as sensitive. To start, the Department examined over 50 transactions reviewed by CFIUS in which the government identified, and took action to address, a risk to national security posed by access to data by countries of concern or persons subject to their ownership, direction, jurisdiction, or control. The Department examined the types and volumes of data involved in each CFIUS transaction to identify the lowest volumes of data that the government identified as a risk to national security posed by each of these transactions, which served as proxy for how sensitive CFIUS has generally considered each category of data with respect to identified national security risks relating to that data.

In the case of personal financial data, personal health data, and covered personal identifiers, the Department was able to identify enough CFIUS transactions to present a reasonable sample. It identified the following approximate numbers as the lowest volumes identified by CFIUS as presenting a national security risk warranting action in the context of the specific transactions involving sensitive personal data that CFIUS reviewed:

- Personal financial data: 16,000 individuals
- Personal health data: 85,000 individuals
- Covered personal identifiers: 100,000 individuals

Based on these data points, the Department confirmed that its sensitivity analysis of these three categories was consistent with previous CFIUS national security assessments, at least in the specific contexts of those case-by-case CFIUS reviews.

Because there was not a sufficiently large sample of CFIUS matters for human genomic data, biometric data, or precise geolocation data, and because there does not appear to be another national security program with relevant quantitative or qualitative data on this topic, the Department examined how the Federal Government and States treat these three remaining categories under privacy laws to help verify the results of its seven-factor assessment. While privacy laws and national security laws generally address different challenges associated with sensitive personal data, as explained in part IV of this preamble, there is some overlap in the ultimate harms that both seek to address. These privacy-based analogues thus help provide some indication of the relative capability of each category of sensitive personal data to be exploited and used to cause harm.

Number Leaks, Nat'l. Cybersec. All. (Aug. 25, 2023), <https://staysafeonline.org/online-safety-privacy-basics/how-your-phone-number-is-exposed/> (<https://perma.cc/4CL3-9WRW>).

³¹⁵ See, e.g., MAID—PII Data: Best MAID—PII Datasets & Databases, Datarade, <https://datarade.ai/search/products/maid-pii-data> [<https://perma.cc/6NWA-YEBK>].

³¹⁶ See Chloe Veltman, Millions of Customers' Data Found on Dark Web in Latest AT&T Data Breach, NPR (Mar. 30, 2024), <https://www.npr.org/2024/03/30/1241863710/at-t-data-breach-dark-web> [<https://perma.cc/GAD6-R9KU>].

³¹⁷ See Complaint ¶ 29, *United States v. Twitter, Inc.*, No. 22-cv-03070 (N.D. Cal. May 25, 2022), ECF No. 1, https://www.ftc.gov/system/files/ftc_gov/pdp/2023062TwitterFiledComplaint.pdf [<https://perma.cc/4Z9J-5N3H>].

³¹⁸ 3 Uses for Mobile Advertising IDs to Copy Today, FullContact (Feb. 21, 2022), <https://www.fullcontact.com/blog/2022/02/21/mobile-advertising-id/> [<https://perma.cc/RR89-25HL>].

³¹⁹ Barley Laing, Why Customer Loyalty Starts with Clean Data, Advert. Week, <https://advertisingweek.com/why-customer-loyalty-starts-with-clean-data/> [<https://perma.cc/LJ3G-9M7F>].

³²⁰ Vivian McCall, How to Make a Throwaway Email Account to Avoid Spam from the websites You Sign up for, Bus. Insider (Dec. 22, 2020), <https://www.businessinsider.com/guides/tech/how-to-make-a-throwaway-email-account> [<https://perma.cc/27C4-DQJQ>].

³²¹ Communicating Using the Private Email Relay Service, Apple Dev., https://developer.apple.com/documentation/sign_in_with_apple/sign_in_with_apple_js/communicating_using_the_private_email_relay_service [<https://perma.cc/62AC-K9HK>].

In the case of human genomic data, the Department confirmed its assessment that this category of data is more sensitive than the three previously mentioned categories of data (covered personal identifiers, personal financial data, and personal health data) by evaluating comparative data from the FTC. The FTC has taken action against companies making deceptive privacy claims on cases involving the human genetic data of as few as 2,600 individuals.³²² In doing so, the FTC's complaint alleged that the company's "disregard for the basic security" of this data caused it to be "publicly exposed online,"³²³ revealing, among other things, "the level of risk for having or developing certain health conditions."³²⁴ The FTC also explained that this kind of "DNA data is sensitive because it's about who" a person is and is "so sensitive there's a law to protect you from discrimination based on genetic information when you're trying to get work or health insurance."³²⁵ In contrast, eight other FTC cases between 2021 and 2023 involving only covered personal identifiers, personal financial data, or personal health data involved data on one million or more individuals. The fact that the FTC took action in a case involving a significantly lower amount of compromised human genomic data supports the Department's assessment that human genomic data is substantially more sensitive than other data types.

In the case of biometric data, the Department confirmed its assessment with reference to State legislation. Three States—Washington,³²⁶ Texas,³²⁷ and Illinois³²⁸—have prohibited the sale, lease, or disclosure of biometric identifiers for purposes other than the provision of a specific commercial service, such as confirming a consumer-requested financial transaction. Massachusetts is also contemplating

such a law at the time of this proposed rule.³²⁹ The legislative action in these cases supports the Department's assessment that the transfer of even very small amounts of biometric data could prove highly damaging and thus that this data should be subject to a lower threshold.

In the case of geolocation data, the Department confirmed its assessment with reference to other government actions and reporting suggesting that even small amounts of geolocation data could be sensitive. The FTC charged two companies with causing injury to consumers by selling geolocation data that did not exclude information on sensitive locations, such as reproductive health clinics, places of worship, and addiction recovery facilities, and issued an order banning one of those companies from selling data without consumer consent.³³⁰ It also noted a data breach that involved 2,200 customers as part of its action against a company that harvested and shared data on people's physical movements.³³¹ The FCC has also levied fines for selling location data without customer consent.³³² The National Security Agency has noted the importance of limiting location data exposure.³³³ Congressional testimony has highlighted how commercial datasets can be used to precisely identify individuals in sensitive national security roles.³³⁴ The

Massachusetts State legislature is considering a bill at the time of this proposed rule that would ban the sale of phone location data.³³⁵ These comparisons all support the Department's assessment that this type of data is relatively more sensitive than other types of data, such as personal identifiers.

C. Proposed Bulk Thresholds for Each Tier

The Department of Justice developed numerical thresholds using the four tiers of sensitivity based on the number of individuals included in a dataset. In the ANPRM, the Department set the overall upper limit for these thresholds at one million individuals.³³⁶ As explained in the ANPRM, within each group, the Department set a potential upper and lower limit for each of the bulk thresholds, relying on orders-of-magnitude differences to develop preliminary judgments.

The Department sought input on the thresholds from the public in response to the ANPRM. Commenters expressed a wide variety of general concerns regarding the ranges of the potential bulk thresholds. Some commenters stated that the potential thresholds were too high, some that they were too low, some that the thresholds should be zero, and some that relying on thresholds was objectionable for other reasons. None of the comments, however, provided any actionable data points, use cases, or evidence that would support an alternative analytical framework or support adopting one particular threshold over another. Given that lack of specificity, the Department (along with the Department of Commerce) followed up individually with each commenter on this topic to seek any additional information available that informed their comments, as described in part III of this preamble. Those engagements did not yield any substantially new qualitative or quantitative information to reliably inform the selection of the proposed bulk thresholds.

Based on this analysis and public comment, the proposed rule would set the following bulk thresholds:

- *Human genomic data:* More than 100 U.S. persons.

³²² Complaint ¶ 28, *1Health.io, Inc.*, No. C-4798 (F.T.C. Sept. 6, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/1Health-Complaint.pdf [<https://perma.cc/W5SZ-CE3A>].

³²³ *Id.*

³²⁴ *Id.* ¶ 9.

³²⁵ Jim Kreidler, *Keep People's Sensitive DNA Information Private*, Fed. Trade Comm'n (June 16, 2023), <https://consumer.ftc.gov/consumer-alerts/2023/06/keep-peoples-sensitive-dna-information-private> [<https://perma.cc/VLC4-JYKM>].

³²⁶ Biometric Identifiers, Wash. Rev. Code 19.375, <https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true> [<https://perma.cc/2GZM-6FEG>].

³²⁷ Biometric Identifiers, Tex. Bus. & Com. Code 503.001, <https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm> [<https://perma.cc/F2WW-ZNR7>].

³²⁸ Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14 (2008), <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57> [<https://perma.cc/KMD8-QP8D>].

³²⁹ Act to Protect Biometric Information, H. 63, 193d. Gen. Ct. (Mass. 2003), <https://malegislature.gov/Bills/193/H63> [<https://perma.cc/26GH-JTCZ>].

³³⁰ Press Release, Fed. Trade Comm'n, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other> [<https://perma.cc/G6L6-G6XL>].

³³¹ Press Release, Fed. Trade Comm'n, *FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data* (Sept. 1, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data> [<https://perma.cc/SG4B-P6SV>].

³³² Derek B. Johnson, *FCC Takes \$200 Million Bite Out of Wireless Carriers for Sharing Location Data*, *CyberScoop* (Apr. 29, 2024), <https://cyberscoop.com/fcc-fines-wireless-carriers-200-million/> [<https://perma.cc/9UKR-4KXY>].

³³³ Nat'l Sec. Agency, PP-20-0535, *Limiting Location Data Exposure* (Aug. 2020), https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_limiting_location_data_exposure_final.pdf [<https://perma.cc/763S-8D5T>].

³³⁴ *Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy, Personal Safety, and National Security: Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Comm.*, 118th Cong. (2023) (statement of Justin Sherman, Senior Fellow and Research Lead, Data Brokerage Project, Sanford School of Public Policy), https://d1dth6e84htgma.cloudfront.net/Sherman_

Testimony 4_19_23_b40d947a8e.pdf [<https://perma.cc/9ACJ-ZT8R>].

³³⁵ Shanklin, *supra* note 279.

³³⁶ 89 FR 15786; cf. 31 CFR 800.241(a) (defining sensitive personal data to include "identifiable data" that a U.S. business collects or maintains "on greater than one million individuals" during a relevant 12-month period).

- *Biometric identifiers and precise geolocation data:* More than 1,000 U.S. persons.

- *Personal health data and personal financial data:* More than 10,000 U.S. persons.

- *Covered personal identifiers:* More than 100,000 U.S. persons.

The proposed bulk thresholds for all the categories of sensitive personal data except human genomic data are approximately the middle order of magnitude of the preliminary ranges identified in the ANPRM (e.g., the proposed threshold of 1,000 U.S. persons for biometric identifiers is the middle order of magnitude in the ANPRM's range of 100 to 10,000).³³⁷ Given the high sensitivity of human genomic data and the significant additional national security risks posed by human genomic data beyond counterintelligence risks, the proposed bulk threshold for human genomic data is the lowest order of magnitude in the preliminary range identified in the ANPRM. These proposed bulk thresholds are generally consistent with the order of magnitude of the minimum number of individuals in a dataset that the United States Government and other actors have treated as presenting a national security risk or as otherwise sensitive in the use cases and comparisons described in part V.B of this preamble.

The Department has considered whether the potential economic impact should affect our choice of thresholds for the purpose of defining “bulk” in these regulations and has determined it should not. First, the Department expects that the proposed rule will likely have some economic impact with respect to the prohibitions and restrictions on covered data transactions that have been determined to pose an unacceptable national security risk. The Department seeks to avoid and minimize unintended economic impacts on activities that do not present such national security risk. Neither the Department nor commenters have identified any actionable data or analysis suggesting that the choice of thresholds above zero is reasonably likely to result in unintended downstream impacts, as explained further in part VII.A of this preamble.

Second, based on the information provided to the Department and the Department's own analysis to date, it seems unlikely that the data or analysis would be detailed and representative enough to reasonably affect the choice of any specific thresholds within the ranges identified in the ANPRM. While

it is theoretically possible that choosing a higher (or lower) threshold would correspondingly affect both the numbers of captured transactions and the resultant costs, it is also possible that a meaningfully significant sample size of U.S. persons conducting prohibited and restricted transactions at volumes that generally exceed the upper end of the ranges in the ANPRM. There is no known, reliable qualitative or quantitative data that objectively favors adopting one of those likely possibilities at this time. For example, the average volume and distribution of volumes of human genomic data in covered data transactions between U.S. persons and countries of concern (or covered persons) is unknown. Because there is no data available to determine how often, for example, U.S. persons engage in such transactions at volumes above 1,000 U.S. persons as compared to 100, there is insufficient data to support a conclusion that the choice between 100 and 1,000 will meaningfully impact the number of transactions subject to the proposed rule. Accordingly, the Department declines to deviate from the risk-based analysis at this time.

VI. Interpretation of “Information or Informational Materials” in IEEPA

The Department proposes exercising its delegated statutory authority to define “information or informational materials” in 50 U.S.C. 1702(b)(3). Under IEEPA, “[t]he President may issue such regulations, including regulations prescribing definitions, as may be necessary for the exercise of the authorities granted by this chapter.”³³⁸ As courts have held, this provision explicitly “authorize[s] the Executive Branch to define the statutory terms of IEEPA,” and definitions promulgated by an agency that has been delegated this authority thus “carry the force of law” subject to judicial deference.³³⁹ Section 2(b) of the Order delegated this statutory authority to the Attorney General, and the Department proposes to exercise this authority to define “information or informational materials” as follows.

To implement 50 U.S.C. 1702(b)(3), the Department proposes defining “information or informational materials” as limited to expressive material and including publications, films, posters, phonograph records,

photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.³⁴⁰

The proposed rule would adopt two exclusions to this definition from existing OFAC regulations and clarify the definition's application to non-expressive materials. First, as previewed in the ANPRM and explained in detail below, the Department's proposed rule would clarify that the phrase “information or informational materials” is limited to expressive material, consistent with the purpose of 50 U.S.C. 1702(b)(3) to protect materials involving the free exchange of ideas from regulation under IEEPA. See § 202.226. The definition of “information or informational materials” does not include non-expressive data—i.e., data that is not intended to communicate any idea. The statute therefore permits the President, and the Attorney General as his delegatee under the Order, to regulate transactions involving the export of sensitive personal data or government-related data because this data is not expressive and therefore falls outside the scope of 50 U.S.C. 1702(b)(3) (“the Berman Amendment”). Second, the proposed definition would, consistent with OFAC regulations,³⁴¹ exclude information or informational materials that are not fully created and in existence at the date of the data transaction, or the substantive or artistic alteration or enhancement of information or informational materials, or the provision of marketing and business consulting services, including to market, produce or co-produce, or assist in the creation of information or informational materials. Third, the proposed definition incorporates the statutory exemption for items controlled for export to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by 18 U.S.C. chapter 37. The definition's application to non-expressive material and exclusion for materials not fully created and in existence are discussed in further detail below.

A. The Berman Amendment Is Intended To Protect the Free Exchange of Ideas

As noted above, § 202.226(a) of the proposed rule clarifies that “information or informational materials” is limited to expressive material rather than

³³⁸ 50 U.S.C. 1704.

³³⁹ *Zarmach Oil Servs., Inc. v. U.S. Dep't of Treas.*, 750 F. Supp. 2d 150, 156 (D.D.C. 2010); see also, e.g., *Holy Land Found. v. Ashcroft*, 333 F.3d 156, 162–63 (D.C. Cir. 2003); *United States v. Lindh*, 212 F. Supp. 2d 541, 562–63 & n.52 (E.D. Va. 2002); *Consarc Corp. v. U.S. Dep't of Treas., Off. of Foreign Assets Control*, 71 F.3d 909, 914–15 (D.C. Cir. 1995); *Consarc Corp. v. Iraqi Ministry*, 27 F.3d 695, 701 (D.C. Cir. 1994).

³⁴⁰ See, e.g., 31 CFR 544.304(a); 31 CFR 547.314(a)(1); 31 CFR 560.315(a); 31 CFR 576.306(a); 31 CFR 594.305(a).

³⁴¹ See, e.g., 31 CFR 560.210(c)(2), 560.210; *United States v. Amirnazmi*, 645 F.3d 564, 587 (3d Cir. 2011).

including every piece of data that might be characterized technically or colloquially as “information or informational materials.” This interpretation is consistent with the statute’s text and purpose, as demonstrated by legislative history and context, as well as judicial interpretations.

The text indicates that the Berman Amendment’s scope is properly limited to expressive materials. The provision restricts authority under IEEPA to regulate imports and exports “regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.” The specific examples accompanying the phrase “information and informational materials”—publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds—reflect Congress’ intent to protect the import or export of expressive speech and communicative works and mediums that may be carrying such expressive content. Although the statute provides that it is “not limited to” the articulated categories of information or specified mediums, the general term “information or informational materials” must be read in the context of those examples and should not be read to extend to dissimilar categories of information to those specifically articulated.³⁴² Because those examples overwhelmingly relate to expressive materials, the term “information or informational materials” is similarly limited under the established interpretive doctrine of *noscurtur a sociis*.

Congress enacted the Berman Amendment in 1988 and expanded it in 1994,³⁴³ and the initial version of the Berman Amendment passed in 1988 further supports this argument. It amended IEEPA to state that the President’s authority under the statute did not include the authority “to regulate or prohibit, directly or

indirectly . . . the importation from any country, or the exportation to any country, whether commercial or otherwise, of publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, or other informational materials. The specified items shared the common attribute of having the primary or exclusive purpose of conveying expressive information, and the catchall term “other informational materials” therefore carried that same limitation under the canon of *ejusdem generis*.³⁴⁴ This interpretation is further reinforced by the statute’s use of “other” before “informational materials,” indicating a commonality with the enumerated items. As further discussed below, there is no indication that, in amending the 1988 text, Congress sought to deviate from that understanding. The 1994 amendment that enacted the current version of the Berman Amendment was titled “Free Trade in Ideas,” indicating the provision’s reach and orientation toward expressive and communicative materials.³⁴⁵ The statute includes an accompanying provision providing “the sense of the Congress that the President should not restrict travel or exchanges for informational, education, religious, cultural, or humanitarian purposes or for public performances or exhibitions.”³⁴⁶ Together, these features confirm that the “information or informational materials” covered by the Berman Amendment are limited to the kind of expressive information that is central to the free exchange of ideas; the Berman Amendment is not intended to broadly encompass every piece of data that might technically or colloquially be described as “information.”

The proposed interpretation is consistent with Congress’ purpose in enacting the Berman Amendment. As one court explained shortly after the Berman Amendment’s initial enactment in 1988, there is an “obvious First Amendment orientation of the words

‘informational materials.’”³⁴⁷ Other courts have reached similar conclusions about the Berman Amendment’s purpose.³⁴⁸ And courts have consistently upheld the Executive Branch’s interpretations that distinguish between the types of informational materials that are covered or not covered, explaining that these reflect “permissible interpretation[s]” of the Berman Amendment “in light of IEEPA’s competing imperatives (*i.e.*, restricting material support for hostile regimes while encouraging the robust interchange of information).”³⁴⁹

These courts’ interpretations are grounded in the relevant historical and legislative context, which reflects Congress’ intent to protect the free exchange of ideas. Before the Berman Amendment’s enactment in 1988, the President’s broad authority to regulate commerce with foreign countries under IEEPA and its predecessor and wartime sibling, the Trading with the Enemy Act of 1917 (“TWEA”), did not contain any statutory exception for “information or informational materials,” and the implementing regulations and licenses generally did not exempt information or informational materials from trade embargoes. Before and during the Cold War, the Executive Branch exercised these authorities to prohibit the importation of and dealing in certain merchandise. These general regulations applied to books, newspapers, and magazines originating in countries designated as enemy nations, such as Cuba, Vietnam, China, North Korea, and

³⁴⁷ *Cernuda v. Heavey*, 720 F. Supp. 1544, 1550 (S.D. Fla. 1989).

³⁴⁸ See, e.g., *United States v. Amirnazmi*, 645 F.3d 564, 586–87 (3d Cir. 2011); *Kalantari v. NITV, Inc.*, 352 F.3d 1202, 1205 (9th Cir. 2003) (explaining that the “Berman Amendment was designed to prevent the executive branch from restricting the international flow of materials protected by the First Amendment”); *Marland v. Trump*, 498 F. Supp. 3d 624, 630 (E.D. Pa. 2020) (explaining that the Berman Amendment prevents the use of IEEPA to “prohibit or restrict directly or indirectly the import or export of information that is protected under the First Amendment to the U.S. Constitution”) (quoting H.R. Conf. Rep. No. 103–482, at 236); *United States v. Griffith*, 515 F. Supp. 3d 106, 116–17 (S.D.N.Y. 2021); *United States v. Alavi*, CR 07–429–PHX–NVW, 2008 WL 1989773, at *1 (D. Ariz. May 5, 2008) (similar).

Two recent cases examining the provision are not to the contrary, since both cases dealt with only expressive materials. See *TikTok Inc. v. Trump*, 507 F. Supp. 3d 92, 98–100, 105 (D.D.C. 2020); *Marland v. Trump*, 498 F. Supp. 3d at 636. The United States Government did not dispute that these expressive communications exchanged on TikTok were “informational materials” under the Berman Amendment. See *TikTok*, 507 F. Supp. 3d, at 108.

³⁴⁹ See *Amirnazmi*, 645 F.3d at 583, 587; see also *Griffith*, 515 F. Supp. 3d at 116–17; *Alavi*, 2008 WL 1989773, at *1.

³⁴² See, e.g., *Dubin v. United States*, 599 U.S. 110, 124–25 (2023) (“‘Under the familiar interpretive canon *noscurtur a sociis*, a word is known by the company it keeps.’ “[T]his canon is often wisely applied where a word is capable of many meanings in order to avoid the giving of unintended breadth to the Acts of Congress.”) *McDonnell v. United States*, 579 U.S. 550, 568–69 (2016) (citations omitted).

³⁴³ Omnibus Trade and Competitiveness Act of 1988, Public Law 100–418, 2502(b), 102 Stat. 1107, 1371–72; Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Public Law 103–236, sec. 525, 108 Stat. 382, 474 (1994).

³⁴⁴ See, e.g., *Bissonnette v. LePage Bakeries Park St., LLC*, 144 S. Ct. 905, 911 (2024) (explaining the “familiar canon of statutory interpretation” of *ejusdem generis* under which “courts interpret a general or collective term at the end of a list of specific items in light of any ‘common attributes shared by the specific items’”) (cleaned up); see also *Ali v. Fed. Bureau of Prisons*, 552 U.S. 214, 225 (2008) (explaining that “the inference embodied in *ejusdem generis*” is “that Congress remained focused on the common attribute when it used the catchall phrase”).

³⁴⁵ Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Public Law 103–236, sec. 525, 108 Stat. 382, 474 (1994); see, e.g., *Merit Mgmt. Grp., LP v. FTI Consulting, Inc.*, 138 S. Ct. 883, 893 (2018) (section headings “supply clues as to what Congress intended”).

³⁴⁶ Public Law 103–236, sec. 525(a), 108 Stat. at 474.

Cambodia.³⁵⁰ Absent a license granted by the Department of the Treasury, Americans could not import these materials into the United States or otherwise deal in them. To obtain such a license, an applicant had to show either that the books, magazines, and other materials were small-value “bona fide gift[s]” that did not provide “any direct or indirect financial or commercial benefit” to the enemy country or its nationals,³⁵¹ or that payment for the commercial import of the materials was made into a blocked account.³⁵² These prohibitions resulted in, for example, customs officials in the 1960s seizing “packages containing English language books and newspapers produced in North Vietnam and China” and refusing their entry until licenses were granted.³⁵³

Prior to the Berman Amendment’s enactment, the United States Government took varying approaches to imports of expressive materials. The Executive Branch initially required licenses for U.S. imports of thousands of Cuban publications destined for Americans’ personal use, and then later “nominally allowed the importation of informational materials from Cuba but in reality, banned such importation by requiring that the importers make payment into blocked U.S. accounts.”³⁵⁴ Plaintiffs challenged these prohibitions and seizures under the First Amendment, but courts upheld them as constitutional on the grounds that the specific restrictions were merely “incidental” to the purpose of the regulations in restricting the flow of capital to enemy nations.³⁵⁵ In contrast, the 1985 Nicaraguan embargo and 1986 Libyan embargo explicitly authorized the import of “books, newspapers, magazines, films, phonograph records, tape recordings, photographs, microfilm, microfiche, posters, and similar materials” and thus preserved Americans’ ability to receive news,

ideas, and other expressive content from those nations.³⁵⁶

Congress enacted the Berman Amendment against this regulatory and judicial backdrop and as an explicit “reaction” to the continued, and continually upheld, import restrictions on and seizures of “shipments of magazines and books” from most embargoed countries.³⁵⁷ The Berman Amendment thus “codif[ie]d” current practice . . . in the recent embargoes of trade with Nicaragua and Libya of exempting information materials and publications from import restrictions,”³⁵⁸ and used the same terms to do so (“publications,” “films,” “posters,” and so on).

The legislative history confirms what context makes clear: The Berman Amendment was designed to reach expressive information protected by the First Amendment. The relevant House committee report explains that Congress intended the Berman Amendment to protect the import and export of expressive materials; the report favorably cited and quoted from an American Bar Association House of Delegates statement that “no prohibitions should exist on imports to the United States of ideas and information if their circulation is protected by the First Amendment.”³⁵⁹ “Accordingly,” the report continued, “these sections also exempt informational materials and publications from the export restrictions that may be imposed under these

acts.”³⁶⁰ Senator Charles Mathias, the sponsor of an earlier bill that contained identical language removing restrictions on the import and export of information and that was the predecessor to the 1988 bill that enacted the Berman Amendment, explained that “[t]he thread that ties all of these changes together” is “an ideal embodied in the first amendment [sic]: The removal of barriers that inhibit the free exchange of ideas across international frontiers.”³⁶¹ Mathias emphasized not the specific doctrine of the First Amendment but rather its “philosophy” and “ideal[s],” including an “open and robust debate in the marketplace of ideas.”³⁶² As he further explained, “this liberty, secured by the first amendment [sic], is thwarted by a number of laws which permit the Government to restrict the flow of information and the travel of individuals into and out of the United States,” including “restrict[ing] the import and export of information on the basis of the political doctrines contained in the information”—restrictions that the Berman Amendment was designed to address.³⁶³

In 1994, Congress updated the Berman Amendment in ways that reinforced the expressive focus of the term “information or informational materials.” Between the enactment of the Berman Amendment in 1988 and Congress’ update in 1994, the Executive Branch had taken “a narrow view of what constituted ‘informational materials.’”³⁶⁴ Some of these restrictive Executive Branch interpretations were successfully challenged in court, and others were not. For example, the Department of the Treasury had interpreted the term “informational materials” as excluding “intangible items, such as telecommunications transmissions” (an interpretation that the courts approved),³⁶⁵ and original art in the form of paintings (an

³⁵⁰ *E.g.*, 31 CFR 515.204 (1985) (Cuba); 31 CFR 500.204 (1976) (China, North Korea, Vietnam, Cambodia).

³⁵¹ 31 CFR 515.544(b) (1985); 31 CFR 500.544 (1971).

³⁵² 31 CFR 515.545(b) (1985); 31 CFR 500.545 (1974).

³⁵³ Burt Neuborne & Steven R. Shapiro, *The Nylon Curtain: America’s National Border and the Free Flow of Ideas*, 26 Wm. & Mary L. Rev. 719, 730 (1985).

³⁵⁴ *Walsh v. Brady*, 927 F.2d 1229, 1230 (D.C. Cir. 1991) (citing 31 CFR 515.545 (1987)); *see id.* at 731.

³⁵⁵ *E.g.*, *Veterans & Reservists for Peace in Vietnam v. Regional Comm’r of Customs*, 459 F.2d 676, 681 (3d Cir. 1972); *Teague v. Regional Comm’r of Customs*, 404 F.2d 441, 445–46 (2d Cir. 1968); *American Documentary Films, Inc. v. Sec’y of Treas.*, 344 F. Supp. 703, 706–07 (S.D.N.Y. 1972).

³⁵⁶ *See* 31 CFR 540.536 (1985); 31 CFR 550.507 (1986); 31 CFR 550.411 (1986).

³⁵⁷ *E.g.*, *United States v. Amirnazmi*, 645 F.3d 564, 584 (3d Cir. 2011); *Kalantari v. NITV, Inc.*, 352 F.3d 1202, 1205 (9th Cir. 2003).

³⁵⁸ *Walsh*, 927 F.2d at 1233 (quoting H.R. Rep. No. 40, 100th Cong., 1st Sess., pt. 3, at 113 (1987)); *see also id.* at 1233 n.3 (explaining that House report’s incorporation into the Berman Act’s official legislative history). The House committee report favorably cited the Nicaragua and Libya blockades, which had exempted certain “informational materials such as books, records, and films.” H.R. Rep. No. 100–40, pt. 3, at 71. The committee indicated an intention to “codify” that practice of “exempting information materials and publications from import restrictions.” *Id.* at 113.

³⁵⁹ H.R. Rep. No. 100–40, *supra* note 358, at 113. Although this committee report accompanied H.R. 3, a predecessor bill that was vetoed in May 1988, *see* H.R. Doc. No. 100–200, 100th Cong., 2d Sess. (1988) (veto message), the President and Congress later agreed on a successor bill, H.R. 4848, that contained the same informational-materials exception as its predecessor and that ultimately was enacted into law as the Omnibus Trade and Competitiveness Act of 1988. Since this Act was “derived largely from [the] predecessor bill” and “was not itself the subject of legislative debate,” the Act “specifically provide[d] that the legislative history for the predecessor bill, H.R. 3, generally is treated as its own legislative history.” *Cernuda*, 720 F. Supp. at 1547–48; *see* Pub. L. 100–418, sec. 2(a), 102 Stat. 1107, 1119 (1988).

³⁶⁰ H.R. Rep. No. 100–40, *supra* note 358, at 113.

³⁶¹ 132 Cong. Rec. 6550 (Mar. 27, 1986) (statement of Sen. Charles Mathias).

³⁶² *Id.* at 6550–51.

³⁶³ *Id.*; *see Cernuda*, 720 F. Supp. at 1550 (explaining that “[t]he point” of the Berman Amendment was to “totally exempt[] from prohibition or regulation the import of ideas and information protected by the First Amendment” and thus “eliminate[] the sort of constitutional questions that arose in cases like *American Documentary Films* and *Teague*”).

³⁶⁴ *United States v. Amirnazmi*, 645 F.3d 583, 584 (3d Cir. 2011).

³⁶⁵ Foreign Assets Control Regulations and Cuban Assets Control Regulations, 54 FR 5229 (Feb. 2, 1989) (codified at 31 CFR 500.206(a), (c), 500.332(b)(2) (1989)); 31 CFR 515.545(b) (2010) (prohibiting the remittance of royalties or other payments relating to works not yet in being); *see Capital Cities/ABC, Inc. v. Brady*, 740 F. Supp. 1007, 1011–12 (S.D.N.Y. 1990).

interpretation that the courts rejected).³⁶⁶

Congress responded to these regulatory and judicial decisions by “clarify[ing]” the text of the Berman Amendment through the passage of the Free Trade in Ideas Act.³⁶⁷ As with the original 1988 version, the 1994 version of the Berman Amendment, as reflected in its text and legislative history, focuses on excluding expressive materials from regulation. In its 1994 changes, Congress added new examples of expressive materials to the Berman Amendment but did not otherwise expand its scope to include, for example, even non-expressive materials. First, Congress changed the term “other informational materials” to “any information or informational materials.” Second, Congress moved the new term from the end of the list to the beginning and expanded the list of materials, so that it now reads “any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.”³⁶⁸ Third, Congress made explicit that the Berman Amendment applied to information or informational materials “regardless of format or medium of transmission.”³⁶⁹

The legislative history of these changes confirms that Congress intended to maintain the Berman Amendment’s exclusive focus on protecting expressive materials from regulation under IEEPA and did not intend to exclude from the President’s regulatory power the full scope of what colloquially might be understood to be information or informational materials. Among other things, the effect of these changes was, as the 1994 House report explained, to “clarify” the Berman Amendment by “eliminating some of the unintended restrictive administrative interpretations of it.”³⁷⁰ For example, by adding the words “regardless of format or medium of transmission,” the 1994 amendment overrode the interpretation excluding intangible materials that was unsuccessfully challenged in *Capital Cities/ABC, Inc. v. Brady*, 740 F. Supp. 1007, 1015 (S.D.N.Y. 1990). Similarly, the 1994 amendment codified the decision in *Cernuda v. Heavey*, 720 F.

Supp. 1544, 1548 (S.D. Fla. 1989), by adding “artworks” to the illustrative list of informational materials and otherwise took the opportunity to “expand[] the exemption’s non-exclusive list of informational materials to include new media, such as compact discs and CD ROMs,” on which expressive information may exist.³⁷¹ But the House conference report makes clear that the 1994 amendment “only intended to address some of those restrictive interpretations” while leaving other interpretations in place.³⁷² For example, Congress “did not disabuse OFAC of its belief that it could permissibly regulate ‘informational materials not fully created and in existence at the date of the transaction’” and “did not counteract” that interpretation, which is discussed in more detail below.³⁷³ By explicitly acknowledging that the bill was intended to overrule some but not all narrow interpretations of “information or informational materials,” Congress rejected a meaning that would include anything that, in a colloquial sense, could potentially be “information or informational materials.”³⁷⁴

Similarly, Rep. Howard Berman, the sponsor of the original Berman Amendment in 1988, described the 1994 amendment as designed to protect the right “to impart and receive information and ideas.”³⁷⁵ “Even at the height of the Cold War,” he recounted, the United States “positively promoted the exchange of literary and artistic work in an attempt to liberalize and open up the cultural and political climate in those countries,” and the then-recent fall of the Soviet Union “suggest[ed] that contact with Americans and the exposure to American ideas were crucial to the momentous changes which are taking place there, to our great national advantage.”³⁷⁶ The legislative history underscores what is apparent in the statutory text and context: The term is not meant to encompass everything that might technically or colloquially be described as “information.”

Congress’ purpose in enacting the Berman Amendment was to protect the

free exchange of ideas, and the Berman Amendment does not exempt from regulation all types of conduct, information, or communications.³⁷⁷ Although the message need not be particularized or articulable, as in the case of many pieces of art, it must still “communicate . . . ideas.”³⁷⁸ The types of “information or informational materials” listed in the Berman Amendment, such as “publications,” “news wire feeds,” and “artworks,” are mediums for expressing and conveying an idea to others.³⁷⁹

B. Regulated Transactions Involving Sensitive Personal Data Under This Proposed Rule Do Not Implicate the Berman Amendment’s Restrictions on Regulating Expressive Material

The proposed rule would regulate transactions involving sensitive personal data that is non-expressive and thus is fully consistent with the Berman Amendment.³⁸⁰ It would regulate commercial transactions involving the export of government-related data or bulk U.S. sensitive personal data that lacks expressive content.

The specific types of sensitive personal data proposed here for regulation are not expressive in nature because the data itself, whether in bulk or in isolation, does not convey an idea.³⁸¹ For example, a person’s fingerprints (biometric identifiers); DNA sequence (genomic data); financial account numbers or their browser’s IP address (covered personal identifiers); debts and income (personal financial data); weight, blood type, test results, and treatments (personal health data); and their telephone’s location history (precise geolocation data) do not convey expressive messages or ideas to the recipient. Sensitive personal data instead serves functional purposes, and the regulations proposed here are designed to prevent the export of this data based on its functionality to create and facilitate national security harms, not regulate the expression of ideas.

For example, human genomic data is the biological code of human functioning and growth. It is primarily used (along with personal health data)

³⁷¹ *Kalantari v. NITV, Inc.*, 352 F.3d 1202, 1205 (9th Cir. 2003).

³⁷² H.R. Rep. No. 103–482, *supra* note 367, at 239.

³⁷³ *United States v. Amirnazmi*, 645 F.3d 564, 586 (3d Cir. 2011).

³⁷⁴ *See, e.g., id.* at 586–87 (“When Congress is aware of an agency’s interpretation of a statute and takes no action to correct it while amending other portions of the statute, it may be inferred that the agency’s interpretation is consistent with congressional intent.”).

³⁷⁵ 138 Cong. Rec. 15052 (June 16, 1992) (statement of Rep. Berman).

³⁷⁶ *Id.*

³⁷⁷ *See, e.g., Texas v. Johnson*, 491 U.S. 397, 404 (1989).

³⁷⁸ *Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos.*, 515 U.S. 557, 570 (1995).

³⁷⁹ 50 U.S.C. 1702(b)(3).

³⁸⁰ *See infra* §§ 202.249(b)(4) (excluding from the definition of “sensitive personal data” “information or informational materials”), 202.226(a) (limiting “information or informational materials” to “expressive materials”).

³⁸¹ So too for “government-related data,” which the proposed rule defines to mean certain sensitive personal data or certain precise geolocation data, regardless of volume.

³⁶⁶ *See Cernuda*, 720 F. Supp. at 1549–52.

³⁶⁷ H.R. Rep. No. 103–482, 103d Cong., 2d Sess., at 239 (conf. rep.), reprinted in 1994 U.S.C.C.A.N. 398, 483; *see* Public Law 103–236, sec. 525(b), 108 Stat. 382, 474 (1994) (codified at 50 U.S.C. 1702(b)).

³⁶⁸ Public Law 103–236, *supra* note 367, at 474.

³⁶⁹ *Id.*

³⁷⁰ H.R. Rep. No. 103–482, *supra* note 367, at 239.

to understand and address vulnerabilities in human functioning, health, and disease. The same human genomic data that can be used to design disease therapy can also be used to identify genetic variability in a population, which can potentially be used for nefarious purposes such as identifying and exploiting susceptibility to disease. Large human genetic datasets used for ancestry, solving crimes, and research can also be misused for counterintelligence purposes, including targeting, surveillance, coercion, blackmail, intimidation, and influence.³⁸² Datasets containing human genomic data do not communicate any idea; they simply contain functionally useful data.

Biometric identifiers (like a fingerprint, palm print, iris pattern, or facial feature) are “the measurement of physiological characteristics” of an individual that are primarily used for security and identity verification—for example, by comparing the measurements of an identifier against those of previously enrolled identifiers permitted to access a system.³⁸³ Similarly, precise geolocation data measures geographic location, ordinarily defined by its longitude and latitude coordinates, that is used to identify the physical location of a device (and thus persons associated with the device). Geolocation data is primarily used to enable and facilitate, for example, navigation, tracking, the implementation of security measures through geofencing, anti-fraud measures, targeted advertising, and the provision of certain services like roadside assistance. Biometric identifiers and precise geolocation data do not communicate any idea; they simply contain functionally useful data.

At their core, and as defined in these proposed regulations, personal financial data and personal health data also contain only functionally useful data that does not convey any idea or message. The former typically identifies and measures an individual’s financial accounts, assets, debts, and liabilities, primarily to enable, facilitate, and track commercial activity (for example, by exchanging account and routing numbers, balances, and amounts to enable payments, or by identifying assets, debts, and liabilities associated with a particular individual to determine creditworthiness for loan applications). The latter typically

identifies and measures an individual’s medical conditions and history, primarily to assess and track an individual’s health condition and determine a medical course of action.

Finally, covered personal identifiers are specifically listed classes and combinations of data that are “reasonably linked to an individual.”³⁸⁴ This data (such as Social Security numbers, financial account numbers, hardware-based identifiers, advertising identifiers, and network-based identifiers) is primarily used to identify devices and individuals, and to distinguish them from each other. They are not typically used to express and communicate ideas or messages.

In sum, the regulations contained in this proposed rule appropriately “balance[] IEEPA’s competing purposes” in “restricting material support for hostile regimes while encouraging the robust interchange of information.”³⁸⁵ The export of non-expressive data (including the sensitive personal data that the proposed rule would regulate) does not implicate the exchange of ideas and expression that the Berman Amendment protects. At the same time, allowing sensitive personal data to fall into the hands of countries of concern would directly support and enable their attempts to undermine national security, including through traditional and economic espionage, surveillance, sabotage, blackmail, and other nefarious activities. Moreover, these categories of sensitive personal data are already subject to some existing government regulation in the context of domestic commercial transactions. It would be unreasonable to interpret IEEPA—a statute that is specifically designed to address foreign threats to national security, foreign policy, and the economy—as disallowing regulation of the same commercial transactions when they involve transferring such data to a country of concern.

This proposed interpretation aligns with the suggestions of several commenters to clarify the extent to which the transmission of expressive content and associated metadata, including through internet traffic, to entities and individuals in countries of concern would be exempt from the proposed regulations. Under this interpretation, expressive content and associated metadata that is not sensitive personal data would be categorically outside the scope of the proposed definition of “sensitive personal data” and thus outside the scope of the

proposed regulations, regardless of the type of activity (or transaction) involved. The Department believes that other aspects of the proposed rule (such as bulk thresholds or the definition of “covered data transaction”) would also protect the dissemination of expressive content and its associated metadata. The Department welcomes further comments on this issue.

To the extent that any parties believe that the sensitive personal data involved in their covered data transactions may nevertheless qualify as “information or informational materials” that is exempt under 50 U.S.C. 1702(b)(3), they can seek clarification using the proposed administrative processes for seeking an advisory opinion or applying for a specific license before engaging in the transaction.

C. Exclusion for Materials Already Created and in Existence

Finally, consistent with longstanding OFAC practice, the proposed rule would exclude “information or informational materials not fully created and in existence at the date of the data transaction, or the substantive or artistic alteration or enhancement of information or informational materials, or the provision of marketing and business consulting services, including to market, produce or co-produce, or assist in the creation of information or informational materials” from the definition of “information or informational materials.”

§ 202.206(b)(1). Many commercial services and transactions may result in the creation of information or informational materials. This exclusion balances “IEEPA’s competing imperatives (*i.e.*, restricting material support for hostile regimes while encouraging the robust interchange of information)” and reflects a “reasoned determination” that 50 U.S.C. 1702(b)(3) is not meant to exempt “information or informational materials” that “would not be produced but for” commercial transactions that could be otherwise prohibited or regulated.³⁸⁶ In the sanctions context, for example, a prohibition on providing consulting services would preclude provision of a consulting report even though such a report might otherwise be characterized as “informational materials.”³⁸⁷ In the

³⁸⁶ *Amirnazmi*, 645 F.3d at 587; see also, *e.g.*, *United States v. Griffith*, 515 F. Supp. 3d 106, 116–17 (S.D.N.Y. 2021).

³⁸⁷ *Cf.*, *e.g.*, Off. of Foreign Assets Control, U.S. Dep’t of Treas., *Guidance on Certain Publishing Activities*, at 2–3 (Oct. 28, 2016), <https://ofac.treasury.gov/media/6516/download?inline> [<https://perma.cc/GF9U-M4TJ>]; Off. of Foreign

Continued

³⁸² See, *e.g.*, Nat’l Counterintel. & Sec. Ctr., *supra* note 83, at 4.

³⁸³ Nat’l Inst. of Standards & Tech., *Biometrics*, <https://www.nist.gov/programs-projects/biometrics> [<https://perma.cc/SV3S-THLD>].

³⁸⁴ 89 FR 15428–29.

³⁸⁵ *United States v. Amirnazmi*, 645 F.3d 564, 587 (3d Cir. 2011).

context of this proposed rulemaking, a U.S. company's customization and sale of bulk U.S. sensitive personal data in response to a customer's particular criteria would fall within this independent exclusion and would not constitute information or informational materials (in addition to falling outside the definition of "information or informational material" because it is non-expressive material).

The legislative history of the Berman Amendment indicates that Congress was aware of this same interpretation in sanctions programs under IEEPA administered by OFAC and chose not to change it. The Department of the Treasury construed the Berman Amendment not to apply to "informational materials not fully created and in existence at the date of the transaction, or to the substantive or artistic alteration or enhancement of informational materials, or to the provision of marketing and business consulting services" shortly after it was enacted.³⁸⁸ As discussed above, when Congress amended the statute in 1994, it overrode other government interpretations of the Berman Amendment but it "did not disabuse OFAC of its belief that it could permissibly regulate 'informational materials not fully created and in existence at the date of the transaction'" and "did not counteract" that interpretation.³⁸⁹ Courts, relying in part on this legislative history, have affirmed this interpretation of the Berman Amendment,³⁹⁰ and the Department accordingly incorporates it into the definition of "information or informational materials" in proposed § 202.226.

VII. Regulatory Requirements

The Department designated the proposed rule as significant under Executive Order 12866, as amended, and the Office of Information and Regulatory Affairs in the Office of Management and Budget ("OMB") reviewed the proposed rule.³⁹¹ In addition, this section includes the required assessments of the reporting and recordkeeping burdens under the Paperwork Reduction Act of 1995,³⁹² and the potential impact on small

entities pursuant to the Regulatory Flexibility Act.³⁹³

A. Executive Orders 12866 (Regulatory Planning and Review) as Amended by Executive Orders 13563 (Improving Regulation and Regulatory Review) and 14094 (Modernizing Regulatory Review)

1. Executive Summary

The Department of Justice estimates the discounted annualized cost of the proposed regulation to be approximately \$502 million annually. The extremely high potential net benefits (*i.e.*, expected benefits less estimated costs) justify moving forward with the proposed rule. The approximately \$502 million estimated annual cost would afford protection to well over 100 million American individuals who are potential targets of adversaries using bulk U.S. sensitive personal data. Also, the approximately \$502 million estimated annual cost of the regulation is about one-third of 1 percent (0.3 percent) of the \$176 billion revenues generated in the U.S. Computing, Infrastructure, Data Processing Services, and Web Hosting Services industry sector.

2. Introduction.

The review that accompanies an NPRM is known as a Preliminary Regulatory Impact Analysis ("RIA"). The Office of Management and Budget's Circular A-4 provides guidance to Executive agencies on how to conduct effective regulatory analyses.³⁹⁴ Circular A-4 recognizes that good regulatory

analyses cannot be conducted according to a formula; that conducting high-quality analysis requires competent professional judgment; and that different regulations may call for different emphases in the analysis, depending on the nature and complexity of the regulatory issue and the sensitivity of the benefit and cost estimates of the key assumptions.³⁹⁵

Circular A-4 states that RIA analysts "should aim for transparency about the key methods, data, and other analytical choices you make in your analysis."³⁹⁶ It also encourages consultation with key stakeholders, which can "be useful in ensuring that your analysis addresses all of the relevant issues and that you have access to all pertinent data," noting that "[e]arly consultation can be especially helpful."³⁹⁷ At the outset of this research, the Department reached out to the private sector and other government agencies regarding data that would be useful to the analysis. The response has, in general, been that the information and data available to and known by other agencies and the private sector that would potentially be relevant to conducting such an analysis are incomplete, irrelevant, and unreliable. The Department's own search found that there are enough information sources available to make a reasonable estimate of the impact of the proposed rule based on a cost analysis that considers the value of transactions lost due to the prohibitions, the security and due diligence costs associated with the pursuit of restricted transactions, and adequate data to approximate the number of firms likely to be affected by the regulation. Regarding the estimated value of transactions lost to the prohibitions, impacts could vary by the bulk thresholds for each of the data categories outlined in the proposed rule. However, due to data limitations, this analysis does not attempt to estimate cost sensitivities based upon alternatives to the proposed bulk thresholds. We welcome comments on addressing this analytical issue.

Given the limitations on available information, the resulting uncertainty, and the qualifications surrounding the analysis, the Department has been unable to assess that any secondary impacts, such as how the prohibition on bulk U.S. sensitive personal data transfers to the countries of concern would influence international trade, are reasonably likely. Based on the available information, such secondary impacts are too speculative and hypothetical to be

Assets Control, U.S. Dep't of Treas., Letter No. 031211-FARCL-IA-14, *Interpretive Ruling: Posting of Information from Iran on Website*, at 2 (Dec. 11, 2003), <https://ofac.treasury.gov/media/7921/download?inline> [<https://perma.cc/J7FP-CVAS>].

³⁸⁸ 31 CFR 500.206(c) (1989).

³⁸⁹ *Amirnazmi*, 645 F.3d at 586.

³⁹⁰ See *Amirnazmi*, 645 F.3d at 583–88; *Griffith*, 515 F. Supp. 3d at 116–17.

³⁹¹ E.O. 12866, 58 FR 51735 (Sept. 30, 1993).

³⁹² 44 U.S.C. 3501 *et seq.*

³⁹³ 5 U.S.C. 601 *et seq.* This proposed rulemaking pertains to a foreign affairs function of the United States and therefore is not subject to the notice-and-comment rulemaking requirements of the Administrative Procedure Act ("APA"), which exempts a rulemaking from such requirements "to the extent there is involved . . . a military or foreign affairs function of the United States." 5 U.S.C. 552(a)(1). The proposed rule is being issued to assist in addressing the national emergency declared by the President with respect to the threat posed to U.S. national security and foreign policy by the continuing effort of countries of concern to access and exploit government-related data or Americans' bulk U.S. sensitive personal data. As described in the Order, this threat to the national security and foreign policy of the United States has its source in whole or substantial part outside the United States. Accordingly, the proposed rule would have a direct impact on foreign affairs concerns, which include the protection of national security against external threats (for example, prohibiting or restricting transactions that pose an unacceptable risk of giving countries of concern or covered persons access to bulk sensitive personal data). Although the proposed rule is not subject to the APA's notice and comment requirements, the Department is engaging in notice and comment rulemaking for this proposed rule, consistent with sections 2(a) and 2(c) of the Order.

³⁹⁴ Off. of Mgmt. & Budget, Circular No. A-4, *Regulatory Analysis* (Nov. 9, 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/11/CircularA-4.pdf> [<https://perma.cc/8J6A-K75Y>].

³⁹⁵ *Id.* at 4.

³⁹⁶ *Id.*

³⁹⁷ *Id.*

quantified in this analysis. Although the scope of the proposed rule is limited, indirect trade impacts could run into the hundreds of millions of dollars; nevertheless, such costs would be impossible to calculate at this juncture, and such analysis is outside the scope of this assessment.

This analysis considers the direct costs of the proposed regulation. Although it does not devote a section to indirect costs, Circular A–4 advises analysts to look beyond the obvious costs and benefits of a regulation for additional costs and benefits, which are sometimes referred to as “indirect” effects or “downstream” effects.³⁹⁸ Beyond the direct costs, there will be other market repercussions associated with the proposed regulation. Foreign firms will have less revenue from selling bulk U.S. sensitive personal data purchased from U.S. firms; new businesses may arise to provide vetting information to firms seeking entrance into the restricted transactions market; misunderstandings of the proposed regulation may result in firms spending more than necessary to comply; overall increased data security may result in more secure data and systems; transactions that are not prohibited may be reduced by firms not understanding nuances of the prohibitions; and, in retaliation, foreign countries may enact their own prohibitions and restrictions that may adversely affect U.S. businesses.

Additionally, staff of the Department of Commerce Office of Undersecretary for Economic Affairs note that there will be indirect costs from the loss of database imports from countries of concern, forgone productivity gains associated with potential innovation resulting from access to restricted data by individuals in countries of concern, and firms’ reduced access to employees from countries of concern. At this point, the Department is not aware of any data with which to assess these costs, and the assessment of such costs is outside the scope of this RIA.

The regulatory review faces significant challenges in developing quantitative estimates of the monetary costs and benefits of the proposed regulation. Among these challenges to a reliable comparison of quantified cost

and benefits, is the nature of the benefits that are expected from the regulation. These benefits include the security of the American people, economic prosperity and opportunity, and democratic values, all of which are beyond a reasonable, reliable, and acceptable estimate of quantified monetary value.³⁹⁹ In contrast, although precise, reliable, and relevant data to estimate the regulation’s cost impacts are not publicly available, the Department has made a preliminary estimate of those costs using knowledge of the entities affected by the proposed rule; the transactions likely to be involved; and previous estimates of the costs of compliance with similar activities, such as due diligence, audits, recordkeeping, and reporting. Policy decisions will be informed by whether the benefits expected from the regulation justify the estimated costs.

3. Market Sectors Impacted by the Proposed Regulation

The firms that are currently active in the collection, processing, sale, or other types of transfers of bulk U.S. sensitive personal data and that are likely to be impacted by the proposed regulation include those that collect sensitive personal data (often referred to as “first parties”) and those that aggregate, assemble, analyze, and sell sensitive personal data (“third parties”). Sensitive personal data passes through a long supply chain of third-party vendors, such as data brokers, that obtain the data from first-party sources such as doctors, hospitals, pharmacies, banks and other financial companies, insurance companies, internet service providers, online and brick-and-mortar retail chains, schools, “smart product” sellers, rental agencies, ancestry agencies, software vendors, geolocation firms, and gaming firms.⁴⁰⁰ Another

sector that may be impacted consists of those firms that export bulk biospecimens such as blood plasma and other medical products, laboratory supplies, and cosmetic products made with human hair. The United States supplies 70 percent of the world’s supply of blood plasma, for example, making it the largest exporter of blood plasma.⁴⁰¹ Additionally, blood plasma has become the United States’ 11th most valuable export.⁴⁰² In 2022, China imported more U.S. exports of “immunological medicines, plasma and other blood fractions” than any other country had in a given year.⁴⁰³ When it comes to the biospecimen segment, the proposed rule exempts items related to clinical trials, and official United States Government business and transactions required or authorized by international agreements, including United States Government business and international agreements related to pandemic preparedness and surveillance.

Bulk personal data that is extracted from different sources and then combined and analyzed can provide comprehensive profiles of individuals. Comprehensive profiles typically include a wide range of personal data, including contact information such as address, phone number, and email address; demographic data, including age, family ties, and ethnic and religious affiliations; data on general interests, such as charitable giving, gambling, pets, preferred celebrities, movies and music genres, and reading preferences; data about a person’s home and neighborhood, including home equity, home size (e.g., number of rooms and baths), and rent or loan amount and interest rate; criminal and civil actions

about such potential impacts, none of the comments were specific enough to identify any concrete product development and testing involving prohibited or restricted transactions. The comments did not describe any specific scenarios in which government-related data or bulk U.S. sensitive personal data are critical to the development or testing of some product with a significant market the proposed rule would eliminate, for example, because there is no substitute development or testing market other than a country of concern or covered person.

⁴⁰¹ David Smith, ‘It’s gamified’: Inside America’s Blood Plasma Donation Industry, *The Guardian* (Mar. 2, 2023), <https://www.theguardian.com/books/2023/mar/02/blood-money-book-kathleen-mclaughlin> [<https://perma.cc/7VFK-QTSL>].

⁴⁰² Peter Jaworski, *Bloody Well Pay Them: The Case for Voluntary Remunerated Plasma Collections*, Niskanen Center (June 14, 2020), <https://www.niskanencenter.org/bloody-well-pay-them-the-case-for-voluntary-remunerated-plasma-collections/> [<https://perma.cc/WVR9-ZGS9>].

⁴⁰³ Ken Roberts, *In 2022, China Dominates U.S. Exports of Immunological Drugs, Plasma and Vaccines*, *Forbes* (Oct. 26, 2022), <https://www.forbes.com/sites/kenroberts/2022/10/26/in-2022-china-now-dominates-us-exports-of-plasma-and-vaccines/> [<https://perma.cc/X9KA-EG82>].

³⁹⁸ *Id.* at 56. The usage of the term “indirect costs” in this analysis differs from the ANPRM’s “Economic Impact,” which discussed the expected “indirect costs” of the rulemaking primarily in terms of due diligence and security costs. See 89 FR 15799–800. In this analysis, the term “indirect costs” refers to downstream effects and does not necessarily encompass due diligence and security costs; to the extent that such costs are discussed, the Department simply refers to them by their own terms.

³⁹⁹ Exec. Off. of the President, *National Security Strategy* (Oct. 12, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-NationalSecurity-Strategy-10.2022.pdf> [<https://perma.cc/6X6U-75DL>].

⁴⁰⁰ See, e.g., *Types of Sensitive Information: A Complete Guide*, SealPath, <https://www.sealpath.com/blog/types-of-sensitive-information-guide/> [<https://perma.cc/7XPU-TLB6>]; Nirmal Ranganathan, *Understanding the Complexities of Enterprise Data Supply Chains*, TechRadar Pro (May 1, 2023), <https://www.techradar.com/opinion/understanding-the-complexities-of-enterprise-data-supply-chains> [<https://perma.cc/AKZ4-UJAE>]; Lou Rabon, *Uncovering Third-Party Risk: What Are They and Where They Come From*, Cyber Defense Group (June 3, 2024), <https://www.cdg.io/blog/third-party-risk> [<https://perma.cc/645V-YUBF>]. This assessment has also considered whether the proposed rule would result in a reasonably measurable impact on product development and testing. Although some commenters raised concern

background data, such as arrests and convictions, and judgments in civil cases; social media and technology data, including home internet provider, social media usage, and computer operating systems; financial data, including credit card usage, loans, and net worth; health data, including alcohol or tobacco usage, medical conditions (e.g., allergies), medicine preferences, and mental health issues; and other data, such as travel, vehicle, and behavior data.⁴⁰⁴

a. Sensitive Personal Data and Government-Related Data

i. Personal Financial Data

The universe of financial institutions that create bulk U.S. sensitive personal data is all firms that provide financial services. The smallest, narrowest set is the financial firms subject to a primary financial regulator. These include banks,⁴⁰⁵ credit unions,⁴⁰⁶ large financial utilities,⁴⁰⁷ securities firms,⁴⁰⁸ investment companies,⁴⁰⁹ and insurance companies.⁴¹⁰ The total number of government-regulated and -supervised financial-services firms in this category is around 35,000.⁴¹¹ The total number of large financial-services firms is about 17,000. The Department arrived at this number by consulting the North American Industry Classification System (“NAICS”), which, in its category for Finance and Insurance

companies, contains the broadest potential set of firms that could be found in the NAICS category for Finance and Insurance companies. This category contains more than 240,000 firms in total, with around 17,000 of these firms having over 20 employees, making them potentially more likely to have in-house data management and control systems.⁴¹²

ii. Personal Health Data

As with human genomic data,⁴¹³ many doctors, hospitals, medical facilities, consumer human genetic testing labs, insurance companies, businesses, healthcare providers, and research institutions sell sensitive health-related data (e.g., Electronic Medical Records (“EMRs”), prescriptions, laboratory tests, insurance claims). There is a large market for such data, which generates significant profits for companies with the capabilities to collect, anonymize, collate, and sell the data to third parties and data brokers. The market for these sales is at least in the billions of dollars.⁴¹⁴ With the EMR market expected to grow at a compound annual growth rate of 6.5 percent to \$46.96 billion in 2028, it is expected that the keepers of this data will take advantage of the increasing demand and massive economic benefits that these data sales can achieve.⁴¹⁵

At the forefront of data sales are the hospitals, medical facilities, pharmaceutical companies, insurers, and pharmacies that have direct access and involvement in the creation and maintenance of patient health data. HIPAA and other privacy laws help protect patients from having their

personal health information shared, but nearly every State either recognizes medical providers as the owners of medical data or does not have any laws conferring patients specific ownership or property rights to their medical records.⁴¹⁶ The situation with clinical trial data is similar, as any data generated by a trial participant becomes the property of the sponsor company.⁴¹⁷

Furthermore, some companies in the health sector may be able to legally sell Americans’ health-related information, depending on the legal requirements applicable to their context.⁴¹⁸ For example, although healthcare providers that conduct certain standard transactions electronically may be HIPAA-covered entities that are generally prohibited from selling protected health information by the HIPAA Privacy Rule,⁴¹⁹ many companies that collect healthcare information are not covered by HIPAA and are not subject to its restrictions. Pairing Americans’ health-related information with publicly available health record databases, healthcare directories and clearinghouses, academic or government databases (e.g., *data.gov*), and basic internet searches makes it increasingly simple to re-identify or link information. Data brokers have flourished by selling packaged datasets on the sensitive health conditions of millions of Americans in the open market.⁴²⁰ As the volume and demand for this data increase, we may see continued growth in the market share.

We also note that the Department of Health & Human Services (“HHS”) is supporting the secure sharing of clinical information via the development of the voluntary Trusted Exchange Framework and Common Agreement.⁴²¹

iii. Precise Geolocation Data

The proposed rule defines “precise geolocation data” as “data, whether real-time or historical, that identifies the

⁴⁰⁴ Urbano Reviglio, *The Untamed and Discreet Role of Data Brokers in Surveillance Capitalism: A Transnational and Interdisciplinary Overview*, 11 Internet Pol’y Rev. (Issue) 3 (Aug. 4, 2022), <https://policyreview.info/articles/analysis/untamed-and-discreet-role-data-brokers-surveillance-capitalism-transnational-and> [<https://perma.cc/A4NS-AF5B>].

⁴⁰⁵ Bd. of Governors of the Fed. Rsv. Sys., 110th Annual Report of the Board of Governors of the Federal Reserve System 26–28 (2023), <https://www.federalreserve.gov/publications/files/2023-annual-report.pdf> [<https://perma.cc/3W34-QKYE>].

⁴⁰⁶ Press Release, Nat’l Credit Union Admin., *Credit Union Assets, Lending, Insured Shares, Delinquencies Grow* (June 2024), <https://ncua.gov/newsroom/press-release/2024/credit-union-assets-lending-insured-shares-delinquencies-grow> [<https://perma.cc/MK9Z-7R3Z>].

⁴⁰⁷ Bd. of Governors of the Fed. Rsv. Sys., *supra* note 405.

⁴⁰⁸ Fin. Indus. Regul. Auth., 2024 FINRA Industry Snapshot 13 (July 18, 2024), <https://www.finra.org/sites/default/files/2024-07/2024-Industry-Snapshot.pdf> [<https://perma.cc/UEV6-9XVM>].

⁴⁰⁹ Inv. Co. Inst., 2024 Investment Company Fact Book 23 (2024) <https://www.ici.org/system/files/2024-05/2024-factbook.pdf> [<https://perma.cc/5CJ3-JWHS>].

⁴¹⁰ Ron Harden, *Insurance Industry Facts*, Nat’l Ass’n of Ins. Pros., Inc., <https://thenaip.org/general/insurance-industry-facts/> [<https://perma.cc/U8S9-BVRD>].

⁴¹¹ This figure includes 3,794 bank holding companies; 1,411 Federal Reserve System member banks; 287 savings and loan holding companies; 8 financial market utilities; 4,572 credit unions; 3,298 securities firms; 16,038 investment companies; and 5,929 insurance entities.

⁴¹² U.S. Census Bureau, *U.S. & states, 6-digit NAICS, 2021 SUBS Annual Data Tables by Establishment Industry* (Dec. 2023), <https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html> [<https://perma.cc/A86S-NKHA>].

⁴¹³ While the NPRM proposes including human ‘omic data beyond genomic data within the scope of the categories of sensitive personal data, the NPRM seeks comments on how that category of human ‘omic data (other than genomic data) should be regulated. The Department defers consideration of that issue until it is settled in the final rule. Section 7(i) of the Order defines human ‘omic data as “data generated from humans that characterizes or quantifies human biological molecule(s), such as human genomic data, epigenomic data, proteomic data, transcriptomic data, microbiomic data, or metabolomic data, as further defined by regulations issued by the Attorney General pursuant to section 2 of this order, which may be informed by the report described in section 6 of this order.” E.O. 14117, 89 FR 15429.

⁴¹⁴ Adam Tanner, *Our Bodies, Our Data: How Companies Make Billions Selling Our Medical Records* (2017).

⁴¹⁵ *Electronic Medical Records Market to Surpass \$46.96 Billion by 2028, Lead [sic] by Asia-Pacific Growth and AI Trends*, Yahoo! Finance (Mar. 11, 2024), <https://finance.yahoo.com/news/electronic-medical-records-market-surpass-192000251.html> [<https://perma.cc/N45N-N5QV>].

⁴¹⁶ Niam Yaraghi, *Who Should Profit from the Sale of Patient Data?* Brookings Inst. (Nov. 19, 2018), <https://www.brookings.edu/articles/who-should-profit-from-the-sale-of-patient-data/> [<https://perma.cc/9886-AS93>].

⁴¹⁷ Paul W. Glimcher, *Who Profits from Medical Records?*, Med. Econ. Oct. 2020, at 50, available at <https://www.medicaleconomics.com/view/who-profits-from-medical-records-> [<https://perma.cc/RP4S-GGZR>].

⁴¹⁸ Justin Sherman, *Your Health Data Might Be for Sale*, Slate (June 22, 2022), <https://slate.com/technology/2022/06/health-data-brokers-privacy.html> [<https://perma.cc/39CR-4ZS3>].

⁴¹⁹ See 45 CFR 164.502(a)(5)(ii), 164.508(a)(4).

⁴²⁰ Sherman, *supra* note 418.

⁴²¹ Notice of Publication of Common Agreement for Nationwide Health Information Interoperability (Common Agreement) Version 2.0, 89 FR 35107 (May 1, 2024).

physical location of an individual or a device with a precision of within one kilometer.” The parameters to be determined are (1) the level at which to set this precision, (2) the level of precision necessary to support common commercial applications of geolocation data, and (3) the effectiveness of applying location fuzzing to geolocation data (decreasing its accuracy) in some commercial applications to reduce potential privacy impacts. These parameters are necessary to provide clear guidance to acquirers and sellers of precise geolocation data.

Mobile applications (“apps”) from smartphones are the primary sources that directly gather location data from consumers, although other technologies are also collecting and transmitting data, such as “Internet of Things” wearable devices and connected vehicles. Once they collect it, many apps share location data with third parties, whether by selling it to data brokers, to advertisers who then sell it to data brokers, or directly to buyers who intend to use the geolocation data.⁴²² Data brokers can “pay a mobile app developer to use the broker’s software development kit . . . in the developer’s app. The broker can then sit within the app and gather data directly on users.” Alternatively, many app developers will sell location data “directly to a data broker through a server-to-server transfer.”⁴²³ As one example, the family safety app Life360 sold location data to nearly a dozen location data brokers in 2021—and in fact, it had agreements to directly transfer location data about its users to data brokers through its own servers.⁴²⁴ Such practices create opportunities for countries of concern to exert malign influence over U.S. persons relevant to national security.

The market for location data is large, and many companies operate as data brokers.⁴²⁵ Significantly, three major

data brokers—Acxiom, LexisNexis, and Nielsen—sell data on current or former U.S. military personnel, some of which is specifically marketed as such.⁴²⁶ All three firms collect and advertise information on individuals, ranging from their family members and friends to their spending habits, mental health conditions, and geolocation.⁴²⁷ Both Acxiom and LexisNexis also provide users with the ability to verify whether someone is active duty.⁴²⁸

iv. Human Genomic and Human ‘Omic Data

There is value in both human genomic and ‘omic data, and there is a large global ecosystem for buying and selling this data for a variety of purposes. The ‘omic data market is growing exponentially due to the use of such data for drug discovery. There is little current regulation that restricts the buying and selling of this data, but there are real risks and potential harms associated with the misuse of such data, ranging from the individual to the population level.

The human genomic data ecosystem is large and has both public and private actors, including healthcare entities, law enforcement, international security agencies, and recreational personal human genomics/biospecimen companies.⁴²⁹ The global human genomics market was valued at \$28 billion in 2022 and is projected to grow to over \$164 billion by 2032, with North America accounting for approximately 45 percent of the market’s current size.⁴³⁰

Personal human genomics companies (e.g., 23andMe, Ancestry, Ariosa Diagnostics, Color Genomics, FamilyTreeDNA, Ionis, GenScript, Illumina, Genentech, My Heritage, Navigenics, Orig3n, and Prenetics) and human biospecimen (e.g., BioChain

Institute, BioIVT, Boca Biologistics, Creative Bioarray, Cureline, Discovery Life Sciences, Infinity BiologiX, Precision for Medicine) companies collect human genomic and related data or human biospecimens, such as tissue and blood samples, that can be used to extract human genomic information for a variety of healthcare and recreational purposes.⁴³¹ It is common for companies in these spaces, especially direct-to-consumer firms, to be owned by pharmaceutical companies or to sell the human genomic data they obtain to pharmaceutical companies. It is also common for them to conduct health research in collaboration with healthcare systems and to enter into partnerships with other industries.⁴³²

There is little readily available information on who is purchasing or reselling human genomic data beyond pharmaceutical companies. Similarly, there is little readily available information on which entities (such as multinational pharmaceutical companies) are transferring human genomic data to their subsidiaries or vendors in countries of concern.

While many of the uses of human genomic data are for the development of new health technologies and pharmaceuticals, and the health and drug discovery environment are highly regulated, the sale of the data appears common and is currently virtually unregulated. As a result, there are few records of current transactions, and any company that collects human genomic data could potentially broker its sale to other companies or interested parties. For example, the States of Vermont and California have data broker registration laws, but even in those States, there is

⁴²² *The Location Data Market, Data Brokers, and Threats to Americans’ Freedoms, Privacy, and Safety: Hearing Before the Joint Committee on Consumer Protection and Professional Licensure*, (Mass. 2023) (written testimony of Justin Sherman, Senior Fellow and Research Lead, Data Brokerage Project, Duke Univ. Sanford Sch. of Pub. Pol’y), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/07/Sherman-Justin_WrittenTestimony_MA_Legislature.pdf [<https://perma.cc/52RR-J2HY>].

⁴²³ *Id.*

⁴²⁴ Alfred Ng & Jon Keegan, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users*, *The Markup* (Dec. 6, 2021), <https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user> [<https://perma.cc/NTK2-CL96>].

⁴²⁵ See *The Location Data Market, Data Brokers, and Threats to Americans’ Freedoms, Privacy, and Safety*, *supra* note 422, at 3 (listing some of the

“significant companies in the location data market”).

⁴²⁶ Justin Sherman, *Data Brokers Are Advertising Data on U.S. Military Personnel*, *Lawfare* (Aug. 23, 2021), <https://www.lawfaremedia.org/article/data-brokers-are-advertising-data-us-military-personnel> [<https://perma.cc/Y9RN-WHZF>].

⁴²⁷ Steven J. Arango, *Data Brokers Are a Threat to National Security*, Vol. 148/12/1, 438 U.S. Naval Inst.: Proceedings (Dec. 2022), <https://www.usni.org/magazines/proceedings/2022/december/data-brokers-are-threat-national-security> [<https://perma.cc/74W3-TCR3>].

⁴²⁸ *Id.*

⁴²⁹ Abraham P. Schwab et al., *Genomic Privacy*, 64 *Clinical Chemistry* 1696 (2018), <https://academic.oup.com/clinchem/article/64/12/1696/5608647> [<https://perma.cc/Q89R-5WRZ>].

⁴³⁰ Precedence Rsch., Report No. 1204, *Genomics Market—Global Industry Analysis, Size, Share, Growth, Regional Outlook and Forecast, 2023 to 2032* (Nov. 2023), <https://www.precedenceresearch.com/genomics-market> [<https://perma.cc/J9WA-RKVB>].

⁴³¹ Susi Geiger & Nicole Gross, *A Tidal Wave of Inevitable Data? Assetization in the Consumer Genomics Testing Industry*, 60 *Bus. & Soc’y* 614 (2021), <https://journals.sagepub.com/doi/10.1177/0007650319826307> [<https://perma.cc/7YSC-VTEW>]; Ramish Cheema, *Top 20 Genomics Companies in the World*, *Yahoo! Finance* (Oct. 30, 2023), <https://finance.yahoo.com/news/top-20-genomics-companies-world-194600414.html> [<https://perma.cc/8WXD-KGCC>]; Kayte Spector-Bagdady, *Hospitals Should Act Now to Notify Patients About Research Use of Their Data and Biospecimens*, 26 *Nature Med.* 306 (2020), <https://www.nature.com/articles/s41591-020-0795-6> [<https://perma.cc/BEX6-3GCJ>]; InsightAce Analytic, Report No. 1264, *Biospecimen Contract Research Services Market Size, Share & Trends Analysis Report, 2024–2032* (2024), <https://www.insightaceanalytic.com/report/global-biospecimen-contract-research-services-market/1264> [<https://perma.cc/N667-TL8F>].

⁴³² Geiger & Gross, *supra* note 431, at 625–26, 638; Shmuel I. Becher & Andelka M. Phillips, *Data Rights and Consumer Contracts: The Case of Personal Genomic Services*, in *Data Rights and Private Law* 83 (Damian Clifford et al. eds., 2023), <https://ssrn.com/abstract=4180967> [<https://perma.cc/35GE-ZQQ4>].

not specific information regarding genomic information sales.⁴³³

v. Biometric Identifiers

The proposed rule defines biometric identifiers” as “measurable physical characteristics or behaviors used to recognize or verify the identity of an individual, including facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints, gait, and keyboard usage patterns that are enrolled in a biometric system and the templates created by the system.” In recent years, such identifiers have become increasingly ubiquitous in our security and verification systems. A wide variety of companies and agencies collect this information, amassing large datasets on everything from face shape, eye scans, and fingerprints to voice recordings and even heartbeats.⁴³⁴

There is also limited information regarding the biometric data broker community. Because of the highly sensitive nature of the data (i.e., fingerprints cannot be changed), brokers are not forthcoming in their advertising or collection of available information.

vi. Covered Personal Identifiers

An individual can have personal identifiers both assigned to them and collected from them in a wide variety of contexts and through a wide variety of entities—including governments, advertisers, and providers of technology and communications services. This,

combined with the fact that personal identifiers have been used in some form for many years, means that they are a widely available form of sensitive personal data. The proposed rule specifies two subcategories of covered personal identifiers that could be used, when combined with each other or combined with other types of sensitive personal data, to “identify an individual from a data set or link data across multiple data sets to an individual.”⁴³⁵ These subcategories of covered personal identifiers in the proposed rule are listed identifiers: (1) In combination with any other listed identifier; or (2) In combination with other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data.⁴³⁶ See § 202.212.

b. The Data-Brokerage Market

Much of the economic impact of the proposed rule’s restrictions on the transfer or sale of data types described in part VII.A.3.a of this preamble will be borne by firms involved in the data-brokerage market. The United States is widely perceived to be the largest data-brokerage market in the world, as described below in this section. While the proposed rule regulates data-brokerage activities (i.e., transactions), there does not appear to be any direct measure of data-brokerage activities.

This analysis therefore uses and examines information regarding first-party data brokers and third-party data brokers as a reasonable measure of data-brokerage activities.

i. Companies That May Meet the Definition of Data Brokers for the Purposes of the Proposed Rule

Data brokers collect, aggregate, and sell personal data.⁴³⁷ First-party or primary data brokers collect and sell information from their own customers. Third-party data brokers purchase and resell data. On the global scale, an estimated 5,000 data-brokerage firms operate worldwide.⁴³⁸ There may be as many as 11,000 firms that fall under the 518210 NAICS code, which covers firms that provide data processing, hosting, and related services.⁴³⁹

ii. Market Size

Estimates of the size of the data broker market vary widely, from \$50 billion to \$300 billion, with one popular estimate claiming that over \$200 billion in revenue is generated globally each year.⁴⁴⁰ For the United States, which maintains approximately 60 percent of the global market, a likely range is between \$30 billion and \$180 billion.⁴⁴¹

Based on total revenue (U.S. and foreign) and the number of employees at these firms, the Department estimates the market size as shown in Table VII–1 of this preamble.

TABLE VII–1—SELECTED DATA BROKER REVENUE AND EMPLOYEE FIGURES

Data broker	Total revenue	U.S. revenue	Foreign revenue	Employees
Acxiom (2018) ^a	\$917.4 million	\$834.6 million	\$82.8 million	3,380
LexisNexis (2021) ^b	\$974.3 million	n/a ^c	n/a ^c	10,200
Oracle America (2023) ^d	\$50 billion	\$31 billion	\$19 billion	^g 164,000
Equifax (2023) ^e	\$5.3 billion	\$4.1 billion	\$1.2 billion	14,900
Experian (2022) ^f	\$6.6 billion	\$4.4 billion	\$2.2 billion	22,000

^a Acxiom LLC 2018 Annual Report, AnnualReports.com (2018), https://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_ACXM_2018.pdf [<https://perma.cc/6BVA-DQS5>].

^b Latka, *How LexisNexis Hit \$974.3M Revenue with a 10.2K Person Team in 2021*, SaaS Database, <https://getlatka.com/companies/lexisnexis> [<https://perma.cc/M4DM-HAC9>].

^c LexisNexis is owned by RELX and is folded into their annual report and therefore the annual report does not provide specific domestic and foreign revenue numbers just for LexisNexis.

⁴³³ Both California’s and Vermont’s regulations provide definitions of “Data Broker” that differ from the definition of “data brokerage” provided in Subpart C of the proposed rule. See Cal. Civ. Code sec. 1798.99.80, *supra* note 62; Vt. Stat. Ann. tit. 9, sec. 2430(4) (2024).

⁴³⁴ Samuel Chapman, *Understanding Biometric Data Collection in 2024*, PrivacyJournal.net (Apr. 10, 2023), <https://www.privacyjournal.net/biometric-data-collection/> [<https://perma.cc/RAQ2-VTLZ>].

⁴³⁵ 89 FR 15428.

⁴³⁶ *Id.*

⁴³⁷ *How to Stop Data Brokers from Selling Your Personal Data*, Kaspersky, <https://>

usa.kaspersky.com/resource-center/preemptive-safety/how-to-stop-data-brokers-from-selling-your-personal-information [<https://perma.cc/ZLU3-S7N9>].

⁴³⁸ Susan Moore, *How to Choose a Data Broker*, Gartner (June 8, 2016), <https://www.gartner.com/smarterwithgartner/how-to-choose-a-data-broker> [<https://perma.cc/5FP2-RGM5>].

⁴³⁹ U.S. Census Bureau, *supra* note 412.

⁴⁴⁰ *How Data Brokers Sell Your Identity & Personal Information*, IDShield: Blog (Mar. 18, 2022), <https://www.idshield.com/blog/internet-privacy/data-brokers-what-they-know-and-how-they-collect-your-data/> [<https://perma.cc/6LRX-SX79>]; Catherine Tucker & Nico Neumann, *Buying Consumer Data? Tread Carefully*, Harv. Bus. Rev.

(May 1, 2020), <https://hbr.org/2020/05/buying-consumer-data-tread-carefully> [<https://perma.cc/GDY3-AWKQ>]; David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, L.A. Times (Nov. 5, 2019), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> [<https://perma.cc/AH6C-UKDA>]; OnAudience.com, *Global Data Market Size: 2017–2021* (Nov. 2020), <https://pressmania.pl/wp-content/uploads/2020/12/Global-Data-Market-Size-2017-2021-OnAudience-Report.pdf> [<https://perma.cc/KX6E-4XC6>].

⁴⁴¹ OnAudience.com, *supra* note 440 at 8, 11.

^dOracle, *Oracle Announces Fiscal 2023 Fourth Quarter and Fiscal Full Year Financial Results* (June 12, 2023), <https://investor.oracle.com/investor-news/news-details/2023/Oracle-Announces-Fiscal-2023-Fourth-Quarter-and-Fiscal-Full-Year-Financial-Results/default.aspx> [https://perma.cc/DL8Y-H2VM]. The U.S. Revenue entry of \$31 billion is for “the America’s.” The Foreign Revenue entry of \$19 billion is for “Europe/Middle East/Africa” and “Asia/Pacific.” Oracle, *Culture and Inclusion Empowers Diversity*, <https://www.oracle.com/careers/culture-inclusion/best-practices/> [https://perma.cc/3M2B-GQ7F].

^eEquifax Inc., *2023 Annual Report* (2024), <https://investor.equifax.com/sec-filings/annual-reports#document-3666-0001308179-24-000246-2> [https://perma.cc/WU9A-NHZ2].

^fExperian, *Annual Report 2023* (2023), <https://www.experianplc.com/content/dam/marketing/global/plc/en/assets/documents/reports/2023/annual-report/experian-annual-report-2023-web.pdf> [https://perma.cc/7QRT-GN3T].

^gOracle Corp., *Annual Report* (Form 10-K) (June 20, 2023), <https://www.sec.gov/Archives/edgar/data/1341439/000095017023028914/orcl-20230531.htm> [https://perma.cc/4ADX-R6EJ].

iii. Products Sold by Data Brokers

Data brokers often collect data regarding, for example, where the average person goes, where they shop, and what they search for online.⁴⁴² Notably, researchers from Duke University who used a secret shopper approach were offered access to thousands of records of military personnel and military veterans’ data containing names, addresses, emails, phone numbers, military agency or branch, medical ailments, political affiliations, religion, gender, age, income, credit rating, and even details on children in the household.⁴⁴³ Not all brokers sell the same data, with many targeting niche industries or markets to help them gain a competitive advantage. Brokers also trade and combine their data with primary collectors to create detailed profiles they can package and commercialize.⁴⁴⁴

iv. Price Information

Depending on its type and volume, personal data can be purchased for prices ranging from less than \$1 for one personal record to millions of dollars for a large dataset. In a secret shopper study, Duke University researchers found that they could purchase a single record for as little as \$0.12 and spend upwards of \$10,000 for approximately 50,000 records of service members and military veterans. The price did not noticeably vary based on the data subjects’ IP location (United States vs. Singapore). The Duke University researchers found that if one broker could not sell the information to them, another one could. There are estimates that mental health datasets could range between \$15,000 and \$100,000 and may be sold for even higher prices if the

datasets include more detailed demographic data.⁴⁴⁵

v. Customers of Data-Brokerage Products

It is known that data brokers sell datasets both domestically and internationally; however, specific transaction activities with these parties are difficult to ascertain from available financial reports. The U.S. Bureau of Economic Analysis (“BEA”) faces significant limitations for estimating the size of the domestic and international markets because BEA data does not break out data brokerage separately as an industry. Furthermore, based on sample financial data of the data-brokerage firms listed in Table VII–1 of this preamble, the Department estimates that the U.S. market produces over 60 percent of data broker revenue.

c. Agreements Affected by the Proposed Regulation

It is difficult to determine an approximate number of affected vendor agreements, employment agreements, and investment agreements that are entered in any given year by a U.S. person due to the scope and nature of these agreements. Each of these three types of agreements are considered restricted transactions if they involve access to government-related data or bulk U.S. sensitive personal data. The Department welcomes comments that provide a source for the annual number of vendor agreements, employment agreements, and investment agreements that might be affected by the regulation.

i. Vendor Agreements

According to the proposed rule, a vendor agreement is defined as “any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.” See § 202.258(a). A potential example of a vendor agreement covered by the

proposed rule is a medical facility in the United States that contracts with a company headquartered in a country of concern to provide information technology (“IT”) related services. The medical facility has bulk personal health data on its U.S. patients, and the IT services provided under the contract involve access to the medical facility’s systems containing that bulk personal health data. (See Example 2 in § 202.258(b)). The NPRM also discusses additional examples of vendor agreements pertaining to technology services and data storage. (See Examples 3 and 4 in § 202.258(b)).

The costs of compliance with the security requirements will vary. Covered persons who have vendor agreements within the scope of the proposed rule may face costs associated with either replacing a vendor located in a country of concern or spending more on compliance (e.g., implementing the security requirements) to maintain those vendor agreements. Furthermore, some U.S. companies may choose to remove vendor agreements altogether rather than bear the cost of complying with the security requirements. In contrast, most Fortune 500 companies or companies in sectors subject to cybersecurity regulations already have cybersecurity controls in place and might only need minor modifications to their existing vendor agreements and data security controls, while companies with less mature cybersecurity programs may require more significant changes.

ii. Employment Agreements

This NPRM defines an employment agreement as “any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level.” See § 202.217(a). A potential example of an employment agreement is a U.S. company that employs a team of individuals who are citizens of and primarily reside in a country of concern and have access to back-end IT services

⁴⁴² Public Hearing on HB 2052 Before the H. Comm. On Bus. & Labor, 82nd Leg. Assemb. (Or. 2023) (written public testimony, Or. Dep’t of Just., Off. of the Att’y Gen.), <https://olis.oregonlegislature.gov/liz/2023R1/Downloads/PublicTestimonyDocument/40843> [https://perma.cc/XVM5-4ZEJ].

⁴⁴³ Sherman et al., *supra* note 6.

⁴⁴⁴ Henrik Twetman & Gundars Bergmanis-Korats, *Data Brokers and Security*, NATO Strategic Comm’n Ctr. of Excellence (2021), <https://stratcomcoe.org/publications/data-brokers-and-security/17> [https://perma.cc/XJ4D-UQYP].

⁴⁴⁵ Joanne Kim, *Data Brokers and the Sale of Americans’ Mental Health Data* (2023) <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf> [https://perma.cc/48UN-ELKG].

and company systems that contain bulk human genomic data (*see* Example 1 in § 202.217(b)). Similarly, the employment of a lead project manager or a CEO of a U.S. company who primarily resides in a country of concern and who has access to bulk U.S. sensitive personal data would be considered a restricted transaction (*see* Examples 2 and 3 in § 202.217(b)).

Any employment agreements involving government-related data or bulk U.S. sensitive personal data between U.S. persons and countries of concern or covered persons would need to comply with security requirements. The cost of security and due diligence requirements may drive some companies to cease employment agreements with these covered persons, while other companies may incur costs to ensure compliance or even implement job transfers to eliminate the potential cost of compliance with the proposed regulation. Ultimately, employment agreements may incur larger upfront costs once the proposed regulation comes into effect that may be minimized over time as the initial market disruptions due to the proposed rule settle, the costs associated with job transfers are minimized, and firms learn how to operate in the changed environment.

iii. Investment Agreements

This NPRM defines an investment agreement as “an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to (1) real estate located in the United States or (2) a U.S. legal entity.” *See* § 202.228(a). An example is when a U.S. company intends to build a data center located in a U.S. territory to store bulk personal health data on U.S. persons, and a foreign private equity fund located in a country of concern agrees to provide capital for the construction of the data center in exchange for acquiring a majority ownership stake in the data center (*see* Example 1 in § 202.227(c)). Ultimately, investment agreements may incur larger upfront costs once the proposed regulation comes into effect that may be minimized over time.

iv. Security Requirements

The proposed rule authorizes three classes of otherwise prohibited transactions (vendor agreements, employment agreements, and investment agreements) if they meet the security requirements proposed by CISA. The goal of the proposed security requirements is to address national

security and foreign-policy threats that arise when countries of concern and covered persons access government-related data or bulk U.S. sensitive personal data that may be implicated by the categories of restricted transactions. The proposed security requirements (incorporated by reference in § 202.402 of this NPRM) have been developed by DHS through CISA, which has published the proposed requirements on its website, as announced via a **Federal Register** request for comments on the proposed security requirements, issued concurrently with this proposed rule. After CISA receives and considers public input, it will revise as appropriate and publish the security requirements.

Regarding investment agreements, as described in § 202.228 and § 202.508, the proposed rule would treat investment agreements entered into by U.S. persons with countries of concern or covered persons as restricted transactions even if they are also covered transactions subject to CFIUS review, unless and until CFIUS issues an interim order, enters into a mitigation agreement, or imposes a condition with respect to a particular covered transaction.⁴⁴⁶ As a result, any investment agreement that is both a restricted transaction under the proposed rule and a covered transaction subject to CFIUS review would be subject to the security requirements under the proposed rule unless and until the transaction is filed with CFIUS and CFIUS takes a “CFIUS action,” as defined in the proposed rule, by entering into a mitigation agreement or imposing mitigation measures. Because the security requirements are likely at least similar to and potentially less burdensome than any bespoke mitigation measures that CFIUS would enter into or impose, the parties to such a covered transaction would likely face, as a result of the proposed rule, only the marginal cost of complying with the security requirements before CFIUS takes action. Because this cost of compliance is marginal, and because it appears likely, based on the Department’s experience, that many investment agreements by countries of concern or covered persons that involve access to sensitive personal data would also be covered transactions subject to CFIUS review, it appears likely that there will not be a meaningful cost for

⁴⁴⁶ Security requirements may only need to be implemented while the transaction is pending CFIUS review if the transaction is undertaken in the interim. *See, e.g.,* Example 9 in § 202.508.

investment agreements to comply with the security requirements.

v. Due Diligence and Recordkeeping

Due diligence and recordkeeping requirements will be important considerations when engaging in a restricted transaction or as a condition of a license (general or specific) and may be similar to certain requirements of an IEEPA-based sanctions program administered by OFAC. Section 202.1101 of the proposed rule requires U.S. persons subject to these affirmative requirements to maintain documentation of their due diligence to assist in inspections and enforcement, and to maintain the results of annual audits that verify their compliance with the security requirements, as applicable, and the conditions of any licenses, where relevant, that the U.S. persons may also have. Entities may be required to collect, maintain, and analyze readily available information to make appropriate judgments regarding their transactions and potential requirements under the proposed regulation. They may also be required to make available to the Department any annual audits that verify the U.S. person’s compliance with the security requirements and any conditions on a license.

vi. Audits

The proposed rule imposes certain audit requirements on restricted transactions to ensure compliance with the security requirements for covered data transactions, such as appointing a qualified auditor to annually assess compliance. Such audits would address the nature of the U.S. person’s covered data transaction and whether it is in accordance with applicable security requirements, the terms of any license issued by the Attorney General, or any other aspect of the regulations.

vii. Licenses

General and specific licenses would be available under the proposed regulation. Such licenses would permit transactions that are otherwise prohibited by the proposed regulation. Both general and specific licenses could include a range of requirements or obligations as the Department deems appropriate. The benefits of this type of regime include giving regulated parties the ability to bring specific concerns to the Department and seek appropriate regulatory relief and affording the Department the flexibility to resolve varied cases either generally or individually.

4. Need for Regulatory Action

There are many statutes, regulations, and programs that aim to keep America secure by monitoring, restricting, prohibiting, or otherwise regulating the flow of goods, services, investments, and information to foreign countries and foreign nationals, especially countries considered to be adversaries. For example, CFIUS has the authority to take action to mitigate any national security risk arising from certain foreign investments in U.S. businesses or involving U.S. real estate, or to recommend that the President suspend or prohibit a transaction on national security grounds. In addition, OFAC “administers and enforces economic and trade sanctions based on U.S. foreign-policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States.”⁴⁴⁷

In Executive Order 13873, the President authorized the Department of Commerce to prohibit transactions in the information and communications technology and services supply chain or to impose mitigation measures to address an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.⁴⁴⁸ The Secretary of Commerce exercises this authority through the Bureau of Industry and Security.⁴⁴⁹ Executive Order 14034 takes various steps to protect sensitive personal data from foreign adversaries.⁴⁵⁰

While existing legislation provides the Department of Justice with authority to promulgate this proposed rule, no existing statute replicates the measures undertaken here. Neither do any of the previous executive actions set forth in Executive Order 14117⁴⁵¹ broadly empower the government to prohibit or otherwise restrict the sale or transfer of government-related data or bulk U.S. sensitive personal data to countries of concern. Therefore, the proposed regulation will not be duplicative of any existing regulatory regime.

As relevant here, the regulatory philosophy of Executive Order 12866

provides that agencies should issue regulations when there is a compelling public need, such as a market failure.⁴⁵² Executive Order 12866 further directs agencies issuing new regulations to identify, where applicable, the specific market failure that warrants new agency action and to assess its significance. In perfect, unregulated markets, supply and demand lead to transactions that allocate resources efficiently, fully supply the market at prices that buyers are willing to pay, and do not harm third parties. However, some transactions result in market failures known as “negative externalities;” that is, harms to parties not directly involved in the transactions. The sale of government-related data or bulk U.S. sensitive personal data to adversaries is an example. Such transactions are mutually beneficial to the parties: U.S. data brokers obtain monetary benefits, and adversaries obtain possession of a potentially strategic asset of sensitive data that they can put to malicious use. However, when the data can be used to harm U.S. nationals who are not directly involved in the transactions by presenting a risk to national security or foreign policy, then the transaction creates negative externalities. These market failures demonstrate a need for the regulation being proposed, which will eliminate or reduce the risk to national security and foreign policy from such transactions. Circular A–4 also recognizes a common need for regulation to protect civil rights, civil liberties, or advancing democratic values, all of which are threatened if government-related data or bulk U.S. sensitive personal data end up in the hands of adversaries.⁴⁵³

5. Baseline (Without the Proposed Rule)

The baseline refers to what the world would look like without the regulatory changes being proposed here, which is closely related to the need for the regulation described above. To inform the public of the rationale behind the agency’s proposed regulations, the Department must analyze the quantifiable and qualitative costs and benefits of the proposed action. The baseline for the proposal under consideration is the state of the world without the regulation, often referred to as the “no-action alternative,” which here includes the current regulatory regime.

a. Baseline National Security and Foreign-Policy Risks by Category of Data

i. Human Genomic and Human ‘Omic Data

Human genomic data presents characteristics that, under certain circumstances, allow for misuse. Although humans share more than 99 percent of their DNA, the remaining differences play a significant role in physical and mental health.⁴⁵⁴ In addition to genomic data, which describes a person’s DNA sequence, if combined with other data, data characterizing other human systems, known as ‘omic data, can also uniquely identify individuals. For example, transcriptomic data describes RNA transcripts, or the expression of genes as impacted by environmental factors; proteomic data describes the complete set of proteins expressed by a cell, tissue, or organism; and metabolomic data describes the small molecule metabolites found within a biological sample.

Human genomic data and human ‘omic data are therefore highly personal, and there are both person- and population-level risks to national security associated with the potential sale of such data to foreign adversaries.⁴⁵⁵ Genomic data has been widely acknowledged in scientific, policy, and ethics literature to have the potential to be used to track an individual; breach their privacy; and expose individuals to discrimination, exclusion, or social embarrassment when paired with other personally identifiable information, such as by coloring public perception of a person’s competence or health. Genomic data that is de-identified by standard healthcare practices (*i.e.*, removal of name, date of birth) can, in some cases, be potentially re-identified by methods that combine genomic data with other privately and publicly available information.⁴⁵⁶ There are also other

⁴⁵⁴ *The Human Genome Project*, Nat’l Hum. Genome Resch. Inst., <https://www.genome.gov/human-genome-project> [<https://perma.cc/55Z4-XHFN>].

⁴⁵⁵ Kirsty Needham, *Special Report: COVID Opens New Doors for China’s Gene Giant*, Reuters (Aug. 5, 2020), <https://www.reuters.com/article/world/special-report-covid-opens-new-doors-for-chinas-gene-giant-idUSKCN2511CD/> [<https://perma.cc/U4B2-Y4TB>]; Nat’l Acad. of Scis., Eng’g & Med., *Safeguarding the Bioeconomy* 296–306 (2020), <https://nap.nationalacademies.org/catalog/25525/safeguarding-the-bioeconomy> [<https://perma.cc/77RH-ACKG>]; Bonomi et al., *supra* note 237, at 647.

⁴⁵⁶ Adam Tanner, *Strengthening Protection of Patient Medical Data*, Century Found. (Jan. 10, 2017), <https://tcf.org/content/report/strengthening-protection-patient-medical-data/> [<https://perma.cc/R26L-G9WP>].

⁴⁴⁷ U.S. Dep’t of Treas., Off. of Foreign Assets Control, <https://ofac.treasury.gov/> [<https://perma.cc/4N8E-X7XM>].

⁴⁴⁸ 84 FR 22689–22690.

⁴⁴⁹ Office of Information and Communications Technology and Services (OICTS), Bureau of Industry and Security, <https://www.bis.gov/OICTS> [<https://perma.cc/MFX8-MDN4>].

⁴⁵⁰ 86 FR 31423.

⁴⁵¹ 89 FR 15422.

⁴⁵² See 58 FR 51735.

⁴⁵³ See Off. of Mgmt. & Budget, *supra* note 394, at 15.

potential risks related to such data.⁴⁵⁷ For instance, the 2023 Annual Threat Assessment of the U.S. Intelligence Community explains that generally, “[r]apid advances in dual-use technology, including bioinformatics, synthetic biology, nanotechnology, and genomic editing, could enable development of novel biological weapons that complicate detection, attribution, and treatment.”⁴⁵⁸ Additionally, as the National Counterproliferation and Biosecurity Center has stated, “[r]esearch in genome editing by countries with different regulatory or ethical standards than those of Western countries probably increases the risk of the creation of potentially harmful biological agents or products.” Furthermore, because biological relatives share some genetic traits, the misuse of genomic and related information can potentially harm not only the individual but also their current and future biological relatives, to some degree.

For example, Huntington’s Disease is neurodegenerative, is frequently highly incapacitating, has no cure, and is tied to specific genetic variants.⁴⁵⁹ Revealing that an individual carries the variants for Huntington’s Disease could therefore be used to claim that a political candidate for office may soon become incapacitated or to harm that person’s family members mentally or emotionally.

At a population level, there are multiple examples of the risks posed by harmful use of genomic data. For example, the PRC has collected and used genetic data from minority groups and potential political dissidents to carry out human-rights abuses against those groups and to support state surveillance.⁴⁶⁰ The PRC’s collection of healthcare data from the United States poses equally serious risks, not only to the privacy of Americans, but also to the economic and national security of the United States.⁴⁶¹

⁴⁵⁷ Jan van Aken & Edward Hammond, *Genetic Engineering and Biological Weapons: New Technologies, Desires and Threats from Biological Research*, 4 EMBO Reports S57 (May 9, 2003), <https://doi.org/10.1038/sj.embor.embor860> [<https://perma.cc/Z95V-SWVL>].

⁴⁵⁸ Off. of the Dir. of Nat’l Intel., *supra* note 91, at 25; Nat’l Counterproliferation & Biosecurity Ctr., *Biological Warfare*, <https://www.dni.gov/index.php/ncbc-features/1548-features-2> [<https://perma.cc/6V8M-354G>].

⁴⁵⁹ *Huntington’s Disease*, Nat’l Inst. of Health, Nat’l Inst. of Neurological Disorders & Stroke, <https://www.ninds.nih.gov/health-information/disorders/huntingtons-disease#toc-what-is-huntington-s-disease> [<https://perma.cc/YE7C-UKN2>].

⁴⁶⁰ Nat’l Counterintel. & Sec. Ctr., *supra* note 83, at 3–4.

⁴⁶¹ *Id.*

It is conceivable that bulk genomic data in the wrong hands could be used to identify or track ethnic or racial subgroups in the United States and to target them for physical, mental, or emotional harm. As the NCSC has publicly explained, for example, “[c]oncerns over the exploitation of healthcare and genomic data by the [People’s Republic of China] are not hypothetical,” as China “has a documented history of exploiting DNA for genetic surveillance and societal control of minority populations in Xinjiang, China.”⁴⁶² Specifically, China “has established a high-tech surveillance system across Xinjiang, as part of a province-wide apparatus of oppression aimed primarily against traditionally Muslim minority groups.”⁴⁶³ This apparatus includes an “initiative launched by the PRC government in 2014” that “has been used to justify the collection of biometric data from all Xinjiang residents ages 12 to 65.”⁴⁶⁴ Chinese authorities have “collected DNA samples, fingerprints, iris scans, and blood types” and linked the biometric data “to individuals’ identification numbers and centralized [it] in a searchable database used by PRC authorities.”⁴⁶⁵ As NCSC has further explained, “[s]pecific abuses by the PRC government as part of this effort include mass arbitrary detentions, severe physical and psychological abuse, forced labor, oppressive surveillance used arbitrarily or unlawfully, religious persecution, political indoctrination, and forced sterilization of members of minority groups in Xinjiang.”⁴⁶⁶ In 2020, the Department of Commerce “sanctioned two subsidiaries of China’s BGI for their role in conducting genetic analysis used to further the PRC government’s repression of Uyghurs and other Muslim minority groups in Xinjiang.”⁴⁶⁷ As this example shows, “[t]he combination of stolen PII, personal health information, and large genomic data sets collected from abroad affords the PRC”—and other countries of concern—“vast opportunities to precisely target individuals in foreign governments, private industries, or other sectors for potential surveillance, manipulation, or extortion.”⁴⁶⁸ The potential exploitation of this kind of data is not limited to targeting and repression within the borders of a

country of concern, as this data could help “not only recruit individuals abroad, but also act against foreign dissidents.”⁴⁶⁹

There are additional risks to national security associated with the sale of bulk genomic data to countries of concern. For example, BGI Group, a Chinese company, grew exponentially during the COVID–19 pandemic by selling COVID–19 test kits in 180 countries around the world, which enabled it to collect biospecimens and DNA sequences from the individuals tested.⁴⁷⁰ The company also built laboratories in 18 countries, widely distributing its genetic sequencing/gathering technology across the globe, and the government of China helped to coordinate some of BGI’s arrangements with other countries. The human genetic samples that BGI collected may be shared publicly on China’s government-funded National GeneBank, creating individual privacy risks, and the Chinese government has indicated that its backing of BGI is intended to support China in commanding a significant position in the international biotechnology industry.⁴⁷¹

ii. Biometric Identifiers

As previously discussed, the gathering and aggregating of biometric data can be a complex process, and much about the market for biometric data is still unknown. The legitimate use of biometrics across many areas of technology is increasing rapidly, and the exposure of biometric data to countries of concern could prove to be especially damaging since the physical characteristics linked to biometrics are often difficult or impossible to change.

The PRC already has a demonstrated ability to collect and exploit the biometric data of its citizens, an effort that has been especially targeted at oppressed groups within its population. This has included gathering data such as “DNA samples, fingerprints, iris scans, and blood types” and creating a database where such data is linked with an individual’s personal identifier.⁴⁷² These capabilities will likely continue to be developed as the technology improves and could easily be used to undermine U.S. national security.

⁴⁶⁹ *Id.*

⁴⁷⁰ Needham, *supra* note 455 (“[i]n science journals and online, BGI is calling on international health researchers to send in virus data generated on its equipment, as well as patient samples that have tested positive for COVID–19, to be shared publicly via China’s government-funded National GeneBank.”).

⁴⁷¹ *Id.*

⁴⁷² Nat’l Counterintel. & Sec. Ctr., *supra* note 83.

⁴⁶² *Id.* at 3.

⁴⁶³ *Id.*

⁴⁶⁴ *Id.*

⁴⁶⁵ *Id.*

⁴⁶⁶ *Id.*

⁴⁶⁷ *Id.*

⁴⁶⁸ *Id.* at 4.

iii. Precise Geolocation Data

Precise geolocation data in the hands of foreign adversaries poses national security risks with respect to two areas: (1) operations, including missions, deployments, exercises, and activities of national security personnel; and (2) personnel, including those in the military and their families, as well as nonmilitary persons with the potential to obtain or hold information vital to national security.⁴⁷³

Potentially sensitive information can be gleaned outside direct conflict zones. Precise geolocation data can be readily used to identify the location and purpose of important national security-related infrastructure, facilities, and equipment, all of which could lead to immense harm to national security.

Precise geolocation data can also be used to coerce military personnel, State Department officials, and anyone else with access to sensitive national security information, including through the use of such data on their family members or other close associates.⁴⁷⁴ Compromising information gleaned from geolocation data can be used by adversaries for surveillance and intelligence gathering as well as to extort, blackmail, dox, and manipulate behavior to obtain sensitive national security information. With all the information that is readily available from data brokers, it is quite feasible to develop effective strategies to identify national security personnel and diplomatic/foreign-policy personnel working with specific sensitive information and to track their movements and behavior.

Adversaries could use these datasets to identify where national security personnel work, then use the personnel's health or financial information to bribe or blackmail them into providing the adversaries with access to restricted systems, sensitive information, or critical programs or infrastructure. Precise geolocation data could also allow these countries to track service members' and other national security personnel's movements, impersonate personnel online or in email, and identify personnel working on specific tasks within the national security community.

Countries of concern can also exploit access to government-related data, regardless of its volume. As one report has explained, for example, location-tracking data on individuals (e.g., military members, government employees and contractors, or senior

government officials) can “reveal sensitive locations—such as visits to a place of worship, a gambling venue, a health clinic, or a gay bar[.]” or “reputationally damaging lifestyle characteristics, such as infidelity[.]” which “could be used for profiling, coercion, blackmail, or other purposes[.]”⁴⁷⁵

In addition, these geolocation capabilities, combined with photography, “can expose personal information, locations, routines and numbers of [Department of Defense (DOD)] personnel, and potentially create unintended security consequences and increased risk to the joint force and mission.”⁴⁷⁶

iv. Personal Health Data

Personal health data also presents threats in the hands of foreign adversaries. There are a few documented cases of data brokers selling sensitive health information to foreign governments, including those in part IV.D.1.a of this preamble. Purchasers may have direct, indirect, or undisclosed ties to foreign officials that provide these entities with access to otherwise prohibited data. The presence of foreign adversaries in the U.S. health data market makes the variety and amount of American health data available in the data-brokerage ecosystem risky. Notably, the types of sensitive personal data (e.g., mental health or HIV/AIDS diagnoses) available, paired with the increasing speed and ease with which artificial intelligence and other technologies can re-identify individuals using as few as 15 demographic attributes (e.g., ZIP code, date of birth, gender, citizenship, race, occupation) from another dataset, have the potential to produce harmful outcomes for the American public if placed in the wrong hands.⁴⁷⁷

Currently, health data brokers collect and sell a wealth of information encompassing everything from general health conditions to addiction and prescription drug use. Additional discussion of these risks associated with personal health data can be found in part V.A.4 of this preamble.

⁴⁷⁵ Sherman et al., *supra* note 6, at 15.

⁴⁷⁶ Press Release, Def. Logistics Agency, *New Policy Prohibits DoD Employees from Using GPS Services in Operational Areas*, (Aug. 8, 2018) (quotation omitted), <https://www.dla.mil/About-DLA/News/News-Article-View/Article/1597116/new-policy-prohibits-dod-employees-from-using-gps-services-in-operational-areas/> (quoting a defense department official) [<https://perma.cc/8BNE-WU65>].

⁴⁷⁷ Adam Tanner, *supra* note 456; Rocher et al., *supra* note 45.

v. Personal Financial Data

Financial data tied to individuals can pose associated national security threats in the hands of foreign adversaries. There is also an associated threat to national security to U.S. persons who might be targeted for recruitment by a foreign adversary through the use of financial data as leverage over such U.S. persons. Data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data in a bank, credit, or other financial statement, including assets, liabilities and debts, and transactions; or data in a credit or “consumer report” expose that individual to more than monetary losses.⁴⁷⁸ The threat of exposing an individual's spending habits, particularly spending that may be embarrassing, can render that person open to extortion or blackmail.⁴⁷⁹ In instances where a threatened individual has access to especially sensitive information, national security may be at risk.

vi. Covered Personal Identifiers

Covered personal identifiers are a form of sensitive personal data that are both widely available and highly variable in nature. For example, covered personal identifiers may include demographic or contact data (e.g., first and last name, birthplace, ZIP code, residential street or postal address, phone number, and email address and similar public account identifiers) that is linked to financial account numbers. Many types of covered personal identifiers can be used effectively in combination with other types of sensitive personal data. The versatility of this data could make covered personal identifiers a valuable target for foreign adversaries attempting to increase the effectiveness of the bulk sensitive personal data in their possession by linking together separate datasets. For example, the PRC has both stolen data on U.S. persons that has included covered personal identifiers (e.g., names and Social Security numbers, as evidenced in the 2015 hack of the health insurer Anthem, Inc.) and has effectively used personal identifiers within internal datasets on their citizens as a way to more effectively surveil marginalized groups.⁴⁸⁰

⁴⁷⁸ Ctr. for Democracy & Tech., Docket No. CFPB–2023–0020, *Response to Request for Information Regarding Data Brokers*, at 3–5 (July 15, 2023), <https://cdt.org/wp-content/uploads/2023/07/CDT-Comment-to-CFPB-on-Data-Brokers-CFPB-2023-002054.pdf> [<https://perma.cc/YTJ8-QMVW>].

⁴⁷⁹ Arango, *supra* note 428.

⁴⁸⁰ Nat'l Counterintel. & Sec. Ctr., *supra* note 83.

⁴⁷³ Hazelrig, *supra* note 4; Sherman et al., *supra* note 6.

⁴⁷⁴ Sherman et al., *supra* note 6 at 14.

vii. Government-Related Data

It has become increasingly evident in recent years that government-related location data is at risk of being exploited by countries of concern through location information collected from electronic devices, including cell phones and fitness apps.⁴⁸¹ Such data can be used to not only track the movements of targeted government associates but also to link them with sensitive activities and vices, such as gambling or prostitution. This information can then be used to pressure these persons to reveal sensitive information, thereby compromising U.S. national security. Methods include malicious cyber-enabled activities, espionage, and blackmail.⁴⁸²

b. Baseline: Total Potential U.S. Population Affected by Risks

Part IV.A.1 of this preamble explains how adversaries can use their access to Americans' bulk sensitive personal data to engage in malicious cyber-enabled activities and malign foreign influence and to track and build profiles on U.S. individuals, including members of the military and government employees and contractors, for illicit purposes such as

blackmail and espionage. As of July 2021, one of the largest data brokers, Acxiom, sold products that purported to cover 45.5 million current and former U.S. military personnel and 21.3 million current and former government employees.⁴⁸³ The proposed rule also observes that countries of concern can exploit their access to Americans' bulk sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, and members of nongovernmental organizations or marginalized communities to intimidate them; curb political opposition; limit the freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties. Even family members of primary targets can be ensnared in such malicious activity. Finally, individuals with access to advanced intellectual property, such as semiconductor designs, could be high-value targets of countries of concern.

Tables VII–2 and VII–3 of this preamble provide estimates of the size of these targeted populations, but these figures should not be added together to calculate a single population figure, since a single individual could be a

member of more than one of the communities.

Several of the estimates presented in Table VII–2 of this preamble required calculations based on certain assumptions. Because data on the number of current Federal employees provided by the Office of Personnel Management does not include employees of the U.S. Postal Service, Office of the Director of National Intelligence, or Central Intelligence Agency, data on those groups was obtained from other sources and added in separate lines. The estimated number of former Federal Government contractors was calculated by applying the economy-wide labor turnover rate from 2001 to 2023 to the number of current Federal Government contractors; the Department assumed that half of the labor turnover involved workers staying in Federal Government contracting, and half involved workers leaving the industry. The estimated number of family members of military veterans was calculated by applying the current average number of family members for current military members to the military veteran population.

TABLE VII–2—AFFECTED POPULATION—GOVERNMENT-RELATED GROUPS

Category	Population
Current Federal Government employees (excluding employees of the U.S. Postal Service, director of National Intelligence, and Central Intelligence Agency) ^a	2,271,498
U.S. Postal Service employees ^b	525,469
Office of the Director of National Intelligence employees ^c	1,750
Central Intelligence Agency employees ^d	20,000
Former Federal Government employees ^e	4,103,208
Current Federal Government contractors ^f	4,100,000
Former Federal Government contractors ^{f g}	1,715,850
Department of Defense active duty ^h	1,304,720
Coast Guard active duty ^h	39,485
Ready Reserve ^h	994,860
Standby Reserve ^h	5,253
Retired Reserve ^h	183,728
Current military family members ^h	2,482,499
Military veterans ⁱ	17,680,000
Former military family members ^{h i}	21,188,328

^a U.S. Off. of Pers. Mgmt., *Status Data: Employment*, Federal Workforce Data (Feb. 2024), <https://perma.cc/7NF9-CTSC>.

^b *Number of Postal Employees Since 1926*, U.S. Postal Service (Feb. 2024), <https://about.usps.com/who/profile/history/employees-since-1926.htm> [<https://perma.cc/6W5W-VJJ6>].

^c Charles C. Clark, *Lifting the Lid*, Gov't Exec. (Sept. 1, 2012), <https://www.govexec.com/magazine/features/2012/09/lifting-lid/57807/> [<https://perma.cc/N8Z8-GEL8>].

^d Michael J. O'Neal, *CIA, Formation and History*, Encyclopedia.com, <https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/cia-formation-and-history> [<https://perma.cc/RZ24-YJAE>].

⁴⁸¹ Def. Logistics Agency, *supra* note 476.

⁴⁸² Sherman et al., *supra* note 6 at 15.

⁴⁸³ Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals* (2021), <https://techpolicy.sanford.duke.edu/wp-content/uploads/>

<sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf> [<https://perma.cc/Q3QL-PK7K>].

^eU.S. Off. of Pers. Mgmt., *Dynamics Data: Separations, FY 20052005–FY 2009* (data cube), Federal Workforce Data (Feb. 2024), https://www.fedscope.opm.gov/ibmcognos/bi/v1/disp?b_action=powerPlayService&m_encoding=UTF-8&BZ=1AAABv9mMvC42pVOQW6DQAZ8jE2SQyOvYRM4CfYRcmhKAYuPVXbZFNFPAB-1cFqEraW2dkyR6PR-bKYI1WxdHsddwPbef2eonMVxOQkYFKhJbbgEIZC9xsNlkyt8mUhAyr7zx1qhjuuoahcjZ6e2GVwzLGeXtj67DmWCATX2y6GvFwd7_rQfn8r3c12dri2Tb9AqZGz27z67XwIVPVueaMTMvsFZmYSCLEZL9zNfGDPN0ma7TIs9NWu2LPFfJv53kJe8xBciEEQkBAEAgSRggpEA90BkQh7TVF0jRdoO7o8EYCGyT8hOIL8jR7Mg7gJMGPZH_wPEXKmbn5lqfmHGNxVvb8l%3D [https://perma.cc/L42Z-AFAA]; U.S. Off. of Pers. Mgmt., *Dynamics Data, Separations, FY 2010–FY 2014* (data cube), Federal Workforce Data (Feb. 2024), https://www.fedscope.opm.gov/ibmcognos/bi/v1/disp?b_action=powerPlayService&m_encoding=UTF-8&BZ=1AAABv4ldgp142pVOwW6CQBD9mR3UQ83sg1U4cAB2iR4Kvjrj01FBDg1MKBvj-NEAabW99L5PMvHnzMk6R4syP5q9Dvuh7exeLwm4GgmiTZAoX_vAg-HasNbTwdBbCL4W0PayhVtXRMdoeo3IWE9NQ2g20GQnpp67PtSMXkcVN9WXL14ICdPqsp278V9Z11XBtm35BShPS27z67X_wEbjsbHMM8Dj9JTBVYMoGfCPwze6sxxNFFsk7yLDNJuc_zLHo24b_DnPgldALycxSshCChWIBFIOFuAcSmDcmRXVNHOhqSH8kQfAJLhOsJLwTgImQd0FMilij-QFy4tTNz0w1vzDjG3wAb-w%3D [https://perma.cc/5D43-3SY8]; U.S. Off. of Pers. Mgmt., *Dynamics Data, Separations, FY 2015–FY 2019* (data cube), Federal Workforce Data (Feb. 2024), [https://perma.cc/646G-6NBA](https://www.fedscope.opm.gov/ibmcognos/bi/v1/disp?b_action=powerPlayService&m_encoding=UTF-8&BZ=1AAABv6ePmJp42pVOQW6DQAZ8jE2SQyOvYfYl4cFjYReFQSAOXnqptsqmiUoiA-6sCVCXtrTOyZl-Hl3tVua3q8mhyHQ9j17tcr5H5GpJvRCgCtVPCjYjOjROosldpPDCU7Qci88aZbo47p-qDqYycnbp2dO2InF265ux6DBL0qbVfDqVeHezp03644a1yN9vb8dq1wwoDjZzdlitVv-4MNmeretWdkWmevyMQKAmR6QqafOdpMYZ6u0m1aFoVJ67wsCvVs4n8HeclLfCECQURCEAAQBARMMBHghHohMyFOaahqkSNvR-ZEAOUSWhOwE8jtytAjlLsAMZDnZHyBmzt3yzFzLCwu_AVRTb_0%3D); U.S. Off. of Pers. Mgmt., *Dynamics Data, Separations, FY 2020–FY 2024* (data cube), Federal Workforce Data (Feb. 2024), [https://perma.cc/58FZ-T7VA](https://www.fedscope.opm.gov/ibmcognos/bi/v1/disp?b_action=powerPlayService&m_encoding=UTF-8&BZ=1AAABv3dM77542pVOwW6DMAz9GZu2h1WOAA05clAkqD0MusKlpylR06kagw4f00BTe1223uyZD8%7EPzmoynVVLwe08kwdr3b6SUyX2PjmeFYlCrSD9HKemNyFiQkkJpEyHzKvC3Jj2o7T6ttwlyfura0bUjcn7pmrPrMc4wotZ_OQz1Ym9Pn%7EbDDWVu9neiteuHRYya_T8Nq9_x9syFT3rj0j0zl%7ElpMnMj0h088crXxYoCu1VmVRGFXvvyJlX0zy76Age00uRCCISAgCAIKYgAk8Ae6B6K99Wto0SFLb0f2RAHmDHBKyE8jvyHIWxF2ACcihtz9ATJy6_Zmp5hdmfAnKkW%7Ev)].

^dDavid Welna & Marisa Peñaloza, *Not Expecting Back Pay, Government Contractors Collect Unemployment, Dip into Savings*, NPR (Jan. 7, 2019), <https://www.npr.org/2019/01/07/682821224/most-contractors-do-not-expect-to-get-back-pay-when-the-shutdown-ends> [https://perma.cc/K4AW-ARFW].

^eU.S. Bureau of Labor Stat., *Total Separations Rate, Total Nonfarm, Not Seasonally Adjusted* (JTU0000000000000000TSR), Job Openings and Labor Turnover Survey, <https://data.bls.gov/toppicks?survey=jt> [https://perma.cc/VQ3Q-7AT3] (data extracted Sept. 2024) (select “Total separations rate, Total nonfarm, not seasonally adjusted” from list; then click “Retrieve data”). Estimate is based on the average annual separations rate from 2000 to 2022. The estimate of former government officials is based on the average turnover rate for all employees in the economy.

^fU.S. Dep’t of Def., ICF, *022 Demographics: Profile of the Military Community* (2022), <https://download.militaryonesource.mil/12038/MOS/Reports/2022-demographics-report.pdf> [https://perma.cc/TP2G-UADR].

^gU.S. Bureau of Labor Stat., *Population Level—Total Veterans, 18 Years and Over* (LNU00049526), Labor Force Statistics from the Current Population Survey, <https://beta.bls.gov/dataViewer/view/timeseries/LNU00049526> [https://perma.cc/P396-7M3A] (data extracted Feb. 2024).

The proposed rule highlights data associated with “activists, academics, journalists, dissidents, political figures, or members of nongovernmental organizations or marginalized communities” that could be used to “intimidate such persons; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.”⁴⁸⁴ Table VII–3 of this preamble describes the size of these populations.

Table VII–3 of this preamble also contains several figures that required calculations based on certain

assumptions. The estimated number of activists was calculated using a survey from the *Washington Post* and Kaiser Family Foundation that asked respondents whether they considered themselves activists; the percentage that answered “yes” was then applied to the current adult population. No data was available on the number of people residing in the United States who would be considered dissidents, so an estimate is provided for the size of this group. For this analysis, marginalized communities were assumed to include members of the lesbian, gay, bisexual, or transgender (“LGBT”) community;

religious minorities; and racial minorities.⁴⁸⁵ The number of religious minorities was calculated using the percentage of the population that identified as Jewish, Muslim, Buddhist, Hindu, or another religion.⁴⁸⁶

As noted earlier in this section, the populations affected by risks have substantial overlap, so the Department is unable to provide a single estimate of the affected population. Nonetheless, these estimates show that a substantial portion of the U.S. population is currently affected by the risks resulting from adversaries’ access to bulk sensitive personal data.

TABLE VII–3—POPULATIONS AFFECTED BY RISKS—OTHER GROUPS

Category	Population
Activists ^{a,b}	46,973,153
Academics ^c	1,380,290
Journalists ^d	44,530
Dissidents ^{e,f,g,h}	127,929
Political figures ⁱ	519,682
Members of non-governmental organizations ^j	715,790
Marginalized communities—LGBT ^k	13,942,200
Marginalized communities—Religious ^{b,l}	14,352,908

⁴⁸⁴ 89 FR 15781.

⁴⁸⁵ The groups that were assumed to be marginalized communities are similar to the groups most likely to be targeted in one or more countries of concern, which differs from the definition of underserved communities defined in Executive Order 13985 (Advancing Racial Equity and Support for Underserved Communities Through the Federal Government), 89 FR 7009 (Jan. 20, 2021). For examples of LGBT, religious, and racial minorities being targeted in the countries of concern, see, e.g.,

Bibek Bhandari & Elgar Hu, ‘Rainbow Hunters’ Target LGBTQ Chinese Students, Foreign Policy (July 28, 2023), <https://foreignpolicy.com/2023/07/28/china-rainbow-hunters-target-lgbtq-students/> [https://perma.cc/UZ37-D48A]; Pew Rsch. Ctr., *Government Policy Toward Religion in the People’s Republic of China—A Brief History, Measuring Religion in China* (Aug. 30, 2023), [https://www.pewresearch.org/religion/2023/08/30/government-policy-toward-religion-in-the-peoples-](https://www.pewresearch.org/religion/2023/08/30/government-policy-toward-religion-in-the-peoples-republic-of-china-a-brief-history/)

[republic-of-china-a-brief-history/](https://perma.cc/25CH-7AKH) [https://perma.cc/25CH-7AKH].

⁴⁸⁶ People who identify as Jewish, Muslim, Buddhist, Hindu, or members of other religions are non-Christian populations that each represent less than 2 percent of the U.S. population. 2022 PRRI *Census of American Religion: Religious Affiliation Updates and Trends*, PRRI (Feb. 24, 2023), <https://www.prri.org/spotlight/prri-2022-american-values-atlas-religious-affiliation-updates-and-trends/> [https://perma.cc/BQA7-MK2J].

TABLE VII-3—POPULATIONS AFFECTED BY RISKS—OTHER GROUPS—Continued

Category	Population
Marginalized communities—Race ^m (white Hispanic population not included)	130,398,545

^a Wash. Post & Kaiser Family Found., *Survey on Political Rallygoing and Activism* (Apr. 2018), <https://files.kff.org/attachment/Topline-Washington-Post-Kaiser-Family-Foundation-Survey-on-Political-Rallygoing-and-Activism> [<https://perma.cc/7ELT-NM6L>].

^b U.S. Census Bureau, K200104: *Population by Age, American Community Survey, 1-Year Supplemental Estimates* (2022), <https://data.census.gov/table/ACSSE2022.K200104> [<https://perma.cc/D6KP-JTKD>].

^c U.S. Bureau of Labor Stat., 25–1000: *Postsecondary Teachers*, National Occupational Employment and Wage Estimates (May 2023), https://www.bls.gov/oes/current/oes_nat.htm [<https://perma.cc/8FTZ-FCMW>].

^d U.S. Bureau of Labor Stat., 27–3023: *News Analysts, Reporters and Journalists*, National Occupational Employment and Wage Estimates (May 2023), https://www.bls.gov/oes/current/oes_nat.htm [<https://perma.cc/8FTZ-FCMW>].

^e U.S. Dep't of Homeland Sec., Off. of Immigr. Stat., 2003 *Yearbook of Immigration Statistics* (2004), <https://www.dhs.gov/ohss/topics/immigration/yearbook/2003> [<https://perma.cc/FSJ3-XRSG>].

^f U.S. Dep't of Homeland Sec., Off. of Immigr. Stat., 2012 *Yearbook of Immigration Statistics* (2013), <https://www.dhs.gov/ohss/topics/immigration/yearbook/2012> [<https://perma.cc/XZG6-WL65>].

^g U.S. Dep't of Homeland Sec., Off. of Immigr. Stat., 2022 *Yearbook of Immigration Statistics* (2023), <https://www.dhs.gov/ohss/topics/immigration/yearbook/2022> [<https://perma.cc/9YXU-Y2EF>].

^h U.S. Dep't of Just., Exec. Off. for Immigr. Rev., *Adjudication Statistics: Asylum Decision Rates by Nationality* (2023), <https://www.justice.gov/eoir/page/file/1107366/dl> [<https://perma.cc/PJ7C-GRK4>].

ⁱ *How Many Politicians Are There in the USA?* PoliEngine, <https://poliengine.com/blog/how-many-politicians-are-there-in-the-us> [<https://perma.cc/D5DG-KJHM>].

^j Ctr. on Nonprofits, Philanthropy, and Soc. Enter., George Mason U., *Nonprofit Employment Data Project Jobs Recovery Data Dashboard* (Jan. 10, 2023), <https://nonprofitcenter.schar.gmu.edu/nonprofit-employment-data-project/resources-and-dashboards/> [<https://perma.cc/2XBZ-ACDW>].

^k Andrew R. Flores & Kerith J. Conron, *Adult LGBT Population in the United States*, Williams Inst., UCLA Sch. of L. (2023), <https://williamsinstitute.law.ucla.edu/publications/adult-lgbt-pop-us/> [<https://perma.cc/MZQ2-EAP9>].

^l 2022 PRRI *Census of American Religion: Religious Affiliation Updates and Trends*, PRRI (Feb. 24, 2023), <https://www.prii.org/spotlight/prri-2022-american-values-atlas-religious-affiliation-updates-and-trends/> [<https://perma.cc/BQA7-MK2J>].

^m U.S. Census Bureau, K200201: *Race*, American Community Survey, 1-Year Supplemental Estimates (2022), <https://data.census.gov/table/ACSSE2022.K200201> [<https://perma.cc/XJ3V-LH8J>].

c. Summary of Baseline (Without the Proposed Rule)

As stated in part IV.A.1 of this preamble, the government-related data or bulk U.S. sensitive personal data discussed here may, under certain conditions, be used against individuals—such as members of the military, government employees, and government contractors—for illicit purposes, including blackmail and espionage. The risks of any particular individual or group being targeted may vary depending on the circumstances, and these data illustrate the range of such activities. Countries of concern can also use access to government-related data or Americans' bulk U.S. sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, and members of nongovernmental organizations or marginalized communities to intimidate such persons; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

The individuals within the subgroups most at risk of having their sensitive personal data exploited by countries of concern not only play important roles in American society, but also make up a large portion of the population. When we consider that threats to the spouses and children of targeted individuals could also be made, the Department estimates that the total population of individuals who could potentially be

targeted is well over 100 million individuals. Thus, the total number of those who are at risk of being targeted by foreign adversaries could exceed one-third of the entire American population. Failing to prevent the current and future sale or transfer of government-related data or bulk U.S. sensitive personal data to countries of concern effectively forgoes all the benefits that may be realized from such an action. Given the nature of the benefits to be gained from protecting national security and foreign policy from malicious actors, these benefits are unable to be monetized or quantified but will be contrasted with the estimated costs of the proposed regulation.

6. Alternative Approaches

In addition to the proposed action, the Department considered two alternatives. The first alternative, the No Action alternative, would take no regulatory action and allow the unrestricted transfer of bulk U.S. sensitive personal data to any foreign company, person, or country, including the countries of concern. The No Action alternative would not achieve the benefits of reducing the risks to the targeted populations or to U.S. national security and foreign policy. The growing threats related to foreign adversaries' use of bulk U.S. sensitive personal data, enhanced by advancing technologies such as artificial intelligence, for purposes of subjecting American citizens to exposure to blackmail and other malicious actions would continue.

In addition to the sale of bulk U.S. sensitive personal data, the vendor, employment, and investment agreements would also continue without restrictions, as would the risks that the proposed rule is intended to reduce. Of course, the No Action alternative would also result in no additional costs to industry. As explained in part VII.A.7 of this preamble, however, the Department considers the expected benefits of the proposed regulation to greatly exceed the estimated costs, resulting in net benefits that are not realized by the No Action alternative. Therefore, the Department rejects the No Action alternative.

The second alternative considered was a prohibition of the transfer to countries of concern of all data that would fall within the scope of the proposed rule. This alternative would go further than directed by the Order, the provisions of which were directed at bulk U.S. sensitive personal data and would entail more complicated and costly enforcement efforts than the proposed rule. Since this alternative would prohibit not only bulk U.S. sensitive personal data but also small transfers of sensitive personal data that may not present any marginal substantial risk to national defense or foreign policy, the small additional benefits are not likely to justify the much larger value of lost transactions and compliance costs than the proposed rule's estimated cost of \$502 million.

Since the marginal costs of this alternative over the costs of the proposed regulation are expected to be larger than the marginal benefits—if there are any—associated with it, this alternative would necessarily have lower net benefits, as measured by total benefits less total costs.

More generally, in addressing proposals from commenters, the Department also considered alternatives that could broaden the scope of the rule (and thus potentially be more costly) or narrow its scope (and thus potentially be less costly). These alternatives include, for example, lowering or increasing the proposed bulk thresholds, prohibiting or restricting (instead of exempting) additional categories of transactions such as those involving telecommunications or clinical-trial data, expanding the list of countries of concern, and expanding the categories of covered persons. The Department declined to adopt them because they would appear not to appropriately tailor the proposed rule to the national security risks and could cause unintended economic effects, for the reasons more fully discussed with respect to those proposals.

7. Benefits of the Proposed Rule

As mentioned in part VII.A.2 of this preamble, the benefits of the proposed rule associated with reducing threats to national security and foreign policy are difficult to measure. While these benefits are difficult to measure, there is a liberal opportunity for foreign adversaries to access and exploit Americans' sensitive data without the proposed rule. This situation and the best-available information indicate that there is a high likelihood of harm to national security and that the harm to national security could be high, suggesting that the expected benefits of the proposed rule exceed its expected costs. Alternatively, even if the likelihood of harm to national security is low in some circumstances, the potential damage to national security remains high, suggesting that even modest risk reductions are justified.

The proposed rule focuses on the risk of access to government-related data or bulk U.S. sensitive personal data by countries of concern and covered persons. Countries of concern can use their access to Americans' bulk sensitive personal data to engage in malicious cyber-enabled activities and malign foreign influence as well as to track and build profiles of U.S. individuals, including members of the military and Federal employees and contractors, for illicit purposes such as blackmail and espionage. Countries of concern can also

exploit their access to Americans' bulk sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, and members of nongovernmental organizations or marginalized communities to intimidate them; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties. Nongovernmental experts have underscored these risks.

Reducing these threats may produce many qualitative benefits, such as improving the security of the American people and safeguarding democratic values, all of which are beyond a reasonable, reliable, and acceptable estimate of quantified monetary value. Other benefits may also arise, such as the creation of new businesses to provide vetting information to firms seeking entrance into the restricted transactions market, or advancements in overall industry cybersecurity technology that result in more secure systems. We make no attempt to quantify these potential benefits, but we welcome comments that may allow us to do so.

8. Costs of the Proposed Rule

The economic costs of the proposed rule are the lost economic value of the covered transactions that are prohibited or forgone, referred to as "direct costs," and the costs of compliance (for restricted transactions, the cost of complying with the security requirements established by DHS/CISA, affirmative due diligence requirements, audit requirements, and affirmative reporting requirements).

Other provisions included in the regulations—including regulations of investment, employment, and vendor agreements through the imposition of security requirements—will have a mixture of economic impacts, such as one-time costs of switching to approaches that will comply with new regulations, and economic benefits, such as improved cybersecurity controls.

The challenge of estimating the economic impact with any degree of precision is that, because there are no regulations prohibiting cross-border bulk U.S. sensitive personal data transactions, currently available data provides incomplete, unreliable, or irrelevant estimates of the types, volume, and value of the bulk U.S. sensitive personal data transfer activity and thus creates uncertainty in estimates of lost value due to the proposed rule.

Similarly, the estimates of the costs of requirements for affirmative due diligence, security, recordkeeping, affirmative reporting, and audits are very preliminary in this analysis because the size of the industry, per-company costs, and per-transaction costs are very difficult to estimate precisely. Furthermore, based on its experience with similar regulations related to economic sanctions and export controls, the Department expects the costs of compliance with this proposed rule to vary significantly across companies.

Our estimates reflect costs for firms that currently engage in transactions involving bulk U.S. sensitive personal data. The universe of firms that engage in transactions involving bulk U.S. sensitive personal data is larger than the subset of such firms that knowingly transfer such data to countries of concern or covered persons; this larger universe of firms will need to undertake some due diligence measures to ensure that their typical data transfers are not in fact going to countries of concern or covered persons. Comments are solicited and welcome on the estimates that follow.

a. Value of Lost and Forgone Transactions

The costs of the proposed rule would include the economic value of lost or forgone transactions related to the sale, transfer, and licensing of bulk U.S. sensitive personal data, as well as biospecimens, to the six countries of concern. These lost or forgone transactions would include transactions that are prohibited as well as covered data transactions that are forgone because an entity decides not to bear the costs of complying with the due diligence and security requirements necessary to engage in a restricted transaction.

The total economic value of lost and forgone transactions should not exceed the total economic value of such exports to these countries of concern, as, all else equal, an entity would forgo a transaction if its expected compliance costs exceed the expected economic value of the transaction. The anticipated value of potentially regulated transactions with all countries of concern except China is negligible, given the lack of general cross-border transactions involving bulk sensitive personal data and the existing impediments to trade, such as economic sanctions. More specifically, in recent years, the proportions of U.S. bidirectional trade and investment

represented by trade with Iran,⁴⁸⁷ North Korea,⁴⁸⁸ and Cuba,⁴⁸⁹ respectively, have been negligible or unknown. Trade with Venezuela represents 0.1 percent of U.S. totals.⁴⁹⁰

Trade with Russia averaged about 0.5 percent of all U.S. trade from 2014 to 2023, dropping to 0.1 percent in 2023.⁴⁹¹ U.S. cross-investment (*i.e.*, two-way foreign direct investment)⁴⁹² with Russia averaged about 0.2 percent of total U.S. foreign cross-investment from 2013 to 2022.⁴⁹³ In contrast, the

respective shares of U.S. imports/exports and cross-investment that are conducted with China have averaged about 12 percent and 1.3 percent, respectively, during the same periods.⁴⁹⁴ Given this, the estimation of the economic costs of lost or forgone transactions here focuses primarily on China, although Russia is also considered.

Similarly, foreign direct investment into the United States from countries of concern in the information industry is a

relatively small portion of the total level of foreign direct investment in this sector. Chinese investment, which has been the highest among countries of concern, has been steadily falling over the past several years. Foreign direct investment figures, based on the country of the ultimate beneficial owner and the country of direct foreign ownership, are presented in Tables VII-4 and VII-5 of this preamble.

TABLE VII-4—FOREIGN DIRECT INVESTMENT POSITION IN THE UNITED STATES ON A HISTORICAL-COST BASIS IN THE INFORMATION INDUSTRY BY COUNTRY OF ULTIMATE BENEFICIAL OWNER

[millions of dollars]

	2016	2017	2018	2019	2020	2021	2022
All Countries Total	171,474	197,266	208,932	204,950	182,913	259,867	254,691
China	1,806	2,413	2,286	2,936	1,700	1,432	452
Hong Kong	366	416	148	562	413	429	417
Venezuela	(*)	(*)	−3	−5	−6	−7	(D)
China + Hong Kong							
Share	1.3%	1.4%	1.2%	1.7%	1.2%	0.7%	0.3%
Venezuela Share	n/a	n/a	0.0%	0.0%	0.0%	0.0%	n/a

Note: (*) indicates a nonzero value that rounds to zero. (D) indicates that the data in the cell have been suppressed to avoid disclosure of data of individual companies.

[illegible]

TABLE VII-5—FOREIGN DIRECT INVESTMENT POSITION IN THE UNITED STATES ON A HISTORICAL-COST BASIS IN THE INFORMATION INDUSTRY BY COUNTRY OF DIRECT FOREIGN PARENT

[millions of dollars]

	2016	2017	2018	2019	2020	2021	2022
All Countries Total	171,474	197,266	208,932	204,950	182,913	259,867	254,691
China	134	(D)	4,286	4,882	3,480	2,809	772
Hong Kong	(D)	(D)	– 53	389	284	282	196
Venezuela	– 4	(D)	– 3	– 2	– 2	(*)	(D)
China + Hong Kong							
Share	n/a	n/a	2.0%	2.6%	2.1%	1.2%	0.5%
Venezuela Share	0.0%	n/a	0.0%	0.0%	0.0%	N/A	N/A

Note: (*) indicates a nonzero value that rounds to zero. (D) indicates that the data in the cell have been suppressed to avoid disclosure of data of individual companies.

Source: U.S. Bureau of Econ. Analysis, *Balance of Payments and Direct Investment Position Data: Foreign Direct Investment in the U.S., Foreign Direct Investment Position in the United States on a Historical-Cost Basis*, By Country and Industry (NAICS) (Millions of Dollars) https://apps.bea.gov/iTable/?ReqID=2&step=-1&_gl=1*a*y559c*_ga*MTM5ODMzNTkyNyxNzEwMjgzOTY0*_ga_J4698JNNFT*MTcyMjk0ODk5My4yNi4xLjE3MjI5NTA2NTEuNTcuMC4w#eyJhcHBZC16Miwic3RicHMlOiIsLDlsMyw0LDUsNywwMF0slmRhdGEiOiItblIN0ZXAxUHJvbXB0NCsIsijjiXSBxblIN0ZXAxUHJvbXB0MilsIjEiXSBxblIN0ZXAxUHJvbXB0MylsIjEiXSBxblIN0ZXAZUeHJvbXB0NCIsIjlyll0sWjYtDGVVNFByb21wdDIULClI0sIl0sWjYtDGVVNVByb21wdDYiLCxlI0sWjYtDGVVNVByb21wY21wdGIlFsiNJiYiLCI0NSIsIjlyllwiNiAlClI0CSIsIjU2liWlNTUiXSV0VsWjYtDGVVOFBjb21wdDBlbiBljXlV0VsWjYtDGVVOFBjb21wdDEwQSQsWjYxIlI0dX00 = [<https://perma.cc/NH7V-GZNU>].

⁴⁸⁷ U.S. Census Bureau, *Trade in Goods with Iran*, <https://www.census.gov/foreign-trade/balance/c5070.html> [<https://perma.cc/EAZ7-PJU2>].

488 U.S. Census Bureau, *Trade in Goods with Korea, North*, <https://www.census.gov/foreign-trade/balance/c5790.html> [<https://perma.cc/NY7X-DRBA>].

489 U.S. Census Bureau, *Trade in Goods with Cuba*, <https://www.census.gov/foreign-trade/balance/c2390.html> [<https://perma.cc/CUF2-FWWY>].

⁴⁹⁰ U.S. Bureau of Econ. Analysis, *U.S. International Trade in Goods and Services, Venezuela*, Venezuela—International Trade and Investment Country Facts, <https://apps.bea.gov/international/factsheet/factsheet.html#219> [<https://perma.cc/2K9N-YGFS>].

491 U.S. Bureau of Econ. Analysis, *U.S. International Trade in Goods and Services, Russia, Russia—International Trade and Investment Country Facts*, <https://apps.bea.gov/international/factsheet/factsheet.html#341> [<https://perma.cc/GF8U-6GK2>].

⁴⁹² Mark Casson & Nigel Wadeson, *Cross-Investments by Multinationals: A New Perspective*, 14 Glob. Strategy J. 279, 279–80 (2023) (defining cross-investment as “where firms conduct FDI into each other’s home countries”).

⁴⁹³ U.S. Bureau of Econ. Analysis, *supra* note 491.

⁴⁹⁴ U.S. International Trade in Goods and Services, China, China—International Trade and Investment Country Facts, <https://apps.bea.gov/international/factsheet/factsheet.html#650> [https://perma.cc/X7OF-CYXH].

Note that some fraction of the lost or forgone data transactions may be for beneficial uses. Beneficial uses of bulk U.S. sensitive personal data in the countries of concern may include consumer-choice improvements and the use of artificial intelligence to expedite innovation in drug discovery and increase knowledge of patterns of, for example, consumption, commerce, transportation, traffic, information/news transmission, nutrition, and health.

The following analysis relies in part on data available from the BEA on U.S. exports of telecommunications, computer, and information services, both in total and for each of the three sub-categories, to China and Russia. Tables VII–6 and VII–7 of this preamble rely on an analysis of the BEA data to approximate the value of lost transactions.

i. Global Market Value of Genomic, Biometric, and Location Data

Genomic data includes data that is used in drug discovery and development, specifically in developing products such as systems, software, and reagents, and in developing processes such as cell isolation, sample preparation, and genomic analysis.⁴⁹⁵ Biometric data is used in consumer electronics and automotive applications for safety, surveillance, and identification methods, including facial, posture, voice, fingerprint, and iris recognition technologies.⁴⁹⁶ Location data is used in smart devices, network services for improved connectivity, systems integration, monitoring, and satellite location technology, as well as to produce timely, relevant and personalized offers/information for customers.⁴⁹⁷

According to market research data from one company,⁴⁹⁸ the global genomics market's value is estimated at \$27.58 billion in 2021, \$32.56 billion in 2022, and, given an estimated compound annual growth rate of 18.2 percent, \$38.49 billion in 2023 and \$45.49 billion in 2024.⁴⁹⁹ One estimate of the global biometric technology market values it at \$34.27 billion in 2022 and, given an estimated 20.4 percent compound annual growth rate, \$41.26 billion in 2023 and \$49.68 billion in 2024.⁵⁰⁰ Finally, one estimate values the global location data market at \$18.52 billion in 2023 and, given an estimated 15.6 percent compound annual growth rate, \$21.41 billion in 2024.⁵⁰¹ Table VII–6 of this preamble presents these global totals for genomic, biometric, and location data estimates.⁵⁰²

TABLE VII–6—GLOBAL TECHNOLOGY MARKET VALUE ESTIMATES FOR GENOMIC, BIOMETRIC, AND LOCATION DATA FOR 2021–2024 (IN BILLIONS OF 2022 DOLLARS) WITH COMPOUND ANNUAL GROWTH RATE (“CAGR”)

Data type	2021	2022	2023	2024	CAGR (%)
Genomic ^a	\$27.58	\$32.56	\$38.49	\$45.49	18.2
Biometric ^b		34.27	41.26	49.68	20.4
Location ^c			18.52	21.41	15.6

^a *Genomics Global Market to Reach \$63.5 Billion in 2026 at a CAGR of 18.2%*, Globe Newswire (Sept. 6, 2022), <https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html> [<https://perma.cc/SUV8-VVMK>].

^b Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), <https://www.grandviewresearch.com/industry-analysis/biometrics-industry> [<https://perma.cc/KN36-3KZW>].

^c Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), <https://www.grandviewresearch.com/industry-analysis/location-intelligence-market> [<https://perma.cc/WS6U-2324>].

ii. U.S. Exports to Relevant Specific Categories and to Countries of Concern

Data is available on U.S. exports in the category of telecommunications, computer, and information services, both in total and for each of these three service subcategories, to China and Russia.⁵⁰³ Data on exports in a relevant sub-category of information services—database and other information services—is available globally and for both China and Russia individually.

Telecommunications, Computer, and Information Services is one of the

eleven service categories BEA presents in the U.S. international transactions accounts. The Telecommunications Services sub-category includes basic services (e.g., transmitting messages between destinations) as well as value-added and support services. The Computer Services sub-category includes software, computing and data-storage services, hardware and software consultancy, and licensing agreements tied to downloading applications. The category of information services includes database services and web search portals, which belong to one

subcategory, and news agency services, which belong to the other.⁵⁰⁴ This Database Services sub-category includes data brokers.

Table VII–7 of this preamble presents the value of U.S. exports of telecommunications services, computer services, information services, and the database and other information services component of information services. The table also reports exports to China for the three components combined and the exports to China and Russia individually for database and other information services.

⁴⁹⁵ *Genomics Global Market to Reach \$63.5 Billion in 2026 at a CAGR of 18.2%*, Globe Newswire (Sept. 6, 2022), <https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html> [<https://perma.cc/SUV8-VVMK>].

⁴⁹⁶ Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), <https://www.grandviewresearch.com/industry-analysis/biometrics-industry> [<https://perma.cc/KN36-3KZW>].

⁴⁹⁷ Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), <https://www.grandviewresearch.com/industry-analysis/location-intelligence-market> [<https://perma.cc/WS6U-2324>].

⁴⁹⁸ *Genomics Global Market to Reach \$63.5 Billion in 2026 at a CAGR of 18.2%*, *supra* note 495.

⁴⁹⁹ *Id.*

⁵⁰⁰ Grand View Research, *supra* note 496.

⁵⁰¹ Grand View Research, *supra* note 497.

⁵⁰² The Department notes several caveats with the Grand View Research estimates shown in Tables

VII–4 and VII–5 of this preamble, including non-transparent methods for gathering data and producing estimates, a non-statistical sample of firms that may not be statistically representative of the industry, and non-response bias from interviewees from the firms.

⁵⁰³ U.S. Bureau of Econ. Analysis, *U.S. International Economic Accounts: Concepts and Methods*, at 248 (June 2023), <https://www.bea.gov/system/files/2023-06/iea-concepts-methods-2023.pdf> [<https://perma.cc/8M48-Q2ZG>].

⁵⁰⁴ *Id.*

TABLE VII-7—U.S. EXPORTS OF TELECOMMUNICATIONS, COMPUTER, AND INFORMATION SERVICES
[In billions of 2023 dollars]

Service	All	China	Russia
Components			
Telecommunications Services	\$9.329	\$0.095	\$0.041
Computer Services	\$50.328	\$1.847	\$0.113
Information Services	\$10.972	\$0.318	\$0.034
Total Value	\$70.629	\$2.260	\$0.188
Percentage of Total	100%	3.20%	0.27%
Database and Other Information Services			
Value	\$10.768	*\$0.318	\$0.032
Percentage of Total	100%	2.94%	0.30%

Source: U.S. Bureau of Econ. Analysis, *International Transactions, International Services, and International Investment Position Tables*, Tables 2.2, <https://www.bea.gov/itable/direct-investment-multinational-enterprises> [<https://perma.cc/9XWQ-A8YQ>] (last updated July 23, 2024).

* An upper bound for 2023 is \$0.318.

The \$10.768 billion Database and Other Information Services sub-category comprises most (98.1 percent) of the \$10.972 billion Information Services category, with the other \$0.275 billion (2.6 percent) in the News-Agency Services category. For the Database and Other Information Services sub-category, U.S. exports to China are \$0.318 billion (\$318 million) for 2023, which is 2.94 percent of the U.S. export total. U.S. exports to Russia are \$0.32 billion (\$32 million), which is 0.30 percent of the U.S. export total.

These U.S. export estimates are significantly over-inclusive, as they include many kinds of data that are explicitly excluded from regulation under the proposed rule, such as web browser history and other expressive data, in addition to services that do not involve data transfer at all. Consequently, the estimates of the costs due to lost or foregone transactions resulting from the proposed rule are probably overstated.

Tables VII-6 and VII-7 of this preamble comprise the “raw” data on U.S. exports to countries of concern that provide upper-bound estimates of the value of lost or forgone transactions. Given the available data that informs the following analysis, the Department welcomes comments on the use of this data and on any alternative or additional data that could also be employed.

iii. Estimates of U.S. Exports of Genomic, Biometric, and Location Data

This section provides estimates of U.S. revenue from sales for three categories of data covered under the proposed rule for which data on the

global market are available: genomic, biometric, and location data.

Given the lack of available published estimates of the value of U.S. exports of such data to China, Russia, and other countries of concern, the Department developed a multi-step method for estimating the value of lost transactions in genomic, biometric, and location data to the countries of concern. To summarize, we began with market research companies’ estimates of the size of the global markets in geometric, biometric, and location data shown in Table VII-6 of this preamble. Then we derived estimates of the value of lost transactions through a three-step process that involved estimating the U.S. share (domestic plus export) of the global market, estimating the percentage of U.S. global sales that are domestic, and finally making some data-informed assumptions about the share of global sales in those industries that were to the countries of concern.

In 2022, the total value of the U.S. location data market was \$4.20 billion, with a projected compound annual growth rate of 13.6 percent.⁵⁰⁵ Based on these estimates, it can be projected that the U.S. portion in 2023 would be \$4.77 billion ($\$4.20 \times 1.136 = \$4.77$). As shown in Table VII-6 of this preamble, the market research company estimated that the global market value of location data in 2023 was \$18.52 billion, so the estimated U.S. portion in 2023 would constitute 25.76 percent of that estimated global value ($\$4.77/\$18.52 = 0.2576$). Because the market research company estimated the U.S. compound annual growth rate for location data to be 13.6 percent and the global

compound annual growth rate to be 15.6 percent, it can be projected that the U.S. portion of the global market in 2024 would fall slightly, from 25.76 percent to 25.31 percent ($(\$4.77 \times 1.136)/(\$18.52 \times 1.156) = 0.2531$).

The market research company estimated that the North American revenue share of the global biometric technology market in 2022 was 30.7 percent.⁵⁰⁶ If Canada and Mexico were responsible for 5 percent of global market value, then the U.S. share of the global biometric data market in 2022 would be 25.7 percent, nearly the same as the portion for location data in 2023. Given the alignment in our estimates of the U.S. market share for location and biometric data markets, we assume that the estimated U.S. location data market in 2024 (25.31 percent) also applies to the U.S. portion of global genomic and biometric data. With that assumption, we estimate that the U.S. genomic data market is worth \$12.57 billion in 2024 (25.31 percent of \$49.68 billion (from Table VII-6 of this preamble)), and the U.S. market is worth \$5.42 billion (25.31 percent of \$21.41 billion). Table VII-8 of this preamble provides 2024 estimates of U.S. revenue (foreign plus domestic) for those three industries.

Next, the Department assumes that U.S. exports in genomic, biometric, and location data constitute 30 percent of total U.S. revenue (domestic sales plus exports). This assumption is based on market research from a U.S.-based company,⁵⁰⁷ which estimated that in

⁵⁰⁶ Grand View Research, *supra* note 496.

⁵⁰⁷ Market research data includes: *Genomics Global Market to Reach \$63.5 Billion in 2026 at a CAGR of 18.2%*, *supra* note 495; Grand View Research, *supra* note 496; Grand View Research, *supra* note 497.

⁵⁰⁵ Grand View Research, *supra* note 497.

2017, 30 percent of revenue for data brokerage companies came from international sales. When applying this assumption to revenue from sales of genomic, biometric, and location data, we estimate that exports of U.S.

genomic data in 2023 were worth \$3.454 billion for genomic data (30 percent of \$11.513 billion); exports of biometric data were worth \$3.772 billion (30 percent of \$12.574 billion); and exports of location data were worth \$1.626

billion (30 percent of \$5.419 billion). Table VII–8 of this preamble presents estimated revenue from U.S. exports (Step 2) alongside the other estimates from which it was derived.

TABLE VII–8—ESTIMATED REVENUE FROM INTERNATIONAL SALES OF GENOMIC, BIOMETRIC, AND LOCATION DATA IN 2023
[In billions of 2024 dollars]

Category of data	Global revenue (from Table VII-6) ^a	U.S. revenue (domestic sales + exports) ^b	Revenue from U.S. exports ^c
Genomic	\$45.49	\$11.51	\$3.45
Biometric	\$49.68	\$12.57	\$3.77
Location	\$21.41	\$5.42	\$1.63
Total	\$116.58	\$29.51	\$8.85
U.S. Revenue Share of Global Total		25.31%	
U.S. Export Share of U.S. Revenue			30%

^a *Genomics Global Market to Reach \$63.5 Billion in 2026 at a CAGR of 18.2%*, Globe Newswire (Sept. 6, 2022), <https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html> [<https://perma.cc/SUV8-VVMK>]; Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), <https://www.grandviewresearch.com/industry-analysis/biometrics-industry> [<https://perma.cc/KN36-3KZW>]; Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), <https://www.grandviewresearch.com/industry-analysis/location-intelligence-market> [<https://perma.cc/WS6U-2324>].

^b Department of Justice estimates based on global revenue data from Table VII–6 of this preamble. U.S. Revenue (Domestic Sales + Exports) is assumed to be 25.31 percent of the total global revenue for each category of data.

^c Department of Justice estimates based on data in global revenue data from Table VII–6 of this preamble. Revenue from U.S. exports is assumed to be 30 percent of the U.S. revenue for each category of data.

To reiterate, the Department assumes that U.S. exports in genomic, biometric, and location data constitute 30 percent of total U.S. revenue (domestic sales plus exports). The Department uses this assumption to inform the analysis throughout part VII of this preamble.

iv. Estimates of U.S. Exports of Genomic, Biometric, and Location Data to the Six Countries of Concern

As delineated above in this section, the current value of potentially regulated transactions with all countries of concern except China and, to a lesser degree, Russia is negligible, given the lack of general cross-border trade in data

and data-driven services and the general impediments to trade with these countries of concern, such as economic sanctions. We therefore focus this part of the analysis on China, and to a lesser degree on Russia due to the \$32 million in U.S. exports of database and other information services to Russia.⁵⁰⁸ The Department lacks data on cross-border transfers of genomic, biometric, and location data other than sales. An example of such cross-border transfers may include transfer of data within multinational companies.

As set forth in Table VII–7 of this preamble and the subsequent discussion

in part VII.A.8.a.ii of this preamble, 3 percent (0.032 = \$0.318 of \$10.768 billion) of U.S. exports of database and other information services are currently to China and 1 percent are to Russia (0.0106 = \$0.111 of \$10.768 billion). Applying these percentages to the value of U.S. exports of genomic, biometric, and location data set forth in Table VII–8 of this preamble yields estimates for the value of U.S. exports of genomic, biometric, and location data to China and Russia. The estimates for U.S. exports of genomic, biometric and location data to China total \$267 million and to Russia total \$94 million.

TABLE VII–9—ESTIMATES OF U.S. EXPORTS OF GENOMIC, BIOMETRIC, AND LOCATION DATA TO CHINA AND RUSSIA
[In billions of 2022 dollars]

Category of data	U.S. exports (from table VII-8)	U.S. exports to China ^a	U.S. exports to Russia ^b
Genomic	\$3.45	\$0.10	\$0.04
Biometric	\$3.77	\$0.11	\$0.04
Location	\$1.63	\$0.05	\$0.02
Total	\$8.85	\$0.27	\$0.10
China share of U.S. exports		3.02%	
Russia share of U.S. exports			1.06%

^a Revenue from U.S. exports to China is assumed to be 3.02 percent of total revenue from U.S. exports for each category of data.

^b Revenue from U.S. exports to Russia is assumed to be 1.06 percent of total revenue from U.S. exports for each category of data.

⁵⁰⁸ See discussion in part VII.A.8.a of this preamble.

Source: Department of Justice estimates based on market research data from U.S.-based company, including: *Genomics Global Market to Reach \$63.5 Billion in 2026 at a CAGR of 18.2%*, Globe Newswire (Sept. 6, 2022), <https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html> [https://perma.cc/SUV8-VVMK]; Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), <https://www.grandviewresearch.com/industry-analysis/biometrics-industry> [https://perma.cc/KN36-3KZW]; Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), <https://www.grandviewresearch.com/industry-analysis/location-intelligence-market> [https://perma.cc/WS6U-2324].

v. Total Estimated Value of Lost and Forgone Transactions

To reiterate, U.S. exports of genomic, biometric, and location data to China and Russia totaled approximately \$361 million in 2022. Some of these exports

may have been for beneficial uses, such as consumer-choice improvement; effective medical responses; and increased knowledge of patterns of consumption, commerce, transportation, traffic, information/news transmission, nutrition, and health. The Department's

estimates of the value of lost transactions do not include the potential value of any lost positive externalities to U.S. residents. The estimated annual value of lost or forgone transactions is presented in Table VII-10 of this preamble.

TABLE VII-10—ESTIMATED ANNUAL VALUE OF LOST TRANSACTIONS: GENOMIC, BIOMETRIC, AND LOCATION DATA
[In millions of 2022 dollars]

Country of concern	Value of forgone transactions
China	\$267
Russia	94
Total	361

Source: Department of Justice estimates based on market research data from U.S.-based company, including: *Genomics Global Market to Reach \$63.5 Billion in 2026 at a CAGR of 18.2%*, Globe Newswire (Sept. 6, 2022), <https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html> [https://perma.cc/SUV8-VVMK]; Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), <https://www.grandviewresearch.com/industry-analysis/biometrics-industry> [https://perma.cc/KN36-3KZW]; Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), <https://www.grandviewresearch.com/industry-analysis/location-intelligence-market> [https://perma.cc/WS6U-2324].

The Department welcomes comments on the use of this data and on any alternative or additional data that could also be employed. The Department reiterates the following limitations on these estimates, described in further detail in the analysis above:

1. The estimate assumes that the U.S. share of the global market value for location data is the same as the U.S. share of the global market value for genomic and biometric technology.

2. The export share of each of these respective U.S. markets is assumed to be the same as the share of revenue of U.S. data-brokerage companies that comes from international sales, which is 30 percent.

3. The estimate assumes that the database (and other information) services category of BEA's data includes most data brokers.

4. The estimate uses the share of U.S. exports of database and other information services that go to China and Russia to estimate the share of U.S. exports of genomic, biometric, and location data that go to China and Russia.

5. The Department assumes that the annual economic value of lost and forgone transactions would be equal to the value of all U.S. exports of biometric, location, and genomic data to China and Russia.

vi. Alternative Methodology for Estimating the Value of Lost and Forgone Transactions

An alternative estimate of the value of U.S. exports to China and Russia for this analysis can be derived from BEA data on the value of U.S. exports of database and other information services. As

shown in the bottom of Table VII-7 of this preamble, BEA's estimates for 2023 were \$318 million for China and \$32 million for Russia.

Given the rapid growth of Chinese exports, the Department projected the 2023 BEA estimate forward to 2024. Based on the growth rates of U.S. exports of information services to China between 2006 and 2023,⁵⁰⁹ using an annual growth rate of 5 percent for China⁵¹⁰ would increase BEA's \$318 million estimate for 2023 to \$334 million for 2024.

The Department's alternative estimates for the value of lost transactions are \$334 million in forgone exports of information services to China and \$32 million in foregone exports of information services to Russia, as shown in Table VII–11 of this preamble.

⁵⁰⁹ U.S. Bureau of Econ. Analysis, *Table 2.3. U.S. Trade in Services, by Country or Affiliation and by Type of Service, International Transactions, International Services, and International Investment* Position Tables, <https://apps.bea.gov/iTable/?reqid=62&step=9&isuri=1&product=4#eyJhCkBpZC16NjIsInN0ZXZBZjlpbW5wS1Y3QwILC1010sN0sImRhIdG9iOltbInBvb2R1SDQwILC1010sN0sWw>

[illegible]

pbHRLcl8jMyIsWyIxiIwiNTUi
LCI2MSIsIjYzIl1dLFsiRmIsdGV
yXyM0IixbljAiXV0sWyjGaWx
0ZXjflzUiLFsiMCjdXV19 [<https://perma.cc/7USS-3PL1>].

⁵¹⁰ Chu Daye, *China Achieves 5.2% GDP Growth in 2023*, Global Times (Jan. 17, 2024), <https://www.globaltimes.cn/page/202401/1305571.shtml> [<https://perma.cc/3NGJ-RXZ7>].

TABLE VII-11—ESTIMATES OF THE ANNUAL VALUE OF LOST TRANSACTIONS USING ALTERNATIVE METHODOLOGY
[In millions of 2022 dollars]

Country of concern	Estimated value of U.S. exports of data and information services
China	\$334
Russia	32
Total	366

Source: U.S. Bureau of Econ. Analysis, *Table 2.3. U.S. Trade in Services, by Country or Affiliation and by Type of Service*, International Transactions, International Services, and International Position Tables, <https://apps.bea.gov/iTable/?reqid=62&step=9&isuri=1&product=4#eyJhcHBpZC16NjlsIn0XZXBzIjpbMSw5LDEwLDcsN10slmHrcGEiOltlbBibGByb2R1Y3QiLC10lloSWyJUYWJsZXUxc3Q1CzMDU4MyJdFsiVGFibGVMaxNU2Vjb25kYXJ5IiwiaWZAZ2NTYiXSBxbklzPzhHRic8IjBSIsWyxiIiwiaWlsilC10lwiNSIsIjYiIjECL3IiwiOCIsIjkiClxMCIsljExIiwiaWMTUiLCIxMyIsIjE0IiwiaWMTUiLCIxNiIsIjE3IiwiaWMTgiXV0sWyJGaWw0ZXJfZnllZlFsiGigiLCI3MyJdXSxbklzPzhHRic8IjMyIsWyxiIiwiaWNTUiLCI2MSIsIjYzIl1dLFsRmlsdGVyXyM0IixbljAiXV0sWyJGaWw0ZXJfZnllZlFsiMCJdXV19> [<https://perma.cc/7UDD-P3PL>]

Under this alternative methodology, the Department's estimate of the economic value of transactions lost due to the proposed rule is \$366 million per year (Table VII-11 of this preamble), compared with the \$361 million estimate reached in the main analysis (Table VII-10 of this preamble).

The alternative methodology may overestimate the annual value of lost transactions, since the BEA category for the Database and Other Information Services may include many kinds of data that are explicitly excluded from regulation under the proposed rule (such as web-browser history and other expressive data).⁵¹¹ The comparability of the main and alternative methodologies suggests that the main estimate of \$361 million may underestimate the annual value of lost transactions because it does not include personal financial data or health records. With these disparities in mind, we are estimating the value of lost transactions at the midpoint of these estimates, \$364 million, and solicit comments on this total.

The Department estimates that the economic value of lost or forgone transactions would be minimal for firms not engaged in data brokerage (*i.e.*, for restricted transactions). In other words, the Department assumes that firms not engaged in data brokerage would bear minimal economic costs beyond those that may be associated with implementing and maintaining a risk-based compliance program (as described in § 202.302 of the proposed rule). For example, the Department assumes that the small number of U.S.-based firms currently using Chinese cloud-service providers to store prohibited or restricted data would be able to switch to another cloud service provider at low or no cost, given that Chinese cloud-

service providers constitute only a tiny fraction of the cloud market for U.S.-based firms. The Department assumes that the other five countries of interest do not sell cloud services of any significant value to the United States.⁵¹²

b. Security Costs

Data security is an important aspect of protecting government-related data or bulk U.S. sensitive personal data from being improperly accessed by foreign adversaries or in ways that could pose a threat to national security. The proposed rule incorporates by reference proposed security requirements that have been developed by DHS through CISA, which represent conditions that businesses must meet to engage in restricted transactions. These security requirements are intended to address national security and foreign-policy threats that arise when countries of concern and covered persons access government-related data or bulk U.S. sensitive personal data that may be implicated by the categories of restricted transactions. Specifically, the proposed rule would prohibit U.S. persons from engaging in transactions unless they comply with three categories of requirements, the first two of which are addressed in the proposed security requirements, which are proposed to be incorporated by reference:

1. Organizational and system-level requirements for instituting cybersecurity policies, practices, and requirements for any covered system (which CISA proposes to define as a specific type of information system that is used to conduct a number of activities related to covered data as part of a restricted transaction).

2. Data-level requirements using any combination of the following capabilities necessary to prevent access to covered data by covered persons or countries of concern:

- a. Data minimization and data masking;
- b. Encryption;
- c. Privacy-enhancing technologies; and
- d. Denial of access.

3. Compliance-Related Requirements for Independent Testing and Auditing

These requirements would impose new costs on firms to the extent that they are not already voluntarily meeting such requirements. Any additional costs may be offset by reducing cyber incidents and their associated costs. The Department estimates the new cybersecurity-related costs imposed on affected firms by analyzing the costs that companies at different sizes and levels of technological maturity face when implementing existing security standards and frameworks of similar scope.

i. Similar Security Standards and Frameworks

The proposed rule would create cybersecurity standards that are based on, and thus overlap with, several similar, widely used cybersecurity standards or frameworks. Currently, firms engaged in transactions that are proposed to be restricted transactions are encouraged—but generally not explicitly required—to comply with existing Federal cybersecurity standards or frameworks. Given the similarities between the proposed rule’s security requirements and existing cybersecurity standards and frameworks, the costs of complying with one of the existing, commonly implemented sets of cybersecurity standards or frameworks are likely similar to the costs that would be incurred by businesses to comply

⁵¹¹ Sherman, *supra* note 6.

⁵¹²David McCabe, *China's Cloud Computing Firms Raise Concern for U.S.*, N.Y. Times (June 21, 2023), <https://www.nytimes.com/2023/06/21/technology/china-cloud-computing-concern.html> [<https://perma.cc/4CQJ-F6GJ>].

with the proposed rule. Furthermore, such costs will be offset because, as commenters generally agreed, most companies will already have foundational baseline security requirements in place.

As required by the Order, the security requirements for firms engaged in restricted transactions are based on the National Institute of Standards and Technology (“NIST”) Cybersecurity Framework (“CSF”) ⁵¹³ and the NIST Privacy Framework (“PF”). ⁵¹⁴ CISA has also leveraged existing performance goals, guidance, practices, and controls, including the CISA Cross-Sector Cybersecurity Performance Goals (“CPGs”), ⁵¹⁵ which are themselves based on the NIST CSF and PF.

The CPGs, NIST CSF, and NIST PF are sets of recommendations, based on current best practices, that companies can voluntarily follow. The CPGs are themselves mapped to the CSF. In its proposed security requirements, CISA has included mapping to the CPGs and NIST CSF and PF, as applicable. Furthermore, the CSF aligns its requirements with other similar standards that are commonly used in industry, including NIST SP 800–53 and International Organization for Standardization/International Electrotechnical Commission (“ISO”)/ (“IEC”) 27001:2013. The ISO/IEC 27001:2013 standard, unlike the CISA and NIST frameworks, has a more formal certification process and has granted certificates to 48,671 companies globally and 1,898 companies in the United States. ⁵¹⁶ Finally, NIST SP 800–171 rev.3, ⁵¹⁷ a common security

framework, lays out security standards for firms handling controlled unclassified information, while the Department of Defense’s Cybersecurity Maturity Model Certification (“CMMC”) program ⁵¹⁸ includes the NIST SP 800–171 requirements but with a more formal auditing and certification process.

ii. Current Industry Compliance Level

The majority of firms affected by the proposed rule likely already comply with some portion of the security requirements in the proposed rule. The level of existing adherence to the proposed security requirements for the average U.S. company would vary significantly based on each firm’s size, industry, existing regulatory landscape, technological maturity, and internalized priorities. ⁵¹⁹ Given the high degree of overlap between the DHS draft security requirements and existing standards and frameworks discussed below, it is possible that the level of existing compliance among affected firms will be high.

One survey of business expenditures on cybersecurity conducted by IANS Research indicates that such spending can vary depending on industry and business size. According to this survey, the average firm spent nearly 10 percent of its IT budget on cybersecurity, with firms in industries like technology, healthcare, and business services spending the highest proportion at over 13 percent. ⁵²⁰ Furthermore, in the same report, an analysis of firm size found that smaller businesses spend the highest proportion of their IT budgets on cybersecurity. ⁵²¹ While it is possible that companies with larger expenditures on cybersecurity would be closer to compliance with the proposed rule, it is difficult to determine with the available data the extent to which companies are

using their cybersecurity budgets to keep up with evolving best practices and maintain the capabilities required by the proposed security requirements.

The level of technological and cybersecurity maturity also varies significantly, even among larger firms. Recent data indicates that there is great variability in cybersecurity practice sophistication and maturity. In 2023, Deloitte conducted a survey of cyber decision makers at firms around the world with at least 1,000 employees and \$500 million in annual revenue. The Deloitte study determined that of these organizations, 38 percent had low cyber maturity (as defined in the study), 41 percent had medium cyber maturity, and 21 percent had high cyber maturity. ⁵²² Another survey of IT professionals found that 45 percent of firms did not have a designated Chief Information Security Officer, which would make them noncompliant with the proposed security requirements. ⁵²³

Furthermore, research suggests that the cost of cybersecurity activities can vary based on factors such as the size of the company, the cybersecurity capabilities required, and whether those capabilities are developed in house or by contracting with third parties. Additionally, the Center for internet Security provided high and low estimates of cybersecurity budgets based on company size, with an average estimate of \$22,000 for a small firm (1 to 10 employees) and about \$800,000 for a large firm (100 to 999 employees). ⁵²⁴

iii. Costs of Compliance

Regarding the cost of compliance, the Department assumes that most affected companies will not have to build cybersecurity capabilities from the ground up to meet the requirements of the proposed rule. Given that most firms will have existing cybersecurity protections in place, a more realistic approach to calculating the potential cost of the proposed rule would be to consider the additional expenditures that a company would have to make to increase its cybersecurity standards. The Department assumes, based on the

⁵¹³ Nat’l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (v. 1.1, Apr. 16, 2018), <https://doi.org/10.6028/NIST.CSWP.04162018> [<https://perma.cc/2FKZ-3PAT>].

⁵¹⁴ Nat’l Inst. of Standards & Tech., *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* (v. 1.0, Jan. 16, 2020), <https://doi.org/10.6028/NIST.CSWP.01162020> [<https://perma.cc/36SC-VZXX>].

⁵¹⁵ Cybersec. & Infrastructure Sec. Agency, *Cross-Sector Cybersecurity Performance Goals: March 2023 Update* (2023), https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_report_v1.0.1_final.pdf [<https://perma.cc/4YRS-Z9UJ>].

⁵¹⁶ Int’l Org. for Standardization, *ISO/IEC 27001:2013&2022 Information Technology—Security Techniques—Information Security Management Systems—Requirements*, 1. ISO Survey 2023 Results—Number of Certificates and Sites per Country and the Number of Sectors Overall (Sept. 18, 2024), <https://www.iso.org/committee/54998.html?i=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnPA3Dluxm&view=documents> [<https://perma.cc/L43C-MVY8>] (click “1. ISO Survey 2023 results—Number of certificates and sites per country and the number of sectors overall” to download spreadsheet; then open tab titled “ISO IEC 27001” in that file).

⁵¹⁷ Ron Ross & Victoria Pillitteri, Nat’l Inst. of Standards & Tech., NIST SP 800–171r3, *Protecting*

Controlled Unclassified Information in Nonfederal Systems and Organizations, Nat’l Inst. of Standards & Tech. (2024), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf> [<https://perma.cc/ER88-7Y8F>].

⁵¹⁸ U.S. Dep’t of Def., Office of the Undersecretary of Defense for Acquisition & Sustainment, *Cybersecurity Maturity Model Certification (CMMC) Model Overview Version 2.0* (2021), https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf [<https://perma.cc/2HAM-92TJ>].

⁵¹⁹ Deloitte, *2023 Global Future of Cyber Survey* (2023), https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2023/gx-deloitte_future_of_cyber_2023.pdf [<https://perma.cc/B9E3-QNRW>].

⁵²⁰ IANS Research, *Benchmark Insights: Security Budget Benchmark Summary Report 4* (2022), <https://cdn.iansresearch.com/Files/Marketing/IANSResearch-2022SecurityBudgetBenchmarkSummaryReport.pdf> [<https://perma.cc/B9SE-4YS5>].

⁵²¹ *Id.*

⁵²² Deloitte, *supra* note 519, at 14.

⁵²³ Navisite, *The State of Cybersecurity Leadership and Readiness, Fall 2021* (2021), at 4, https://lp.navisite.com/1/824543/2023-05-19/3733vx/824543/1684513240bPrtcWBS/state_of_cybersecurity_leadership_and_readiness_report.pdf [<https://perma.cc/6VQG-VGZG>].

⁵²⁴ The average budget estimates for the small and large firms were calculated by averaging the high and low estimates from the relevant size category. Ctr. for internet Sec., *The Cost of Cyber Defense: CIS Controls Implementation Group 1*, at 8 (v. 1.0, 2023), https://learn.cisecurity.org/1/799323/2023-08-02/4t3qkj/799323/1694810927NC0iZQGR/CISControls_Cost_of_Cyber_Defense_2023_08.pdf [<https://perma.cc/C46G-EZFR>].

design of the proposed rule, that added cybersecurity compliance costs will closely mirror the costs that companies face when complying with similar or more onerous/prescriptive standards, such as NIST 800–171, NIST 800–53, ISO/IEC 27001, and the CMMC program, providing a helpful tool to estimate the added compliance costs associated with the data security requirements, though such estimates may be conservative. Furthermore, since some firms may already clearly be in voluntary compliance with more stringent standards than the proposed security standards, which would allow them to forgo some of the following steps, some of the costs may not be incurred by all firms.

The first step that most firms engaging in restricted transactions will take toward compliance is completing an assessment of their current capabilities and shortcomings. For example, it would cost a small to medium-sized firm that is working toward compliance with NIST 800–171 and NIST 800–53 around \$30,000 to \$35,000 to build in-house assessment capabilities.⁵²⁵ Along the same lines, another source estimates that an assessment for a CMMC certification for a firm with 250 employees could cost up to \$35,000.⁵²⁶ For the initial assessment stage of the ISO/IEC 27001 certification process, a small business would expect to spend \$25,000 to \$40,000 to complete the process internally and around \$30,000 to hire a consultant.⁵²⁷ However, a

company with more complicated compliance issues could expect to pay as much as \$130,000 for the consulting and assessment.⁵²⁸ Thus, the Department finds that an assessment will cost between \$25,000 and \$130,000 for most firms, depending on the scale of the compliance needs involved.

The next step in the compliance process is remediating the issues found in the initial assessment. It is likely that remediation would involve a combination of fixed and recurring costs. One-time remediation costs could involve revising security policies or patching vulnerabilities in covered systems, while recurring costs could include subscriptions to services that provide data encryption, multifactor authentication, or password management services, as well as costs associated with maintaining access controls or required documentation. Estimates for remediation costs for NIST 800–171 compliance range between \$35,000 and \$115,000.⁵²⁹ Another estimate suggests that mid-sized companies with lower levels of technological maturity can expect to pay approximately \$100,000 to correct any compliance issues.⁵³⁰

In accordance with the security requirements with which U.S. persons engaged in restricted transactions must comply under the proposed rule, every firm, regardless of its initial compliance level, will need to annually verify its compliance through audits and testing. This is a common cost that firms incur

to comply with existing frameworks or standards. For a small company with 50 employees, the annual recertification audit for ISO/IEC 27001 compliance costs an estimated \$6,000 to \$7,500.⁵³¹ The continuous monitoring costs associated with NIST 800–171 compliance for small businesses are estimated to be around \$6,500 to \$13,000.⁵³² However, annual surveillance audits to ensure compliance with ISO/IEC 27001 standards can cost as much as \$40,000.⁵³³

Table VII–12 of this preamble summarizes the high and low estimates for the costs—both one-time and ongoing—that an average U.S. company engaged in restricted transactions may face under the proposed rule. A firm may find itself in the higher-cost category based on either greater size and complexity or a lower level of technological maturity. For this analysis, it is assumed that even firms in the low-cost scenario will have added costs in each category. Furthermore, based on the Department's experience, half of the added one-time remediation costs in both the high and low estimates are assumed to recur annually. Finally, for the added training costs, the low estimate was taken from the small business low-cost figure in a report by the Center for internet Security, and the high estimate was taken from the mid-sized business high-cost figure in the same report.⁵³⁴

TABLE VII–12—COSTS OF COMPLYING WITH THE PROPOSED SECURITY REQUIREMENTS

Category	Cost—Low	Cost—High	Type
Initial Assessment	\$25,000	\$130,000	One-time.
Remediation	35,000	115,000	One-time.
Ongoing Remediation	17,500	57,500	Annually recurring.
Compliance Audits	6,000	40,000	Annually recurring.
Training	120	3,660	Annually recurring.

c. Costs Associated With Compliance Program: Due Diligence, Recordkeeping, and Auditing

In addition to security requirements, the proposed rule also introduces affirmative due diligence,

recordkeeping, affirmative reporting, and auditing requirements as conditions of a license or for U.S. persons engaged in restricted transactions, each of which would likely impose added costs. In this section, the Department estimates costs

for affirmative due diligence, recordkeeping, and auditing for firms engaged in licensed or restricted transactions.

The compliance program for affirmative due diligence,

⁵²⁵ *Estimated Costs Associated with NIST 800–53 and NIST 800–171 Security Risk Assessments*, GoldSky Security (Apr. 29, 2021), <https://www.goldskysecurity.com/estimated-costs-associated-with-nist-800-53-and-nist-800-171-security-risk-assessments/> [https://perma.cc/87V6-FZ4N].

⁵²⁶ *CMMC Certification Cost: The Price of Compliance*, Cuick Trac, <https://www.cuicktrac.com/blog/cmmc-certification-cost/> [https://perma.cc/KR79-AWLA].

⁵²⁷ *How Much Does ISO 27001 Certification Cost?*, OneTrust: Blog (Sept. 21, 2022), <https://www.onetrust.com/blog/iso-27001-certification/> [https://perma.cc/G5UU-P62E].

⁵²⁸ *Cost of Compliance with CMMC and NIST–171*, Hyper Vigilance, <https://blog.hypervigilance.com/cost-of-cmmc-nist-compliance> [https://perma.cc/PF8Z-QVTM].

⁵²⁹ *Navigate NIST 800–171 with Confidence*, Fortified Services, <https://nist171.fortifiedservices.com/> [https://perma.cc/K92U-UGAY]; *Cost of Compliance with CMMC and NIST–171*, supra note 528.

⁵³⁰ *Cost of Compliance with CMMC and NIST–171*, supra note 528.

⁵³¹ *How Much Does ISO 27001 Certification Cost?*, supra note 527.

⁵³² *Navigate NIST 800–171 with Confidence*, supra note 529.

⁵³³ Srividhya Karthik, *ISO 27001 Certification Cost: Plan Your Compliance Budget Better*, Sprinto (Mar. 1, 2024), <https://sprinto.com/blog/iso-27001-certification-cost/> [https://perma.cc/YP75-YW6G].

⁵³⁴ Ctr. for internet Sec., supra note 524, at 22.

recordkeeping, and auditing would consist partly of risk-based procedures for verifying the data flows involved in any restricted transaction. Further requirements would include a policy describing the compliance program and process, a policy describing the implementation of any applicable security requirements or other conditions, annual certification of such compliance policies, maintenance records documenting the due diligence performed in implementing the compliance policy with respect to data transactions, and an annual certification of the completeness and accuracy of the records documenting due diligence as supported by an audit.

With regard to due diligence, recordkeeping, and auditing costs for U.S. companies, precise numbers on the number of affected firms, their sizes, and per-company or per-transaction costs are very difficult to estimate. Further, the compliance costs for firms that have established programs relative to existing Federal and State regulations may be minimal, as their compliance approach can be modified at low or no cost to address the proposed security requirements, whereas firms without such compliance programs would likely incur higher costs.

In particular, many firms may have existing compliance programs targeted at three notable provisions that were passed and implemented in recent years: the California Consumer Privacy Act of 2018 (“CCPA”)⁵³⁵ the EU’s General Data Protection Regulation (“GDPR”),⁵³⁶ and the APEC CBPR.⁵³⁷ More than 10 other U.S. States have also recently passed data privacy legislation, and many others are considering such laws.⁵³⁸ Due to these laws and existing Federal export-related regulations, it is possible that some expected due diligence costs imposed by the proposed rule may have already been incurred by affected businesses. However, given that

the definitions under the proposed rule do not fully align with the definitions used in these frameworks, there are likely to be separate due diligence costs.

The Department has estimated upper- and lower-bound costs to firms from the proposed rule related to due diligence, recordkeeping, and auditing based on our analysis of the literature regarding the CCPA, GDPR, and other data privacy rules and related research. These upper- and lower-bound estimates and the supporting literature are discussed in this part VII.A.8.c of this preamble. In summary, part VII.A.8.c.i of this preamble estimates that Know Your Customer/Know Your Vendor (“KYC”/“KYV”) costs for verifying one’s business and its executives are between \$150 (lower bound) and \$4,230 (upper bound). In addition, parts VII.A.8.c.ii through VII.A.8.c.iv of this preamble estimate that the combined annual recordkeeping and auditing costs per firm are between a lower bound of \$1,260 (\$300 for auditing + \$960 for recordkeeping) and an upper bound of \$232,500 (\$7,500 for auditing + \$225,000 for recordkeeping). These estimates are based on the Department’s analysis, but could be different depending on industry and context. The Department welcomes additional input from stakeholders on this point.

i. Due Diligence Costs

The proposed rule requires entities engaged in restricted transactions to perform due diligence that includes KYC/KYV activities, which may involve verifications to confirm the legitimacy and eligibility of customers and vendors. Costs would generally be incurred one time per customer or vendor, but they could be repetitive if there is reason to believe that a customer or vendor’s legitimacy or eligibility has changed. The Department estimates the due diligence (*i.e.*, KYC/KYV) costs for verifying one business

and its executives at between \$150 (lower bound) and \$4,230 (upper bound).

The upper-bound estimate assumes that the background check costs for one customer or vendor business would include a background check for the business and three background checks for executives residing outside the United States. The Department estimates an upper-bound cost of \$1,200 per business background check based on a study showing an upper-bound range of more than \$1,000 for a due diligence background check of a business.⁵³⁹ The Department estimates an upper-bound cost of \$1,010 per executive background check based on the highest cost for a background check of an executive residing in a country of concern (which is associated with Venezuela) from Table VII–13 of this preamble.⁵⁴⁰ Therefore, the upper-bound background check costs for one customer business with three executives could be as high as \$4,230 (\$1,200 per business⁵⁴¹ + (\$1,010 per executive⁵⁴² * 3)).

One company, Global Background Screening, charges \$150 to \$250 for business background checks, with the higher end for businesses headquartered outside the United States.⁵⁴³ These business background checks include documentation on directorship, financials, registration, judgments, liens, bankruptcies, and credit risk.⁵⁴⁴ Screenings for firm executives appear to be separate costs, which vary by country of residence and type of background check, as summarized in Table VII–13 of this preamble. Countries identified in the proposed rule as countries of concern (*see* § 202.209) are included in Table VII–13 of this preamble where sufficient data is available. Santoni also advertises due diligence business background checks, which appear to include foreign firms and officers, ranging from \$395 to more than \$1,000.⁵⁴⁵

⁵³⁵ California Consumer Privacy Act of 2018, *supra* note 28.

⁵³⁶ Regulation (EU) 2016/679, *supra* note 28.

⁵³⁷ Asia-Pac. Econ. Coop., APEC Cross-Border Privacy Enforcement Arrangement (CPEA) (Feb. 2024), <https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group/cross-border-privacy-enforcement-arrangement#> [<https://perma.cc/GRA3-8UQX>].

⁵³⁸ US State Privacy Legislation Tracker, Int’l Ass’n of Privacy Pros. (July 22, 2024), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [<https://perma.cc/WF3A-PJ5K>].

⁵³⁹ Tim Santoni, *So What’s the Difference Between Background Checks and Investigations?*, Santoni, [https://santoniservices.com/whats-new-at-santoni/whats-the-difference-between-background-](https://santoniservices.com/whats-new-at-santoni/whats-the-difference-between-background-checks-and-investigations/)

[checks-and-investigations/](https://perma.cc/WM9X-5YMY) [<https://perma.cc/WM9X-5YMY>].

⁵⁴⁰ International Screening Checkout Portal, Global Background Screening, <https://www.globalbackgroundscreening.com/online-background-check/International-Employee-Screening-Select-Country-For-Pricing-p303546142> [<https://perma.cc/3AUN-84R4>] (select most expensive options for all Venezuelan searches and verifications from dropdowns).

⁵⁴¹ Santoni, *supra* note 539 (estimating that a due diligence background check for a business may cost over \$1,000).

⁵⁴² International Screening Checkout Portal, *supra* note 540.

⁵⁴³ Background Check on a Business, Global Background Screening, [https://www.globalbackgroundscreening.com/online-](https://www.globalbackgroundscreening.com/online-background-check/background-check-on-a-business-p316742635)

[background-check/background-check-on-a-business-p316742635](https://perma.cc/3AUN-84R4) [<https://perma.cc/3AUN-84R4>].

⁵⁴⁴ Carlos Crameri, *Business Credit Reports for Informed Decision-Making*, Global Background Screening (Mar. 21, 2023), <https://www.globalbackgroundscreening.com/online-background-check/BACKGROUND-CHECK-ON-A-BUSINESS-p316742635> [<https://perma.cc/QE6U-FFMR>]; for more detailed pricing, *see* *Background Check on a Business*, Global Background Screening, <https://www.globalbackgroundscreening.com/online-background-check/background-check-on-a-business-p316742635> [<https://perma.cc/3AUN-84R4>].

⁵⁴⁵ Santoni, *supra* note 539.

TABLE VII-13—ESTIMATED INTERNATIONAL SCREENING COSTS FOR INDIVIDUALS BY COUNTRY OF RESIDENCE

Type of screening	China	Russia	Cuba	Venezuela	All nations low	All nations high
Criminal background	\$80–\$110	\$129	\$169	\$135	\$59	\$260
Civil judgements	80	145	239	159	45	279
Identity verification	25	25	25	25	25	25
Bankruptcy records	50			188	23	188
Credit history	80	127	274	234	50	532
Employment verification	35–99	35–99	35–99	35–99	35	99
Education verification	35	35	35	35	35	35
Worldscan (global databases)	11–65	11–65	11–65	11–65	11	65
Social media scan	50–70	50–70	50–70	50–70	50	70
Totals	446–614	557–695	838–976	872–1,010	333	1,553

Source: *International Screening Checkout Portal*, Global Background Screening, <https://www.globalbackgroundscreening.com/online-background-check/International-Employee-Screening-Select-Country-For-Pricing-p303546142> (reflecting costs of services at the time the Department drafted the proposed rule).

The remainder of this section summarizes additional research on background check costs for foreign firms and for individuals residing outside the United States, which is broadly consistent with the Department's upper- and lower-bound estimates discussed so far in this section.

The U.S. International Trade Administration ("ITA") provides basic background check and in-depth data on foreign firms to help U.S. companies determine the suitability of possible business partners. To be eligible for the service, companies must be export-ready and endeavoring to export goods or services of U.S. origin with at least 51-percent U.S. content. The ITA provides partial profiles that include general business information, background and product data, pertinent executives, reputation information, brief analysis of information collected, and identities of the references used. Fees for these partial profiles range from \$150 to \$450 depending on the size of the inquiring firm. Full business profiles add onsite visits and interviews of company executives, with costs ranging from \$700 to \$2,000. Costs could increase if ITA staff are required to travel more than 80 kilometers or 2 hours from an ITA office.⁵⁴⁶

Diligentia, Inc. categorizes background checks on individuals based on the thoroughness of the investigation. An individual or red flag investigation is designed to identify adverse issues predominantly via online searches, at a cost of \$500 to \$1,500. A professional background investigation is a more thorough review that adds onsite records depository visits and analysis of documents there, at a cost of \$1,500 to \$2,500. A comprehensive background

investigation goes even further, with additional analyses, reviews of business interests, the use of other intelligence sources, financial investigation, and a credit history, at a cost of more than \$2,500. This provider does not advertise a price difference between domestic and foreign background investigations.⁵⁴⁷

Checkr states that international background checks can range from \$30 to \$500, with their fees varying from \$32 to \$300 and covering more than 200 countries. Checkr asserts that a global background check may include searches for criminal history, watchlist posting, education/employment verification, and media checks.⁵⁴⁸

An ITA partial or full profile of foreign businesses would likely be preferable for U.S. companies due to the real or perceived credibility of a government agency and the comparatively reasonable costs. Accordingly, for verifying one business and its executives, the Department relied on ITA's pricing for the estimated lower-bound cost of \$150.

The sources supporting our cost estimates do not discuss whether the costs include extensive investigations that involve foreign travel or contracting with third parties in foreign locations to

perform onsite visits, inquiries, interviews, and other in-depth activities. The Department estimates that it is unlikely that firms would allocate resources for these kinds of investigations, particularly when the ITA service is available. However, some firms may not meet the ITA's eligibility criteria for their services. Thus, it is possible that KYC/KYV activities may need to be performed via a private vendor, such as one of the vendors just described. Again, based on the analysis, the Department estimates the due diligence costs for verifying one business and its executives at between \$150 (lower bound) and \$4,230 (upper bound).

These estimates are based on Department analysis but could be different depending on the industry and context. The DOJ welcomes additional input from stakeholders on this point.

ii. Recordkeeping Costs

The proposed rule's recordkeeping requirements would include generating or maintaining documents pertinent to various data transactions details, verifications of transaction partners, transactions agreements, licenses, exemptions, advisory opinions, annual due diligence certifications, and supporting documentation, as applicable. Data brokers incorporated in the United States market and sell data on individuals not only domestically but from many other countries;⁵⁴⁹ for example, Acxiom markets data coverage for more than 62 countries.⁵⁵⁰ Assuming that this data on foreign persons includes individuals protected by EU

⁵⁴⁷ Brian Willingham, *How Much Does a Background Investigation Cost?*, Diligentia Group (Apr. 23, 2024), <https://diligentiagroup.com/background-investigations/how-much-does-a-background-investigation-cost/> [<https://perma.cc/2RGF-LH5G>].

⁵⁴⁸ Simple, *Transparent Pricing: Background Check Pricing for Businesses of All Sizes*, Checkr, https://checkr.com/pricing?utm_medium=ppc&utm_source=google&utm_campaign=pricing_sitelink&utm_term=checkr&utm_campaign=FM_Brand_Search_LP_Control_1122&utm_source=google&utm_medium=ppc&utm_content=677534444565&bm=p&bn=g&device=c&utm_adgroup=Brand_Core&gad_source=1&gclid=Cj0KCQjwYL24BhCLARIsAL0fSAQPeVlJGXfAoN59kjZi4TEplchvwY7u4ZdX3iPL0SgZ0ZVLLjPwaApKyEALw_wcB [<https://perma.cc/7U3R-T8R5>].

⁵⁴⁶ Int'l Trade Admin., *International Company Profile (Full and Partial)*, <https://www.trade.gov/international-company-profile-0> [<https://perma.cc/N3PX-4DEZ>].

⁵⁴⁹ Sherman, *supra* note 483.

⁵⁵⁰ Acxiom LLC, *Global Data Navigator* (2018), <https://marketing.acxiom.com/rs/982-LRE-196/images/Acxiom%20Global%20Data.pdf> [<https://perma.cc/4NX5-M8P6>].

law, these data brokers are subject to the GDPR.

Since 2018, the GDPR has required all organizations that target or collect data relative to persons in the EU to abide by privacy and security standards outlined in that law. One of the seven data protection principles in the GDPR is accountability or due diligence. Accordingly, data controllers (*i.e.*, holders of data) must be able to demonstrate compliance relative to accountability by (1) designating data protection responsibilities as appropriate; (2) maintaining comprehensive records of collected data, its use, and those responsible for it; (3) training staff and executing technical and organizational security measures; (4) implementing contracts with third parties that process data on their behalf; and (5) appointing a data protection officer (if a public authority or regularly processing personal data on a large scale).⁵⁵¹ Thus, a portion of covered persons subject to the proposed rule are already complying with GDPR recordkeeping requirements and would arguably not incur the full magnitude of these new costs.

iii. Executive Order on Modernizing Regulatory Review Recordkeeping and Related Costs

As shown in the following analysis, the annual recordkeeping and related costs per firm are estimated to be between \$960 (lower bound) and \$225,000 (upper bound).

The Department calculates a lower-bound estimate of annual recordkeeping costs per firm by starting with the average annual incremental compliance costs/administrative burdens from the EU impact assessment of GDPR. According to the EU's impact assessment of the GDPR, average annual incremental compliance costs/administrative burdens for small and medium-sized enterprises ("SMEs")⁵⁵² are approximately \$9,624 (in 2024 dollars).⁵⁵³ The Department assumes

that the incremental recordkeeping costs of the proposed rule would only be about 10 percent of the estimated incremental annual costs for GDPR compliance. This assumption is based on the facts that the GDPR includes extensive recordkeeping requirements⁵⁵⁴ and that many of the proposed rule's recordkeeping requirements are similar in scope to the obligations of existing data protection regulations.⁵⁵⁵ Furthermore, the EU's impact assessment of the GDPR includes costs of compliance beyond recordkeeping costs. Based on these considerations and input from SMEs, the Department estimates that 1,400 small to medium-sized firms will incur recordkeeping costs of \$960 per firm per year.

An upper-bound estimate of annual recordkeeping costs per firm is also based on estimates of company privacy protection annual costs, which for large firms were estimated at \$4.5 million per firm.⁵⁵⁶ The Department further estimates that the incremental recordkeeping costs of the proposed rule for large firms would be approximately 5 percent of the estimated annual costs for privacy protections. This assumption is based on the same factors as those described for the lower-bound annual recordkeeping cost estimate as well as the fact that the prior study included additional necessary costs (*e.g.*, IT upgrades) beyond recordkeeping alone. Further, the Department believes that larger firms predominantly have the added benefit of possessing additional sophistication in complying with existing data privacy and security regimes and already have significant compliance programs and mechanisms in place. Thus, based on this analysis and subject-matter expert input, the Department estimates that 100 firms will incur the higher recordkeeping costs of \$225,000 per firm.

To provide context on these upper- and lower-bound recordkeeping costs, this section summarizes additional studies.

The CCPA mandated that businesses in California update privacy policies, develop mechanisms for providing notice to consumers when collecting personal information ("PI"), and adequately respond to consumer wishes regarding the handling of such data. The State of California Department of Justice, Office of the Attorney General's ("CDOJAG") standardized regulatory impact assessment for the CCPA regulations estimated the following rule-imposed costs per firm: \$959 in one-time operational costs (*e.g.*, establishing workflows/plans), \$7,500 for technological systems development (assumed one-time), \$615 per year for training, \$984 per year to abide by record-keeping requirements (one data privacy professional at \$61.50 per hour * 16 hours),⁵⁵⁷ and \$492 (assumed per year) to provide financial incentives or differential services/prices to promote non-discriminatory practices in their treatment of consumers exercising their CCPA rights. Apart from the \$984 in compliance-related costs, the CDOJAG assumed that there were no incremental costs for collecting the information subject to the CCPA's recordkeeping requirement, as affected businesses likely already had mature mechanisms for identifying, processing, and analyzing PI from their data-mapping and consumer response practices. The CDOJAG's total estimated costs per firm to comply with the CCPA were about \$29,000 (\$2,900 annually) for the period from 2020 to 2030.⁵⁵⁸

Christensen et al. estimated GDPR compliance costs at between \$5,065 and \$12,157 (2024 dollars)⁵⁵⁹ per year per SME, which represents a 16- to 40-percent increase in annual IT budgets. These presumably would align with the aforementioned GDPR accountability

⁵⁵¹ Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR.eu, <https://gdpr.eu/what-is-gdpr/> [<https://perma.cc/ECS2-P67N>].

⁵⁵² According to the European Commission, SMEs consist of the following company types: medium with <250 employees, ≤€50 million turnover, or a balance sheet total ≤€43 million; small with <50 employees, ≤€10 million turnover, or a balance sheet total ≤€10 million; and micro with <10 employees, ≤€2 million turnover, or a balance sheet total ≤€2 million. See European Comm'n, *SME definition*, Internal Market, Industry, Entrepreneurship and SMEs, https://single-market-economy.ec.europa.eu/smes/sme-definition_en [<https://perma.cc/N4UX-WV5V>].

⁵⁵³ €5.258 billion/926,272 active cross-border firms = €5,676 per SME per year = \$7,068 at July 2012 average exchange rate (€1.00 = \$1.24). European Comm'n, Doc. 52012SC0072, *Commission*

Staff Working Paper Impact Assessment, Annex 9 (Jan. 25, 2012), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012SC0072&qid=1713360200812> [<https://perma.cc/W3FZ-GQ9Z>].

⁵⁵⁴ Regulation (EU) 2016/679, *supra* note 28, at art. 30.

⁵⁵⁵ *Id.*; see *infra* note 557 and accompanying text.

⁵⁵⁶ This cost figure was converted into 2024 dollars. Cisco, *Data Privacy Benchmark Study, Forged by the Pandemic: The Age of Privacy* 9 (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2021.pdf [<https://perma.cc/6UTB-48C3>]. Note that large firms were assumed to be the complement of the aforementioned small to medium-sized firms.

⁵⁵⁷ Off. of Att'y Gen., Cal. Dep't of Just, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* 24 (2019), https://doj.ca.gov/wp-content/uploads/sites/352/Forecasting/Economics/Documents/CCPA_Regulations-SRIA-DOF.pdf [<https://perma.cc/5J5S-7DNA>]. The record-keeping requirements contained in the CCPA consist mainly of documenting business practices when processing consumer requests on how their particular data is handled. Businesses are required to compile metrics on these requests and their responses. These metrics include the number of requests to know, delete, and opt out that were received, complied with, and denied.

⁵⁵⁸ *Id.* Ten-year costs per firm: \$959 + \$7,500 + \$6,150 + \$9,840 (\$61.50 × 16 hrs. × 10 yrs.) + \$4,920 = \$29,369 for 10 years (*Id.*, at 24–28).

⁵⁵⁹ €3,000 (\$3,720 in 2012 dollars) to €7,200 (\$8,929 in 2012 dollars) per SME per year; Laurits R. Christensen et al., *The Impact of the Data Protection Regulation in the E.U.* (Feb. 13, 2013), https://www.analysisgroup.com/globalassets/insights/publishing/2013_data_protection_reg_in_eu_christensen_rafer_et_al.pdf [<https://perma.cc/4K3B-DF2R>].

elements identified by Wolford,⁵⁶⁰ which are generally consistent with those of the proposed rule.

A 2018 International Association of Privacy Professionals and Ernst & Young (“IAPP”/“EY”) study/survey identified much higher average expected spending of about \$3 million per firm on GDPR compliance, or \$300,000 annually if assumed over 10 years. This included \$1,276,000 already spent, another \$822,000 expected for adaptation of products and services, and \$989,000 for other adaptation activities. However, the average annual costs per firm due to GDPR were unclear based on the IAPP/EY 2018 and 2019 surveys. Company annual mean and median privacy-related spending ranged from \$128 to \$147 on a per-employee basis. Survey respondents were a mix of company sizes ranging from under 100 employees to more than 75,000.⁵⁶¹

A 2021 Cisco annual global survey of all major industries found that annual privacy budgets doubled from the previous year to an average of \$2.4 million (with smaller firms at a lower end of \$1.6 million and larger firms at an upper end of \$3.7 million, as reported in 2020).⁵⁶² This average figure of \$2.4 million is comparable to a high-end estimate found in another study that aimed to project the costs to businesses incurred by possible Florida consumer privacy legislation; that study had a lower-bound estimate of about \$733,000 in one-time costs per firm and subsequent ongoing annual costs ranging from about \$542,000 to \$1.5 million.⁵⁶³ Organizations may spend an average of about \$1,406 per subject rights request by consumers pursuant to privacy regulations.⁵⁶⁴ According to one estimate, data processing agreements may have an average cost of \$785.⁵⁶⁵

Though privacy budgets, including some of their underlying elements, are different in scope and detail from the proposed rule they nonetheless have relevance for estimating the costs of the proposed rule as these budgets often serve similar objectives and require companies to undertake similar processes to protect sensitive data.

The relatively new APEC CBPR is a voluntary accountability framework regulating data transfers between member nations that is somewhat similar to the EU’s GDPR, but based on Organisation for Economic Co-operation and Development (“OECD”) privacy principles.⁵⁶⁶ In the United States, APEC CBPR annual certification costs range from \$15,000 to \$40,000.⁵⁶⁷ The APEC CBPR’s data security⁵⁶⁸ due diligence mechanism is another requirement with which firms may already be complying and thus could reduce incremental costs of the proposed rule due to comparable or related requirements.

In summary, available sources show variations regarding the compliance costs for data privacy and cybersecurity regulations specific to recordkeeping. The Department estimates that it is very likely that incremental recordkeeping costs for at least some firms impacted by the proposed rule are zero, as the CDOJAG discussed in its cost estimates for the CCPA. Conversely, the possibility exists that larger firms have not been subject to the EU’s GDPR and would be impacted by the proposed rule, resulting in their incurring some portion of the \$4.5 million in 2024 in estimated annual recordkeeping costs documented by Cisco for such firms.⁵⁶⁹ These ranges, along with the other data and analysis discussed throughout this subpart, were taken into consideration for the calculations of the proposed rule’s average annual lower- and upper-bound costs per firm of \$960 and \$225,000. Part VII.F of this preamble estimates that costs due to the proposed annual reporting requirements for certain categories of U.S. persons

engaged in certain subsets of restricted transactions would range from \$821,100 (lower bound) to \$1,642,200 (upper bound).

iv. Auditing Costs

As shown in the following analysis, annual auditing costs per firm are estimated to be between \$300 (lower bound) and \$7,500 (upper bound).

Auditing costs for restricted transactions would be incurred in the form of independent examinations to support the due diligence certifications. TrustNet offers services to help firms determine their compliance with the CCPA. One such service is a CCPA gap assessment, which covers scope, project management, risk assessment, controls identification, testing/analysis, remediation roadmap, and reporting. The cost of this service starts at \$10,000. TrustNet also offers a CCPA compliance assessment with costs starting at \$15,000, which covers similar elements.⁵⁷⁰

According to Neumetric, a cybersecurity products and services company, GDPR accreditation or certification is not offered by the EU or any of its member states. Firms do not need to certify that they are GDPR compliant; however, there are third-party certification bodies/consultants that offer GDPR certification services for consultant fees ranging from \$3,000 to \$11,000, on average.⁵⁷¹ This does not include internal costs to prepare for certification or other prerequisites for obtaining ISO/IEC 27001 and ISO 27701 certification, which could cost between \$1,000 and \$4,000.⁵⁷² Another source estimated that costs for GDPR certification range from about \$5,000 to \$20,000 or more (excluding ISO/IEC 27001 and ISO 27701 certification).⁵⁷³

The American Institute of Certified Public Accountants has developed a cybersecurity compliance framework known as Service Organization Control 2 (“SOC 2”). Cybersecurity audit costs can be divided into SOC 2 Type 1 audits and SOC 2 Type 2 audits. Type 1 audits evaluate the suitability of controls at a specific point in time and can cost between \$5,000 and \$25,000. Type 2 audits gauge the effectiveness of controls over a more extended

⁵⁶⁰ Wolford, *supra* note 551.

⁵⁶¹ Int’l Ass’n of Privacy Pros. & Ernst & Young, *IAPP-EY Annual Privacy Governance Report 2018* (2018), https://iapp.org/media/pdf/resource_center/IAPP_EY_Governance_Report_2018.pdf [<https://perma.cc/SA8P-QV3G>]; Int’l Ass’n of Privacy Pros. & Ernst & Young, *IAPP-EY Annual Privacy Governance Report 2019* (2019), https://iapp.org/media/pdf/resource_center/IAPP_EY_Governance_Report_2019.pdf [<https://perma.cc/DG8X-3W5G>].

⁵⁶² Cisco, *supra* note 556.

⁵⁶³ Florida TaxWatch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida*, TaxWatch Research Blog (Oct. 11, 2021), <https://floridatxwatch.org/Research/Blog/who-knows-what-analysis-of-data-privacy-legislation-in-florida> [<https://perma.cc/2TD9-RLBR>].

⁵⁶⁴ Rob van der Meulen, *4 Key Trends in the Gartner Hype Cycle for Legal and Compliance Technologies, 2020*, Gartner (Sept. 21, 2020), <https://www.gartner.com/smarterwithgartner/4-key-trends-in-the-gartner-hype-cycle-for-legal-and-compliance-technologies-2020> [<https://perma.cc/2AN5-PDTJ>].

⁵⁶⁵ *Data Processing Agreement Cost*, ContractsCounsel, <https://www.contracts-counsel.com/b/data-processing-agreement-cost> [<https://perma.cc/PDW6-LFZN>].

⁵⁶⁶ Clare Sullivan, *EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era*, 35 *Comput. L. & Sec. Rev.* 380 (2019), <https://doi.org/10.1016/j.clsr.2019.05.004> [<https://perma.cc/EGH9-D7ER>].

⁵⁶⁷ ISO 27701 vs. APEC CBPR, nccgroup (July 20, 2023), <https://www.nccgroup.com/us/iso-27701-vs-apec-cbpr/> [<https://perma.cc/8VWV-FYMB>].

⁵⁶⁸ Asia-Pac. Econ. Coop., *APEC Privacy Framework* ¶ 32 (2015), [https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-\(2015\)/217_ECSCG_2015-APEC-Privacy-Framework.pdf](https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSCG_2015-APEC-Privacy-Framework.pdf) [<https://perma.cc/C8RN-V2ND>].

⁵⁶⁹ Cisco, *supra* note 556, at 9.

⁵⁷⁰ *CCPA Assessment Cost*, TrustNet, <https://trustnetinc.com/california-consumer-privacy-act-cost/> [<https://perma.cc/V88J-WW5M>].

⁵⁷¹ *GDPR Certification Cost: Factors, Examples and Benefits*, Neumetric (May 15, 2023), <https://www.neumetric.com/gdpr-certification-cost/> [<https://perma.cc/X8ZM-HW32>].

⁵⁷² *Id.*

⁵⁷³ Ayush Saxena, *Compliance Q&A: How Much Does GDPR Compliance Cost?*, Sprinto (Apr. 3, 2024), <https://sprinto.com/blog/gdpr-compliance-cost/> [<https://perma.cc/NA35-YAQP>].

timeframe and can range in costs from \$30,000 to \$100,000.⁵⁷⁴ The latter is more appropriate for firms processing highly sensitive personal data on a regular basis.⁵⁷⁵ “Dunkelberger provides a slightly different range for SOC 2 Type 1 audits, estimating that they can cost \$15,000 to \$50,000 for small to medium-sized businesses and between \$50,000 to \$100,000 for large businesses; and for SOC 2 Type 2 Audits, estimating that they can cost \$30,000 to \$75,000 for small to medium-sized businesses and \$75,000 to \$150,000 for large businesses. These costs include the price of a readiness assessment, audit, remediation, and consultant fees.⁵⁷⁶

As these estimates show, the costs of annual audits for compliance with CCPA, GDPR, and SOC 2 range from \$3,000 to \$150,000, depending on audit type and firm size. The Department expects that such examiners may not always charge these full rates separately just to certify compliance with the proposed rule, due to redundancies with existing legislation and efficiencies of conducting simultaneous audits pursuant to multiple rules. Nevertheless, there would be increased costs, as there are likely to be variations in addition to the redundancies. For purposes of this analysis, the Department assumes that for all small firms, the proposed rule would result in audit costs that are 10 percent of the estimated cost of an audit from the reviewed literature, or \$300 (\$3,000 * 10 percent incremental cost). The Department assumes that for all large firms, the proposed rule would result in audit costs that are 5 percent of the estimated cost of an audit from the reviewed literature, or \$7,500 (\$150,000 * 5 percent incremental cost).

v. Estimated Recordkeeping Costs From the Reviewed Literature

The wide-ranging estimates of recordkeeping costs in the studies reviewed, and the entwinement of the former with other costs, demonstrate the difficulty in determining specific costs for each due to the proposed rule. Further, the literature is not specific to compliance with this proposed rule. Rather, the literature relates to the business costs of protecting personal

information from unauthorized dissemination while establishing procedures for its processing and transfer, in addition to protocols for responding to consumer preferences regarding handling of their own personal information. In recent years, privacy and protection laws affecting the entities that will likely be impacted by the proposed rule have proliferated. Thus, the recordkeeping costs contemplated under the proposed rule have already been incurred to some extent.

vi. Summary of a Compliance Program: Due Diligence, Recordkeeping, and Auditing

From this examination of the available literature, the due diligence, recordkeeping, and auditing requirements are likely to unevenly impact firms that must comply with the proposed rule, depending on the size of each firm and how much it currently spends on the components of due diligence. Although the means by which firms will comply is uncertain, the Department has relied on a variety of research in the topic areas to make preliminary estimates of costs due to the proposed rule.

Uncertainty is prevalent in these restricted transactions and data-brokerage market cost estimates for several reasons. In particular, the estimates of recordkeeping costs based on the percentage of the costs of compliance with GDPR and other data protection regimes reported in various studies are highly speculative. Estimates of the proposed rule-imposed incremental costs above and beyond similar compliance activities already taking place are also speculative. Consequently, the Department welcomes comments on these cost calculations from affected industries and stakeholders to better inform decision making relative to the proposed rule.

Beyond the cost impacts of the proposed regulation, there could possibly be adjustments and market movements in reaction to changes in the threshold levels that are being proposed. This analysis assumes that all the current bulk U.S. sensitive personal data transactions are above the lower threshold levels as defined by the proposed rule. If the threshold levels are set at the higher level in the final rule, it is possible that there may be less immediate market disruption but also a greater risk of more data falling into malicious hands, including through evasion techniques such as structuring and smurfing (*i.e.*, conducting smaller and more frequent transactions using

additional individuals). Since there is no available data on the number of transactions by volume of personal data being transferred, the impacts of selecting one bulk threshold over another within the ranges in the NPRM are uncertain at the time of the proposal, and the Department welcomes comments on this subject.

Note that the recordkeeping costs discussed here (part VII.A of this preamble) are also included in part VII.F of this preamble (Paperwork Reduction Act), which presents cost estimates for the six new information collection requests introduced by the proposed rule. The costs of affirmative annual reporting are also discussed above. In addition to recordkeeping costs and the cost of affirmative annual reporting, part VII.F of this preamble presents estimates for the applications for specific licenses, reports of rejected prohibited transactions, requests for advisory opinions, petitions for removal from the Covered Persons List, and reports of known or suspected violations of onward transfers prohibition. All of those information collections affect a relatively small number of firms. Additional detail on those annual costs is available in the Information Collection Request submitted for Office of Management and Budget review under the Paperwork Reduction Act and publicly available on [reginfo.gov](https://www.reginfo.gov).

9. Summary of Regulatory Analysis

Regulatory analysis in the areas of national security and foreign policy is often not easily quantifiable or monetizable due to an array of factors, such as inadequate information, inaccessibility of sensitive or proprietary data; and the absence of a good measure of the effectiveness of the regulations.

The purpose of the Preliminary RIA is to gather and analyze enough adequate information to inform agency decision makers about whether a proposed rulemaking is in the public's interest. The analysis should describe the impacts on firms in the market and in the supply chain, remembering that the intermediate firms in the chain are customers of the suppliers. To the extent possible, the impacts on the general public should be considered, as well as—in the case of this proposed rulemaking—the impact on national security and foreign policy and the impact of data-brokerage restrictions on the positive uses of bulk data. The precision of estimates depends on the availability of data, the confidence in the accuracy of the data, and the degree of understanding of the impacted markets.

⁵⁷⁴ Tim Mektrakarn, *How Much Does a SOC2 Audit Cost in 2024?*, Bright Defense (Aug. 7, 2024), <https://www.brightdefense.com/resources/soc-2-audit-costs/> [<https://perma.cc/G7FD-28Y6>].

⁵⁷⁵ Meeba Gracy, *SOC 2 Type 1 vs Type 2 (A Detailed Comparison)*, Sprinto (Mar. 16, 2024), <https://sprinto.com/blog/soc-2-type-1-vs-type-2/> [<https://perma.cc/BZL4-GJY4>].

⁵⁷⁶ David Dunkelberger, *SOC 2 Budgeting: How Much Does a SOC 2 Audit Cost?*, I.S. Partners: Blog (Nov. 6, 2023), <https://www.ispartnersllc.com/blog/soc-2-audit-cost/> [<https://perma.cc/KCJ8-SMNA>].

These economic impact estimates lack precision due to significant gaps in the available data on the number of firms and data transactions that would be affected by the proposed rule and by the lack of confidence in much of the available data. Due to relatively recent and emerging developments in studying the market for data, relevant, reliable, and representative size, sales, employment, and other descriptive information on the data-brokerage market and other entities that will be subject to the proposed rule does not appear to be currently available. The Department is not aware of reliable data on the exact number of firms that currently engage in prohibited data-brokerage transactions, the size distribution of these firms, or the numbers of firms that sell above or below the threshold levels that would bring them under the proposed rule's umbrella. The Department welcomes additional input on this point. The low and high threshold levels for the different categories of sensitive personal data or government-related data vary by factors of 10 to 1 for human genomic data and 1,000 to 1 for personal health data and personal financial data. Furthermore, the Department lacks data on the broader universe of firms that

transact in government-related data or bulk U.S. sensitive personal data in the context of restricted transactions. As noted in the NPRM, firms that transact in bulk U.S. sensitive personal data above the proposed thresholds, as laid out in part V.C of this preamble, will need to ensure that their typical data transfers are not in fact going to countries of concern or covered persons (for prohibited transactions) and to comply with the security and due diligence requirements for restricted transactions.

This analysis leverages the limited available data on the number of data-brokerage firms and the volume of data-brokerage exports, along with estimates of security and due diligence costs from studies of similar policies and guidelines. The Department finds that, based on certain assumptions, the proposed rule will have at least some measurable economic impacts. From Table VII–10 of this preamble, the Department estimates that the total annual value of lost transactions is \$361 million, or an estimated \$80,222 per firm for 4,500 firms (3,000 data brokers + 1,500 firms engaged in restricted transactions).

Table VII–14 of this preamble presents estimates of security compliance costs derived from data

shown in part VII.B.2 of this preamble and estimates of due diligence, recordkeeping, and auditing costs derived from data shown in part VII.A.8.c of this preamble. The variations in costs are due to firm size and other factors. As explained in part VII.A.8.c of this preamble, the Department estimates the KYC/KYV (*i.e.*, due diligence) costs for verifying one business and its executives to be between a lower bound of \$150 and an upper bound of \$4,230. There is no information on how many verifications a firm will do, but the Department assumes for purposes of this analysis 10 verifications per firm per year, for a total cost of between \$1,500 and \$42,300. Adding the lower bounds of due diligence costs (\$1,500), auditing costs (\$300), and recordkeeping costs (\$960) per firm, the resulting costs at a lower bound are \$2,760 per firm for other compliance costs. Adding the upper bound of due diligence costs (\$42,300), audit costs (\$7,500), and recordkeeping costs (\$225,000) per firm, the resulting costs are \$274,800 for total compliance annual costs per large firm. Table VII–14 of this preamble shows annual compliance costs per firm. The Department welcomes additional input on this point.

TABLE VII–14—ANNUAL COMPLIANCE COSTS PER FIRM
[For Firms Engaged in Restricted Transactions]

Cost category	Low (small firms)	High (large firms)
Security: One-Time Costs	\$60,000	\$245,000
Security: Recurring Costs	23,620	101,160
Other Compliance Costs (Due Diligence, Audits, Recordkeeping)	2,760	274,800

When the proposed rule is finalized and becomes effective, market dynamics will set in, and firms will exit and enter the market as they adjust to the new regulatory environment. As noted in part VII.A.3.b of this preamble, the U.S. data-brokerage market ranges from around \$30 billion to \$180 billion per year, suggesting average revenues per firm at around \$10 million to \$60 million per year, assuming an estimated 3,000 firms. The compliance costs per firm will determine whether firms pursue restricted transactions.

For the purposes of this estimate, the Department assumes that 1,500 firms will engage in restricted transactions, the largest 100 will incur the high costs, and the remaining 1,400 will incur the lower costs. Although it is estimated that there are a relatively few U.S.-based firms conducting business with Chinese cloud-service providers that may

continue these activities under the restrictions, it is expected that a large—but unknown—number of other firms will pursue the restricted transaction opportunities involving employment and investment agreements. Under these conditions, the Department assumes that about 1,500 firms beyond the 3,000 data brokers will be active in pursuing vendor, employment, and investment agreement opportunities in the restricted transactions market, the 100 largest of which will be at the high cost and 1,400 of which will incur the lower costs.

The annualized costs of the proposed rule are determined by deriving the 10-year projections for three cost components: the economic value of lost transactions, security costs, and other compliance costs (due diligence, auditing, and recordkeeping). Our analysis assumes that 4,500 firms,

including 3,000 data brokers and 1,500 other firms engaged in restricted transactions, will incur economic costs. The analyses also assume that 4,300 of those firms are small firms (including 2,900 data brokers and 1,400 firms engaged in restricted transactions) and 200 of those firms are large firms (100 data brokers and 100 firms engaged in restricted transactions). The analysis also assumes that the data-brokerage industry affected by the proposed rule is growing at a 5-percent annual rate.

Turning to compliance costs, our analyses assume that 1,500 firms will incur compliance costs as a result of the proposed rule. The Department assumes that security costs have one-time components—initial assessment and remediation—that are only realized in the first year, as well as recurring components—ongoing remediation, compliance audits, and training—that

are present for all 10 years. In addition, it is assumed that the other compliance costs, including affirmative due diligence, auditing, and recordkeeping costs, will decline as firms become more efficient and learn to pursue lower-cost compliance options. These due diligence, auditing, and recordkeeping costs are presented as annually decreasing, but at a decreasing rate. As companies move away from reliance on employees in countries of concern or vendors in countries of concern, the Department assumes that these costs will decrease over time. Further, since the security measures are all reliant on existing NIST standards and CISA performance goals to which many companies already align their security posture, the Department assumes that due diligence, auditing, and recordkeeping costs will decrease 15 percent in the second year, 12 percent in the third year, 9 percent in the fourth year, 7 percent in the fifth year, and then 5 percent, 4 percent, 3 percent, 2 percent, and 1 percent in each of the sixth through tenth years. The costs are

presented undiscounted (0-percent rate) and at discounted by 2 percent.

In sum, the parameter assumptions of the 10-year projections are:

1. The annual growth rate of the economic value of lost transactions is 5 percent, compounded annually.
2. Due diligence, auditing, and recordkeeping costs in Year 1 are taken from Table VII–14 of this preamble. Costs in Years 2 through 10 decrease, but at a decreasing rate of 15 percent, 12 percent, 9 percent, 7 percent, 5 percent, 4 percent, 3 percent, 2 percent, and 1 percent.
3. Security costs have both one-time and recurring components in Year 1 and only recurring components in Years 2 through 10 (as shown in Table VII–14 of this preamble).
4. The analysis assumes either undiscounted costs or a 2-percent annual discount rate.
5. The value of lost transactions is from Table VII–10 of this preamble.
6. Small firms will bear “low” costs shown in the security cost and lost transaction totals, and large firms will

bear the “high” costs shown in the security cost and lost transaction totals in Tables VII–15 and VII–16 of this preamble.

7. One thousand five hundred (1,500) firms will incur compliance costs as a result of the proposed rule, and a broader group of 4,500 firms will incur costs due to lost transactions.

The 10-year annualized cost analysis (undiscounted and for a 2-percent discount rate) for security and other compliance costs (due diligence, auditing, and recordkeeping costs) is presented in Table VII–15 of this preamble for the 1,400 small firms and in Table VII–16 of this preamble for the 100 large firms. These estimates for security, due diligence, auditing, and recordkeeping costs for both small and large firms engaged in restricted transactions are combined with the industry-wide estimates for the economic value of lost transactions to obtain total costs for all firms, which are presented in Table VII–17 of this preamble.

TABLE VII–15—10-YEAR ANNUALIZED COST ANALYSIS FOR SECURITY, DUE DILIGENCE, AUDITING (AND RECORDKEEPING) FOR (THE 1,400) SMALL FIRMS
[Millions of dollars]

Cost category	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total	Annualized
Undiscounted												
Security	\$117	\$35	\$36	\$38	\$40	\$42	\$44	\$47	\$49	\$51	\$500	\$50
Due Diligence, Au- dits, and Record- keeping	4	3	3	3	3	3	3	3	3	3	33	3.3
Total	121	38	40	41	43	45	47	50	52	55	532	53
Discount Rate: 2 Percent												
Security	117	34	35	36	37	38	39	41	42	43	463	46
Due Diligence, Au- dits, and Record- keeping	4	3	3	3	3	3	3	3	3	3	30	3.0
Total	121	37	38	39	40	41	42	43	45	46	493	49

Key Assumptions: Industry growth rate of 5 percent; due diligence, auditing, and recordkeeping costs decreasing at a decreasing rate of 15–12–9–7–5–4–3–2–1 percent over years 2–10.

These year-to-year changes are the same in percentage terms for the analysis of large firms in Table VII–16 of this preamble.

TABLE VII–16—10-YEAR ANNUALIZED COST ANALYSIS FOR SECURITY AND DUE DILIGENCE (AND RECORDKEEPING) FOR (THE 100) LARGE FIRMS
[Millions of dollars]

Cost category	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total	Annualized
Undiscounted												
Security	\$35	\$11	\$11	\$12	\$12	\$13	\$14	\$14	\$15	\$16	\$152	\$15
Due Diligence, Au- dits, and Record- keeping	27	25	23	22	22	22	22	22	23	24	232	23

TABLE VII-16—10-YEAR ANNUALIZED COST ANALYSIS FOR SECURITY AND DUE DILIGENCE (AND RECORDKEEPING) FOR (THE 100) LARGE FIRMS—Continued
[Millions of dollars]

Cost category	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total	Annualized
Total	62	35	34	34	34	35	35	37	38	40	383	38
Discount Rate: 2 Percent												
Security	35	10	11	11	11	12	12	12	13	13	140	14
Due Diligence, Audits, and Recordkeeping	27	24	22	21	20	19	19	19	19	20	212	21
Total	62	35	33	32	31	31	31	32	32	33	352	35

Key Assumptions: Industry growth rate of 5 percent; due diligence, auditing, and recordkeeping costs decreasing at a decreasing rate of 15–12–9–7–5–4–3–2–1 percent over years 2–10.

The total annualized costs of the proposed rule for small and large firms are combined and presented in Table VII-17 of this preamble, estimated at \$549 million undiscounted and \$502

million discounted at 2 percent (any differences are due to rounding). Tables VII-15 and VII-16 of this preamble only include the costs of the security, due diligence, and recordkeeping

requirements of the proposed rule, while Table VII-17 of this preamble also includes the costs associated with the value of lost transactions.

TABLE VII-17—10-YEAR ANNUALIZED COST ANALYSIS FOR ALL FIRMS
[Millions of dollars]

Cost category	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total	Annualized
Undiscounted												
Lost Transactions	\$364	\$382	\$401	\$421	\$442	\$465	\$488	\$512	\$538	\$565	\$4,578	\$458
Security	152	45	48	50	52	55	58	61	64	67	652	65
Due Diligence, Audits, and Recordkeeping	31	28	26	25	25	25	25	25	26	27	264	26
Total	547	456	475	497	520	544	571	598	628	659	5,494	549
Discount Rate: 2 Percent												
Lost Transactions	364	375	22	398	410	422	435	448	461	475	4,173	417
Security	152	44	46	47	49	50	52	53	55	56	604	60
Due Diligence, Audits, and Recordkeeping	31	28	25	24	23	22	22	22	22	23	241	24
Total	547	447	93	469	481	494	508	523	538	554	5,018	502

Key Assumptions: Industry growth rate of 5 percent; due diligence, auditing, and recordkeeping costs decreasing at a decreasing rate of 15–12–9–7–5–4–3–2–1 percent over years 2–10.

Table VII-18 of this preamble summarizes the 10-year annualized cost analysis (presented in Tables VII-15, VII-16, and VII-17 of this preamble) for small and large firms separately and in total, both undiscounted and with a discount rate of 2 percent.

This cost estimate reflects the likelihood that a number of smaller firms will drop out of the market if the costs of compliance are greater than expected revenues (*i.e.*, if marginal costs exceed marginal revenues). Of course, this could also be true of larger firms that lack the infrastructure or financial resources to comply with the proposed rules and therefore choose to forgo

certain transactions or business operations in that market altogether.

In addition to the potential decrease in the number of firms in the industry, another related effect is that the proposed rule may create a barrier to entry for potential data brokers. That is, the same compliance burdens that affect marginal current brokers will also affect potential ones.

TABLE VII-18—SUMMARY OF TOTAL 10-YEAR ANNUALIZED COSTS
[Undiscounted and for a 2-Percent Discount Rate]

Discount rate	Total cost
Undiscounted	\$549,000,000
2 Percent	502,000,000

These preliminary estimated costs of the proposed rule appear to be reasonable when balanced against the expected benefits of preventing the potential risk and harms to national security and foreign policy that are possible when government-related data or bulk U.S. sensitive personal data is transferred to foreign adversaries. These

benefits are beyond monetary calculation but suggest that the proposed rule will have very large net benefits, including protections to well over 100 million American individuals who are potential targets of adversaries using government-related data or bulk U.S. sensitive personal data. A wide range of benefits of the regulation will also be realized by firms, including the savings associated with potentially reducing the likelihood of data breaches thanks to improved security, which are estimated to cost an average of \$4.88 million per breach.⁵⁷⁷ And firms that sell data to, or buy data from, brokers will have increased confidence in the security and due diligence arrangements associated with the regulation.

Both the benefits to be realized and the costs to the economy and government will be determined, to some extent, by the effectiveness of

compliance and enforcement activities and by the methods that market participants use to attempt to avoid detection of prohibited or restricted activities. For example, “back doors” are used to circumvent economic sanctions, and digital assets are used to hide sanctioned transactions themselves. The countries of concern are known to conduct commercial and military operations through proxies. As shown in parts IV.D.1.b and IV.D.1.f of this preamble, Cuba and Venezuela have acted as third parties to promote malicious acts by other countries of concern. Unless the due diligence requirements are fully complied with and the due diligence procedures and inquiries provide accurate information, the effectiveness of the proposed rule may be weakened, leading to reduced expected benefits.

One commenter suggested that the Department conduct a retrospective review of the impact after the final rule becomes effective. The Order already requires such a review. Under section 5 of the Order, within 1 year after the final rule becomes effective, the Department must submit a report to the President that addresses, to the extent practicable, the effectiveness of the measures imposed under the Order in addressing threats to the national security of the United States described in the Order and the economic impact of the implementation of the Order, including on the international competitiveness of U.S. industry. The Order requires the Department to solicit public comment in evaluating the economic impact. The Department also intends to regularly monitor the effectiveness and impact of the regulations once they become effective.

TABLE VII–19—OMB CIRCULAR A–4 ACCOUNTING STATEMENT PROVISIONS PERTAINING TO PREVENTING ACCESS TO U.S. SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS NPRM

Category	Estimate			Units			Notes
	Primary	Low	High	Dollar year	Discount rate	Time horizon	
Benefits							
Annualized monetized benefits	The benefits of the proposal include the security of the American people, economic prosperity and opportunity, and democratic values, all of which are beyond a reasonable, reliable, and acceptable estimate of quantified monetary value. Details in NPRM.						
Annualized quantified, but non-monetized, benefits.	The Department did not identify any benefits that were quantified.						
Unquantified benefits	Discussed in NPRM.						
Cost							
Annualized monetized costs	\$549,000,000				undiscounted	Years 1–10	The primary costs of the proposed rule are the lost value of transactions due to the prohibitions and costs related to the restrictions that will require due diligence expenditures for enhanced security, KYC/ KYV verifications, recordkeeping, reporting, and audits.
	\$502,000,000				2%	Years 1–10	
Annualized quantified, but non-monetized, costs.							
Unquantified costs							
Transfers							
Annualized monetized Federal budgetary transfers. From/To:							
Other annualized monetized transfers From/To:							
Effects							
Effects on State, local, or Tribal governments.	The proposed rule would not have Tribal implications warranting the application of Executive Order 13175. It would not have substantial direct effects on one or more Indian Tribes, on the relationship between the Federal Government and Indian Tribes, or on the distribution of power and responsibilities between the Federal Government and Indian Tribes.						
Effects on small businesses	This analysis assumes that the small entities affected by the proposed rule will incur compliance costs of around \$32,380 per firm annually, compared with an annual compliance cost of \$400,460 for the largest affected firms. Both cost figures are undiscounted. The Department estimates that the proposed rule will impact just over 4,000 small entities, and that the highest-cost scenario will apply to approximately 100 firms.						
Effects on wages	The Department did not estimate any impacts on wages.						

⁵⁷⁷ Cost of a Data Breach Report 2024, IBM, <https://www.ibm.com/reports/data-breach> [<https://perma.cc/8GNL-YEUX>].

TABLE VII-19—OMB CIRCULAR A-4 ACCOUNTING STATEMENT PROVISIONS PERTAINING TO PREVENTING ACCESS TO U.S. SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS NPRM—Continued

Category	Estimate			Units			Notes
	Primary	Low	High	Dollar year	Discount rate	Time horizon	
Effects on growth	The Department did not estimate any impacts on growth.						

B. Regulatory Flexibility Act

The Department is proposing this rule to address the growing threat posed by the efforts of foreign adversaries to access and exploit the government-related data or Americans' bulk U.S. sensitive personal data. On February 28, 2024, the President issued Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." This Order directs the Attorney General to, among other things, determine which classes of data transactions ought to be prohibited due to the unacceptable risk they pose by allowing countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data. The Order also directs the Attorney General to work with relevant agencies to identify countries of concern and classes of covered persons, establish a process to issue licenses authorizing transactions that would otherwise be prohibited or restricted transactions, address the need for requirements for recordkeeping and reporting transactions, and determine which classes of transactions will be required to comply with separate security requirements.

The need for the proposed rule stems from the increased efforts that countries of concern are making to obtain sensitive personal data of Americans and to utilize it in a way that undermines national security and foreign policy. Advances in computing technology, artificial intelligence, and methods for processing large datasets allow countries of concern to more effectively leverage collected data for malicious purposes. The capability currently exists to allow those who government-related data or Americans' bulk U.S. sensitive personal data to combine and manipulate it in ways that could identify sensitive personal data, including personal identifiers and precise geolocation information.

1. Succinct Statement of the Objectives of, and Legal Basis for, the Proposed Rule

Through the Order, the President used his authority under IEEPA and the National Emergencies Act to declare national emergencies and regulate certain types of economic transactions in order to protect the country against foreign threats. The Order expands upon the national emergency previously declared by Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), which was modified by Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries). Furthermore, the President, under title 3, section 301 of the U.S. Code, authorized the Attorney General, in consultation with the heads of relevant executive agencies, to employ the President's powers granted by IEEPA as may be necessary or appropriate to carry out the purposes of the Order.

IEEPA empowers the President to "investigate, regulate, or prohibit" foreign exchanges in cases where there is a threat coming from outside the United States that threatens the country's "national security, foreign policy, or economy." Existing IEEPA-based programs include those administered by OFAC, which enforces economic and trade sanctions, and the Department of Commerce's Bureau of Industry and Security, which is responsible for information and communications technology and services supply chain security.

2. Description of and, Where Feasible, an Estimate of the Number of Small Entities to Which the Proposed Rule Will Apply

The proposed rule would affect data-brokerage firms and other firms engaged in covered data transactions that pose a risk of exposing government-related data or bulk U.S. sensitive personal data to countries of concern or covered persons. The Department has estimated

that about 4,500 firms, just over 90 percent of which are small businesses (hereafter referred to as "small entities"), would be impacted by the proposed rule. Therefore, the Department estimates that this proposed rule would impact approximately 4,050 small entities and approximately 450 firms that would not be classified as small entities.

Small entities, as defined by the Regulatory Flexibility Act, include small businesses, small nonprofit organizations, and small governmental jurisdictions. The definition of "small entities" includes the definition of "small businesses" pursuant to section 3 of the Small Business Act of 1953, as amended: "A small business concern . . . shall be deemed to be one which is independently owned and operated, and which is not dominant in its field of operation." The definition of "small business" varies from industry to industry (as specified by NAICS code and found in 13 CFR 121.201) to reflect the typical company size in each industry.

NAICS code 518210, "Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services," contains all the affected data brokers as well as some of the other entities engaged in one or more of the classes of restricted data transactions.⁵⁷⁸ The number of small entities affected by the proposed rule was estimated by using the Small Business Administration ("SBA") small business size standard for the NAICS code to calculate the proportion of firms that are considered small entities. Data brokers are only a subset of the total firms contained in the identified NAICS code; however, for this analysis, it was assumed that the proportion of small entities was the same for both the broader NAICS industry and the specific data broker industry. Because more than 90 percent of impacted firms across all relevant industries can be considered small entities, the proposed rule would have an impact on a substantial number of small entities.

⁵⁷⁸ 518210—Computing Infrastructure Providers, Data Processing, Web Hosting, and Related

Services, North American Industry Classification System, <https://www.naics.com/naics-code->

<description/?v=2022&code=518210> [<https://perma.cc/5PWG-AQWL>].

TABLE VII–20—SMALL BUSINESS SIZE STANDARD AND AFFECTED FIRMS

Number of affected firms	Share of affected firms that are small	Number of affected small firms
4,500	Approximately 90 percent	Approximately 4,050.

This analysis assumes that the small entities affected by the proposed rule will incur compliance costs of around \$32,380 per firm per year, compared with an annual compliance cost of \$400,460 for the largest affected firms.

The Department is not aware of reliable revenue data by firm size for the data broker industry, but a reasonable assumption is that if a firm’s revenues from data sales are not sufficient to cover the compliance costs, then that firm will have an incentive to exit that market. Furthermore, calculating the proportion of the costs associated with the proposed rule that falls on small firms is complicated by the fact that several of the proposed rule’s provisions—specifically the requirements related to cybersecurity, due diligence, recordkeeping, and reporting—likely involve high fixed costs. Even if small entities have less complex business operations, leading to fewer complications related to compliance, they may still face a higher cost burden from the proposed rule than larger firms. Large entities will likely already have a greater portion of the fixed costs associated with the proposed rule covered by existing capabilities. Therefore, while the costs associated with the security and due diligence requirements will be smaller in absolute terms for smaller entities, such entities will likely need to pay a higher proportion of their overall budgets to comply. Due to the unknowns and the large number of small entities, it is possible that a substantial number of small firms will experience a significant impact. The Department welcomes comments on this topic.

3. Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Proposed Rule

The proposed rule would require firms engaged in restricted transactions to adhere to certain standards for data security, due diligence, recordkeeping, and reporting. *See* § 202.401. To mitigate the risk of sharing government-related data or bulk U.S. sensitive personal data with countries of concern or covered persons through restricted transactions, organizations engaged in restricted transactions would be required to institute organizational and system-level cybersecurity policies, practices, and requirements and data-

level requirements developed by DHS through CISA in coordination with the Department. *See* § 202.402. Those requirements, which CISA will release through a separate Request For Information, overlap with several similar, widely used cybersecurity standards or frameworks. In addition, the security requirements developed by CISA would require firms to protect the data associated with restricted transactions using combinations of the following capabilities necessary to prevent access to covered data by covered persons or countries of concern:

1. data minimization and data masking;
2. encryption;
3. privacy-enhancing technologies; and
4. denial of access.

Firms will also be required to undergo annual independent testing and auditing to ensure their continuing compliance with the security requirements.

Additionally, in order to ensure that government-related data or Americans’ bulk U.S. sensitive personal data are not accessible by countries of concern or covered persons, firms will be required to engage in due diligence before pursuing restricted transactions, which involves utilizing KYC/KYV programs to complete background checks on potential partners. Furthermore, firms will be required to keep records that contain extensive details of their restricted transactions as well as the details of the other parties involved. They will also be required to undergo annual audits of their records to ensure compliance and assess potential risks.

4. Identification of All Relevant Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rule

As discussed in part IV.K of this preamble, while the PADFAA seeks to address some of the same national security risks of the proposed rule, there are clear differences between the PADFAA, the Order, and this proposed rule, including the scope of regulated data brokerage activities, the types of bulk sensitive personal data that are covered, and the relevant countries of concern. Further, while the PADFAA allows the FTC to investigate certain data-brokerage activities involving countries of concern as unfair trade practices consistent with the FTC’s

existing jurisdiction, the proposed rule establishes a new set of consistent regulatory requirements that apply across multiple types of commercial transactions and sectors. Finally, as stated in part IV.K of this preamble, the Department will coordinate closely with the FTC to ensure consistency in how both authorities are implemented.

Some restricted transactions under the proposed rule could also end up being subject to review and action by CFIUS. The Foreign Investment Risk Review Modernization Act of 2018 gave CFIUS the authority to review certain non-controlling foreign investments that may pose a risk to national security by allowing the sensitive personal data of U.S. citizens to be exploited.⁵⁷⁹ However, while CFIUS acts on a transaction-by-transaction basis, the proposed rule would create restrictions and prohibitions on covered data transactions that would apply to categories of data transactions involving the six countries of concern. In a situation where a covered data transaction regulated by the proposed rule was later subject to a CFIUS review, it would be exempt from the proposed rule to the extent that CFIUS takes any of the actions identified in the proposed rule. *See* §§ 202.207; 202.508.

Furthermore, the categories of covered data transactions covered by the proposed rule extend beyond the scope of CFIUS, including the provision of government-related data or bulk U.S. sensitive personal data through data brokerage, vendor agreements, and employment agreements. The proposed rule also covers investment agreements that may not be covered by CFIUS as well as cases where the relevant risks do not result from the covered transaction or may occur before a CFIUS action takes place.

C. Executive Order 13132 (Federalism)

The proposed rule would not have federalism implications warranting the application of Executive Order 13132. The proposed rule does not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.

⁵⁷⁹ *See* Foreign Investment Risk Review Modernization Act of 2018, *supra* note 11.

D. Executive Order 13175 (Consultation and Coordination With Indian Tribal Governments)

The proposed rule would not have Tribal implications warranting the application of Executive Order 13175. It does not have substantial direct effects on one or more Indian Tribes, on the relationship between the Federal Government and Indian Tribes, or on the distribution of power and responsibilities between the Federal Government and Indian Tribes.

E. Executive Order 12988 (Civil Justice Reform)

This proposed rule meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988.

F. Paperwork Reduction Act

The collections of information contained in this notice of proposed rulemaking have been submitted to the Office of Management and Budget for review in accordance with the Paperwork Reduction Act of 1995, 44 U.S.C. 3507(d), under control number 1124-AA01.

Written comments on this collection can be submitted by visiting www.reginfo.gov/public/do/PRAMain. Find this document by selecting “Currently Under Review—Open for Public Comments” or by using the search function. Comments on the collection of information should be received by November 29, 2024.

The Department of Justice is soliciting comments from members of the public concerning this collection of information to:

- Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
- Evaluate the accuracy of the agency’s estimate of the burden of the proposed collection of information;
- Enhance the quality, utility, and clarity of the information to be collected; and
- Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated collection techniques or other forms of information technology.

The proposed rule includes seven new collections of information: annual reports; applications for specific licenses; reports on rejected prohibited transactions; requests for advisory opinions; petitions for removal from the designated Covered Persons List; reports

of known or suspected violations of the onward transfers prohibition; and recordkeeping requirements for restricted transactions.

Based on wage rates from the Bureau of Labor Statistics and lower- and upper-bound estimates (used because this is a new program and there is uncertainty in the estimated number of potential respondents for each of the forms), the following are the estimated burdens of the proposed collections:

- *Annual reports.* The Department estimates that 375 to 750 filers will send an average of one annual report per year, spending an estimated average of 40 hours to prepare and submit each annual report. The Department estimates the aggregated costs for all filers at \$821,100 to \$1,642,200 annually for annual reports.

- *Applications for specific licenses.* The Department estimates that 15 to 25 filers will send an average of one application for a specific license per year, spending an estimated average of 10 hours to prepare and submit each application for a specific license. The Department estimates the aggregated costs for all filers at \$8,211 to \$13,685 annually for applications for specific licenses.

- *Reports on rejected prohibited transactions.* The Department estimates that 15 to 25 filers will send an average of one report on a rejected prohibited transaction per year, spending an estimated average of 2 hours to prepare and submit each application for a specific license. The Department estimates the aggregated costs for all filers at \$1,642 to \$2,737 annually for reports on rejected prohibited transactions.

- *Requests for advisory opinions.* The Department estimates that 50 to 100 filers will send an average of one request for an advisory opinion per year, spending an estimated average of 2 hours to prepare and submit each request for an advisory opinion. The Department estimates the aggregated costs for all filers at \$5,474 to \$10,948 annually for requests for advisory opinions.

- *Petitions for removal from covered persons list.* The Department estimates that 15 to 25 filers will send an average of one petition for removal from the Covered Persons List per year, spending an estimated average of 5 hours to prepare and submit each petition for removal from the Covered Persons List. The Department estimates the aggregated costs for all filers at \$4,106 to \$6,843 annually for petitions for removal from the Covered Persons List.

- *Reports of known or suspected violations of onward transfers*

prohibition. The Department estimates that 300 to 450 filers will send an average of one report of known or suspected violations of the onward transfers prohibition per year, spending an estimated average of 2 hours to prepare and submit each report of known or suspected violations of the onward transfers prohibition. The Department estimates the aggregated costs for all filers at \$32,844 to \$49,266 annually for reports of known or suspected violations of the onward transfers prohibition.

- *Recordkeeping requirements for restricted transactions.* The Department estimates that 1,400 small to medium-sized firms will incur a total of \$1,344,000 in recordkeeping costs per year. Also, the Department estimates that 100 large firms will incur a total of \$84,844,000 in recordkeeping costs per year.

Under the Paperwork Reduction Act, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number assigned by the Office of Management and Budget.

G. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act requires that Federal agencies prepare a written statement assessing the effects of any Federal mandate in a proposed or final agency rule that may directly result in the expenditure of \$100 million or more in 1995 dollars (adjusted annually for inflation) in any 1 year by State, local, and Tribal governments, in the aggregate, or by the private sector (2 U.S.C. 1532(a)). However, the Unfunded Mandates Reform Act does not apply to “any provision” in a proposed or final rule that is “necessary for the national security” (2 U.S.C. 1503(5)).

In the Order, the President explained that “[t]he continuing effort of certain countries of concern to access Americans’ sensitive personal data and United States Government-related data constitutes an unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security and foreign policy of the United States.” The Order expanded the scope of the national emergency declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans’ Sensitive Data From Foreign Adversaries). Section 2(a) of the Order thus requires the Attorney General to issue the regulations in this

part, subject to public notice and comment, “[t]o assist in addressing the national security emergency described” in the Order. Because the entirety of this proposed rule and every provision in it addresses the national emergency described by the President in the Order, the Department has concluded that the Unfunded Mandates Reform Act does not apply to this proposed rule.

List of Subjects in 28 CFR Part 202

Computer technology, Health records, Incorporation by reference, Investments, Military personnel, National security, Personally identifiable information, Privacy, Reporting and recordkeeping requirements, Security measures.

■ Under the rulemaking authority vested in the Attorney General in 5 U.S.C. 301; 28 U.S.C. 509, 510 and delegated to the Assistant Attorney General for National Security by A.G. Order No. 6067–2024, and for the reasons set forth in the preamble, the Department of Justice proposes to add part 202 to chapter I of title 28 of the Code of Federal Regulations to read as follows:

PART 202—ACCESS TO U.S. SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS

Sec.

Subpart A—General

- 202.101 Scope.
- 202.102 Rules of construction and interpretation.
- 202.103 Relation of this part to other laws and regulations.
- 202.104 Delegation of authorities.
- 202.105 Amendment, modification, or revocation.
- 202.106 Severability.

Subpart B—Definitions

- 202.201 Access.
- 202.202 Attorney General.
- 202.203 Assistant Attorney General.
- 202.204 Biometric identifiers.
- 202.205 Bulk.
- 202.206 Bulk U.S. sensitive personal data.
- 202.207 CFIUS action.
- 202.208 China.
- 202.209 Country of concern.
- 202.210 Covered data transaction.
- 202.211 Covered person.
- 202.212 Covered personal identifiers.
- 202.213 Cuba.
- 202.214 Data brokerage.
- 202.215 Directing.
- 202.216 Effective date.
- 202.217 Employment agreement.
- 202.218 Entity.
- 202.219 Exempt transaction.
- 202.220 Former senior official.
- 202.221 Foreign person.
- 202.222 Government-related data.
- 202.223 Human biospecimens.

- 202.224 Human genomic data.
- 202.225 IEEPA.
- 202.226 Information or informational materials.
- 202.227 Interest.
- 202.228 Investment agreement.
- 202.229 Iran.
- 202.230 Knowingly.
- 202.231 Licenses; general and specific.
- 202.232 Linked.
- 202.233 Linkable.
- 202.234 Listed identifier.
- 202.235 National Security Division.
- 202.236 North Korea.
- 202.237 Order.
- 202.238 Person.
- 202.239 Personal communications.
- 202.240 Personal financial data.
- 202.241 Personal health data.
- 202.242 Precise geolocation data.
- 202.243 Prohibited transaction.
- 202.244 Property; property interest.
- 202.245 Recent former employees or contractors.
- 202.246 Restricted transaction.
- 202.247 Russia.
- 202.248 Security requirements.
- 202.249 Sensitive personal data.
- 202.250 Special Administrative Region of Hong Kong.
- 202.251 Special Administrative Region of Macau.
- 202.252 Telecommunications service.
- 202.253 Transaction.
- 202.254 Transfer.
- 202.255 United States.
- 202.256 United States person or U.S. person.
- 202.257 U.S. device.
- 202.258 Vendor agreement.
- 202.259 Venezuela.

Subpart C—Prohibited Transactions and Related Activities

- 202.301 Prohibited data-brokerage transactions.
- 202.302 Other prohibited data-brokerage transactions involving potential onward transfer to countries of concern or covered persons.
- 202.303 Prohibited human genomic data and human biospecimen transactions.
- 202.304 Prohibited evasions, attempts, causing violations, and conspiracies.
- 202.305 Knowingly directing prohibited or restricted transactions.

Subpart D—Restricted Transactions

- 202.401 Authorization to conduct restricted transactions.
- 202.402 Incorporation by reference.

Subpart E—Exempt Transactions

- 202.501 Personal communications.
- 202.502 Information or informational materials.
- 202.503 Travel.
- 202.504 Official business of the United States Government.
- 202.505 Financial services.
- 202.506 Corporate group transactions.
- 202.507 Transactions required or authorized by Federal law or international agreements, or necessary for compliance with Federal law.
- 202.508 Investment agreements subject to a CFIUS action.

- 202.509 Telecommunications services.
- 202.510 Drug, biological product, and medical device authorizations.
- 202.511 Other clinical investigations and post-marketing surveillance data.

Subpart F—Determination of Countries of Concern

- 202.601 Determination of countries of concern.

Subpart G—Covered Persons

- 202.701 Designation of covered persons.
- 202.702 Procedures governing removal from the Covered Persons List.

Subpart H—Licensing

- 202.801 General licenses.
- 202.802 Specific licenses.
- 202.803 General provisions.

Subpart I—Advisory Opinions

- 202.901 Inquiries concerning application of this part.

Subpart J—Due Diligence and Audit Requirements

- 202.1001 Due diligence for restricted transactions.
- 202.1002 Audits for restricted transactions.

Subpart K—Reporting and Recordkeeping Requirements

- 202.1101 Records and recordkeeping requirements.
- 202.1102 Reports to be furnished on demand.
- 202.1103 Annual reports.
- 202.1104 Reports on rejected prohibited transactions.

Subpart L—Submitting Applications, Requests, Reports, and Responses

- 202.1201 Procedures.

Subpart M—Penalties and Finding of Violation

- 202.1301 Penalties for violations.
- 202.1302 Process for pre-penalty notice.
- 202.1303 Penalty imposition.
- 202.1304 Administrative collection and litigation.
- 202.1305 Finding of violation.
- 202.1306 Opportunity to respond to a pre-penalty notice or finding of violation.

Subpart N—Government-Related Location Data List

- 202.1401 Government-Related Location Data List.

Authority: 50 U.S.C. 1701 *et seq.*; 50 U.S.C. 1601 *et seq.*; E.O. 14117, 89 FR 15421.

Subpart A—General

§ 202.101 Scope.

(a) Executive Order 14117 of February 28, 2024 (Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern) (“the Order”), directs the Attorney General to issue regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer,

transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest (“transaction”), where the transaction: involves United States Government-related data (“government-related data”) or bulk U.S. sensitive personal data, as defined by final rules implementing the Order; falls within a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because the transactions may enable access by countries of concern or covered persons to government-related data or bulk U.S. sensitive personal data; and meets other criteria specified by the Order.

(b) This part contains regulations implementing the Order and addressing the national emergency declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans’ Sensitive Data from Foreign Adversaries) and Executive Order 14117.

§ 202.102 Rules of construction and interpretation.

(a) The examples included in this part are provided for informational purposes and should not be construed to alter the meaning of the text of the regulations in this part.

(b) As used in this part, the term “including” means “including but not limited to.”

(c) All references to “days” in this part mean calendar days. In computing any time period specified in this part:

(1) Exclude the day of the event that triggers the period;

(2) Count every day, including Saturdays, Sundays, and legal holidays; and

(3) Include the last day of the period, but if the last day is a Saturday, Sunday, or Federal holiday, the period continues to run until the end of the next day that is not a Saturday, Sunday, or Federal holiday.

§ 202.103 Relation of this part to other laws and regulations.

Nothing in this part shall be construed as altering or affecting any other authority, process, regulation, investigation, enforcement measure, or review provided by or established under any other provision of Federal law, including the International Emergency Economic Powers Act.

§ 202.104 Delegation of authorities.

Any action that the Attorney General is authorized to take pursuant to the Order or pursuant to this part may be taken by the Assistant Attorney General for National Security or by any other person to whom the Attorney General or Assistant Attorney General for National Security in writing delegates authority so to act.

§ 202.105 Amendment, modification, or revocation.

Except as otherwise provided by law, any determinations, prohibitions, decisions, licenses (whether general or specific), guidance, authorizations, instructions, orders, or forms issued pursuant to this part may be amended, modified, or revoked, in whole or in part, at any time.

§ 202.106 Severability.

If any provision of this part is held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, or stayed pending further agency action or judicial review, the provision is to be construed so as to continue to give the maximum effect to the provision permitted by law, unless such holding will be one of utter invalidity or unenforceability, in which event the provision will be severable from this part and will not affect the remainder thereof.

Subpart B—Definitions

§ 202.201 Access.

The term *access* means logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology systems, cloud-computing platforms, networks, security systems, equipment, or software.

§ 202.202 Attorney General.

The term *Attorney General* means the Attorney General of the United States or the Attorney General’s designee.

§ 202.203 Assistant Attorney General.

The term *Assistant Attorney General* means the Assistant Attorney General, National Security Division, United States Department of Justice, or the Assistant Attorney General’s designee.

§ 202.204 Biometric identifiers.

The term *biometric identifiers* means measurable physical characteristics or behaviors used to recognize or verify the identity of an individual, including facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints, gait, and keyboard usage

patterns that are enrolled in a biometric system and the templates created by the system.

§ 202.205 Bulk.

The term *bulk* means any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the same U.S. person and the same foreign person or covered person:

(a) Human genomic data collected about or maintained on more than 100 U.S. persons;

(b) Biometric identifiers collected about or maintained on more than 1,000 U.S. persons;

(c) Precise geolocation data collected about or maintained on more than 1,000 U.S. devices;

(d) Personal health data collected about or maintained on more than 10,000 U.S. persons;

(e) Personal financial data collected about or maintained on more than 10,000 U.S. persons;

(f) Covered personal identifiers collected about or maintained on more than 100,000 U.S. persons; or

(g) Combined data, meaning any collection or set of data that contains more than one of the categories in paragraphs (a) through (g) of this section, or that contains any listed identifier linked to categories in paragraphs (a) through (e) of this section, where any individual data type meets the threshold number of persons or devices collected or maintained in the aggregate for the lowest number of U.S. persons or U.S. devices in that category of data.

§ 202.206 Bulk U.S. sensitive personal data.

The term *bulk U.S. sensitive personal data* means a collection or set of bulk data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted.

§ 202.207 CFIUS action.

The term *CFIUS action* means any agreement or condition the Committee on Foreign Investment in the United States has entered into or imposed pursuant to 50 U.S.C. 4565(l)(1), (3), or (5) to resolve a national security risk involving access by a country of concern or covered person to sensitive personal data that the Committee on Foreign Investment in the United States has explicitly designated, in the agreement or document containing the condition, as a CFIUS action, including:

(a) Suspension of a proposed or pending transaction, as authorized under 50 U.S.C. 4565(l)(1);

(b) Entry into or imposition of any agreement or condition with any party to a covered transaction, as authorized under 50 U.S.C. 4565(l)(3); and

(c) The establishment of interim protections for covered transactions withdrawn before CFIUS's review or investigation is completed, as authorized under 50 U.S.C. 4565(l)(5).

§ 202.208 China.

The term *China* means the People's Republic of China, including the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau, as well as any political subdivision, agency, or instrumentality thereof.

§ 202.209 Country of concern.

The term *country of concern* means any foreign government that, as determined by the Attorney General with the concurrence of the Secretary of State and the Secretary of Commerce, (1) has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons, and (2) poses a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or security and safety of U.S. persons.

§ 202.210 Covered data transaction.

(a) *Definition.* A *covered data transaction* is any transaction that involves any access to any government-related data or bulk U.S. sensitive personal data and that involves:

- (1) Data brokerage;
- (2) A vendor agreement;
- (3) An employment agreement; or
- (4) An investment agreement.

(b) *Examples.* (1) *Example 1.* A U.S. institution conducts medical research at its own laboratory in a country of concern, including sending several U.S.-citizen employees to that laboratory to perform and assist with the research. The U.S. institution does not engage in data brokerage or a vendor, employment, or investment agreement that gives a covered person or country of concern access to government-related data or bulk U.S. sensitive personal data. Because the U.S. institution does not engage in any data brokerage or enter into a vendor, employment, or investment agreement, the U.S. institution's research activity is not a covered data transaction.

(2) [Reserved]

§ 202.211 Covered person.

(a) *Definition.* The term *covered person* means:

(1) A foreign person that is an entity that is 50 percent or more owned, directly or indirectly, by a country of concern, or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;

(2) A foreign person that is an entity that is 50 percent or more owned, directly or indirectly, by an entity described in paragraph (a)(1) of this section or a person described in paragraphs (a)(3), (4), or (5) of this section;

(3) A foreign person that is an individual who is an employee or contractor of a country of concern or of an entity described in paragraphs (a)(1), (2), or (5) of this section;

(4) A foreign person that is an individual who is primarily a resident in the territorial jurisdiction of a country of concern; or

(5) Any person, wherever located, determined by the Attorney General:

(i) To be, to have been, or to be likely to become owned or controlled by or subject to the jurisdiction or direction of a country of concern or covered person;

(ii) To act, to have acted or purported to act, or to be likely to act for or on behalf of a country of concern or covered person; or

(iii) To have knowingly caused or directed, or to be likely to knowingly cause or direct a violation of this part.

(b) *Examples*—(1) *Example 1.* Foreign persons primarily resident in Cuba, Iran, or another country of concern would be covered persons.

(2) *Example 2.* Chinese or Russian citizens located in the United States would be treated as U.S. persons and would not be covered persons (except to the extent individually designated). They would be subject to the same prohibitions and restrictions as all other U.S. persons with respect to engaging in covered data transactions with countries of concern or covered persons.

(3) *Example 3.* Citizens of a country of concern who are primarily resident in a third country, such as Russian citizens primarily resident in a European Union country or Cuban citizens primarily resident in a South American country that is not a country of concern, would not be covered persons except to the extent they are individually designated or to the extent that they are employees or contractors of a country of concern government or a covered person that is an entity.

(4) *Example 4.* A foreign person is located abroad and is employed by a company headquartered in China.

Because the company is a covered person that is an entity and the employee is located outside the United States, the employee is a covered person.

(5) *Example 5.* A foreign person is located abroad and is employed by a company that has been designated as a covered person. Because the foreign person is the employee of a covered person that is an entity and the employee is a foreign person, the person is a covered person.

§ 202.212 Covered personal identifiers.

(a) *Definition.* The term *covered personal identifiers* means any listed identifier:

(1) In combination with any other listed identifier; or

(2) In combination with other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data.

(b) *Exclusion.* The term *covered personal identifiers* excludes:

(1) Demographic or contact data that is linked only to other demographic or contact data (such as first and last name, birthplace, ZIP code, residential street or postal address, phone number, and email address and similar public account identifiers); and

(2) A network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar service.

(c) *Examples of listed identifiers in combination with other listed identifiers*—(1) *Example 1.* A standalone listed identifier in isolation (*i.e.*, that is not linked to another listed identifier, sensitive personal data, or other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data)—such as a Social Security Number or account username—would not constitute a covered personal identifier.

(2) *Example 2.* A listed identifier linked to another listed identifier—such as a first and last name linked to a Social Security number, a driver's license number linked to a passport number, a device Media Access Control ("MAC") address linked to a residential address, an account username linked to a first and last name, or a mobile advertising ID linked to an email address—would constitute covered personal identifiers.

(3) *Example 3.* Demographic or contact data linked only to other demographic or contact data—such as a first and last name linked to a residential street address, an email address linked to a first and last name, or a customer loyalty membership record linking a first and last name to a phone number—would not constitute covered personal identifiers.

(4) *Example 4.* Demographic or contact data linked to other demographic or contact data and to another listed identifier—such as a first and last name linked to an email address and to an IP address—would constitute covered personal identifiers.

(5) *Example 5.* Account usernames linked to passwords as part of a sale of a dataset would constitute covered personal identifiers. Those pieces of account-authentication data are not linked as a necessary part of the provision of telecommunications, networking, or similar services. This combination would constitute covered personal identifiers.

(d) *Examples of a listed identifier in combination with other data disclosed by a transacting party—*(1) *Example 1.* A foreign person who is a covered person asks a U.S. company for a list of Media Access Control (“MAC”) addresses from devices that have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building. The U.S. company then sells the list of MAC addresses, without any other listed identifiers or sensitive personal data, to the covered person. The disclosed MAC addresses, when paired with the other data disclosed by the covered person—that the devices “have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building”—makes it so that the MAC addresses are linked or linkable to other sensitive personal data, in this case precise geolocation data of the location of the fast-food restaurant that the national security-related individuals frequent with their devices. This combination of data therefore meets the definition of covered personal identifiers.

(2) *Example 2.* A U.S. company sells to a country of concern a list of residential addresses that the company describes (whether in a heading on the list or separately to the country of concern as part of the transaction) as “addresses of members of a country of concern’s opposition political party in New York City” or as “addresses of active-duty military officers who live in Howard County, Maryland” without any other listed identifiers or sensitive personal data. The data disclosed by the

U.S. company’s description, when paired with the disclosed addresses, makes the addresses linked or linkable to other listed identifiers or to other sensitive personal data of the U.S. individuals associated with them. This combination of data therefore meets the definition of covered personal identifiers.

(3) *Example 3.* A covered person asks a U.S. company for a bulk list of birth dates for “any American who visited a Starbucks in Washington, DC, in December 2023.” The U.S. company then sells the list of birth dates, without any other listed identifiers or sensitive personal data, to the covered person. The other data disclosed by the covered person—“any American who visited a Starbucks in Washington, DC, in December 2023”—does not make the birth dates linked or linkable to other listed identifiers or to other sensitive personal data. This combination of data therefore does not meet the definition of covered personal identifiers.

(4) *Example 4.* Same as Example 3, but the covered person asks the U.S. company for a bulk list of names (rather than birth dates) for “any American who visited a Starbucks in Washington, DC, in December 2023.” The other data disclosed by the covered person—“any American who visited a Starbucks in Washington, DC, in December 2023”—does not make the list of names, without more, linked or linkable to other listed identifiers or to other sensitive personal data. This combination of data therefore does not meet the definition of covered personal identifiers.

(5) *Example 5.* A U.S. company sells to a covered person a list of residential addresses that the company describes (in a heading in the list or to the covered person as part of the transaction) as “households of Americans who watched more than 50% of episodes” of a specific popular TV show, without any other listed identifiers or sensitive personal data. The other data disclosed by the U.S. company—“Americans who watched more than 50% of episodes” of a specific popular TV show—does not increase the extent to which the addresses are linked or linkable to other listed identifiers or to other sensitive personal data. This combination of data therefore does not meet the definition of covered personal identifiers.

§ 202.213 Cuba.

The term *Cuba* means the Republic of Cuba, as well as any political subdivision, agency, or instrumentality thereof.

§ 202.214 Data brokerage.

(a) *Definition.* The term *data brokerage* means the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.

(b) *Examples—*(1) *Example 1.* A U.S. company sells bulk U.S. sensitive personal data to an entity headquartered in a country of concern. The U.S. company engages in prohibited data brokerage.

(2) *Example 2.* A U.S. company enters into an agreement that gives a covered person a license to access government-related data held by the U.S. company. The U.S. company engages in prohibited data brokerage.

(3) *Example 3.* A U.S. organization maintains a database of bulk U.S. sensitive personal data and offers annual memberships for a fee that provide members a license to access that data. Providing an annual membership to a covered person that includes a license to access government-related data or bulk U.S. sensitive personal data would constitute prohibited data brokerage.

(4) *Example 4.* A U.S. company owns and operates a mobile app for U.S. users with available advertising space. As part of selling the advertising space, the U.S. company provides the bulk precise geolocation data, IP address, and advertising IDs of its U.S. users’ devices to an advertising exchange based in a country of concern. The U.S. company’s provision of this data as part of the sale of advertising space is data brokerage and a prohibited transaction.

(5) *Example 5.* Same as Example 4, but the U.S. company provides the data to an advertising exchange based in the United States. As part of the sale of the advertising space, the U.S. advertising exchange provides the data to advertisers headquartered in a country of concern. The U.S. company’s provision of the data to the U.S. advertising exchange would not be a transaction because it is between U.S. persons. The advertising exchange’s provision of this data to the country of concern-based advertisers is data brokerage because it is a commercial transaction involving the transfer of data from the U.S. advertising exchange to the advertisers headquartered in the country of concern, where those country-of-concern advertisers did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.

Furthermore, the U.S. advertising exchange's provision of this data to the country of concern-based advertisers is a prohibited transaction.

(6) *Example 6.* A U.S. information technology company operates an autonomous driving platform that collects the precise geolocation data of its cars operating in the United States. The U.S. company sells or otherwise licenses this bulk data to its parent company headquartered in a country of concern to help develop artificial intelligence technology and machine learning capabilities. The sale or license is data brokerage and a prohibited transaction.

§ 202.215 Directing.

The term *directing* means having any authority (individually or as part of a group) to make decisions for or on behalf of an entity and exercising that authority.

§ 202.216 Effective date.

The term *effective date* refers to the effective date of the applicable prohibitions and directives contained in this part, which is 12:01 a.m. ET on [date to be determined].

§ 202.217 Employment agreement.

(a) *Definition.* The term *employment agreement* means any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level.

(b) *Examples*—(1) *Example 1.* A U.S. company that conducts consumer human genomic testing collects and maintains bulk human genomic data from U.S. consumers. The U.S. company has global IT operations, including employing a team of individuals who are citizens of and primarily resident in a country of concern to provide back-end services. The agreements related to employing these individuals are employment agreements. Employment as part of the global IT operations team includes access to the U.S. company's systems containing the bulk human genomic data. These employment agreements would be prohibited transactions (because they involve access to bulk human genomic data).

(2) *Example 2.* A U.S. company develops its own mobile games and social media apps that collect the bulk U.S. sensitive personal data of its U.S. users. The U.S. company distributes

these games and apps in the United States through U.S.-based digital distribution platforms for software applications. The U.S. company intends to hire as CEO an individual designated by the Attorney General as a covered person because of evidence the CEO acts on behalf of a country of concern. The agreement retaining the individual as CEO would be an employment agreement. The individual's authorities and responsibilities as CEO involve access to all data collected by the apps, including the bulk U.S. sensitive personal data. The CEO's employment would be a restricted transaction.

(3) *Example 3.* A U.S. company has derived U.S. persons' biometric identifiers by scraping public photos from social media platforms. The U.S. company stores the derived biometric identifiers in bulk, including face-data scans, for the purpose of training or enhancing facial-recognition software. The U.S. company intends to hire a foreign person, who primarily resides in a country of concern, as a project manager responsible for the database. The agreement retaining the project manager would be an employment agreement. The individual's employment as the lead project manager would involve access to the bulk biometric identifiers. The project manager's employment would be a restricted transaction.

(4) *Example 4.* A U.S. financial-services company seeks to hire a data scientist who is a citizen of a country of concern who primarily resides in that country of concern and who is developing a new artificial intelligence-based personal assistant that could be sold as a standalone product to the company's customers. The arrangement retaining the data scientist would be an employment agreement. As part of that individual's employment, the data scientist would have administrator rights that allow that individual to access, download, and transmit bulk quantities of personal financial data not ordinarily incident to and part of the company's underlying provision of financial services to its customers. The data scientist's employment would be a restricted transaction.

(5) *Example 5.* A U.S. company sells goods and collects bulk personal financial data about its U.S. customers. The U.S. company appoints a citizen of a country of concern, who is located in a country of concern, to its board of directors. This director would be a covered person, and the arrangement appointing the director would be an employment agreement. In connection with the board's data security and cybersecurity responsibilities, the

director could access the bulk personal financial data. The director's employment would be a restricted transaction.

§ 202.218 Entity.

The term *entity* means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

§ 202.219 Exempt transaction.

The term *exempt transaction* means a data transaction that is subject to one or more exemptions described in subpart E of this part.

§ 202.220 Former senior official.

The term *former senior official* means either a "former senior employee" or a "former very senior employee," as those terms are defined in 5 CFR 2641.104.

§ 202.221 Foreign person.

The term *foreign person* means any person that is not a U.S. person.

§ 202.222 Government-related data.

(a) *Definition.* The term *government-related data* means the following:

(1) Any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List in § 202.1401 which the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights about locations controlled by the Federal Government, including insights about facilities, activities, or populations in those locations, to the detriment of national security, because of the nature of those locations or the personnel who work there. Such locations may include:

(i) The worksite or duty station of Federal Government employees or contractors who occupy a national security position as that term is defined in 5 CFR 1400.102(a)(4);

(ii) A military installation as that term is defined in 10 U.S.C. 2801(c)(4); or

(iii) Facilities or locations that otherwise support the Federal Government's national security, defense, intelligence, law enforcement, or foreign policy missions.

(2) Any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and Intelligence Community.

(b) *Examples of government-related data marketed by a transacting party*—

(1) *Example 1.* A U.S. company advertises the sale of a set of sensitive

personal data as belonging to “active duty” personnel, “military personnel who like to read,” “DoD” personnel, “government employees,” or “communities that are heavily connected to a nearby military base.” The data is government-related data.

(2) *Example 2.* In discussing the sale of a set of sensitive personal data with a covered person, a U.S. company describes the dataset as belonging to members of a specific named organization. The identified organization restricts membership to current and former members of the military and their families. The data is government-related data.

§ 202.223 Human biospecimens.

The term *human biospecimens* means a quantity of tissue, blood, urine, or other human-derived material, including such material classified under any of the following 10-digit Harmonized System-based Schedule B numbers:

- (a) 0501.00.0000 Human hair, unworked, whether or not washed or scoured; waste of human hair
- (b) 3001.20.0000 Extracts of glands or other organs or of their secretions
- (c) 3001.90.0115 Glands and other organs, dried, whether or not powdered
- (d) 3002.12.0010 Human blood plasma
- (e) 3002.12.0020 Normal human blood sera, whether or not freeze-dried
- (f) 3002.12.0030 Human immune blood sera
- (g) 3002.12.0090 Antisera and other blood fractions, Other
- (h) 3002.51.0000 Cell therapy products
- (i) 3002.59.0000 Cell cultures, whether or not modified, Other
- (j) 3002.90.5210 Whole human blood
- (k) 3002.90.5250 Blood, human/animal, other
- (l) 9705.21.0000 Human specimens and parts thereof

§ 202.224 Human genomic data.

The term *human genomic data* means data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a human cell, including the result or results of an individual’s “genetic test” (as defined in 42 U.S.C. 300gg–91(d)(17)) and any related human genetic sequencing data.

§ 202.225 IEEPA.

The term *IEEPA* means the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*).

§ 202.226 Information or informational materials.

(a) *Definition.* The term *information or informational materials* is limited to expressive material and includes publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. It does not include data that is technical, functional, or otherwise non-expressive.

(b) *Exclusions.* The term *information or informational materials* does not include:

- (1) Information or informational materials not fully created and in existence at the date of the data transaction, or the substantive or artistic alteration or enhancement of information or informational materials, or the provision of marketing and business consulting services, including to market, produce or co-produce, or assist in the creation of information or informational materials;
- (2) Items that were, as of April 30, 1994, or that thereafter become, controlled for export to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by 18 U.S.C. chapter 37.

(c) *Examples*—(1) *Example 1.* A U.S. person enters into an agreement to create a customized dataset of bulk U.S. sensitive personal data that meets a covered person’s specifications (such as the specific types and fields of data, date ranges, and other criteria) and to sell that dataset to the covered person. This customized dataset is not fully created and in existence at the date of the agreement, and therefore is not information or informational materials.

(2) *Example 2.* A U.S. company has access to several pre-existing databases of different bulk sensitive personal data. The U.S. company offers, for a fee, to use data analytics to link the data across these databases to the same individuals and to sell that combined dataset to a covered person. This service constitutes a substantive alteration or enhancement of the data in the pre-existing databases and therefore is not information or informational materials.

§ 202.227 Interest.

Except as otherwise provided in this part, the term *interest*, when used with respect to property (*e.g.*, “an interest in property”), means an interest of any nature whatsoever, direct or indirect.

§ 202.228 Investment agreement.

(a) *Definition.* The term *investment agreement* means an agreement or

arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to:

(1) Real estate located in the United States; or

(2) A U.S. legal entity.

(b) *Exclusion for passive investments.* The term *investment agreement* excludes any investment that:

(1) Is made:

(i) Into a publicly traded security, with “security” defined in section 3(a)(10) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(10)), denominated in any currency that trades on a securities exchange or through the method of trading that is commonly referred to as “over-the-counter,” in any jurisdiction;

(ii) Into a security offered by:

(A) Any “investment company” (as defined in section 3(a)(1) of the Investment Company Act of 1940 (15 U.S.C. 80a–3(a)(1))) that is registered with the United States Securities and Exchange Commission, such as index funds, mutual funds, or exchange traded funds; or

(B) Any company that has elected to be regulated or is regulated as a business development company pursuant to section 54(a) of the Investment Company Act of 1940 (15 U.S.C. 80a–53), or any derivative of either of the foregoing; or

(iii) As a limited partner into a venture capital fund, private equity fund, fund of funds, or other pooled investment fund, if the limited partner’s contribution is solely capital and the limited partner cannot make managerial decisions, is not responsible for any debts beyond its investment, and does not have the formal or informal ability to influence or participate in the fund’s or a U.S. person’s decision making or operations;

(2) Gives the covered person less than 10% in total voting and equity interest in a U.S. person; and

(3) Does not give a covered person rights beyond those reasonably considered to be standard minority shareholder protections, including (a) membership or observer rights on, or the right to nominate an individual to a position on, the board of directors or an equivalent governing body of the U.S. person, or (b) any other involvement, beyond the voting of shares, in substantive business decisions, management, or strategy of the U.S. person.

(c) *Examples*—(1) *Example 1.* A U.S. company intends to build a data center located in a U.S. territory. The data center will store bulk personal health

data on U.S. persons. A foreign private equity fund located in a country of concern agrees to provide capital for the construction of the data center in exchange for acquiring a majority ownership stake in the data center. The agreement that gives the private equity fund a stake in the data center is an investment agreement. The investment agreement is a restricted transaction.

(2) *Example 2.* A foreign technology company that is subject to the jurisdiction of a country of concern and that the Attorney General has designated as a covered person enters into a shareholders' agreement with a U.S. business that develops mobile games and social media apps, acquiring a minority equity stake in the U.S. business. The shareholders' agreement is an investment agreement. These games and apps developed by the U.S. business systematically collect bulk U.S. sensitive personal data of its U.S. users. The investment agreement explicitly gives the foreign technology company the ability to access this data and is therefore a restricted transaction.

(3) *Example 3.* Same as Example 2, but the investment agreement either does not explicitly give the foreign technology company the right to access the data or explicitly forbids that access. The investment agreement nonetheless provides the foreign technology company with the sufficient ownership interest, rights, or other involvement in substantive business decisions, management, or strategy such that the investment does not constitute a passive investment. Because it is not a passive investment, the ownership interest, rights, or other involvement in substantive business decisions, management, or strategy gives the foreign technology company the ability to obtain logical or physical access, regardless of how the agreement formally distributes those rights. The investment agreement therefore involves access to bulk U.S. sensitive personal data. The investment agreement is a restricted transaction.

(4) *Example 4.* Same as Example 3, but the U.S. business does not maintain or have access to any government-related data or bulk U.S. sensitive personal data (e.g., a pre-commercial company or startup company). Because the data transaction cannot involve access to any government-related data or bulk U.S. sensitive personal data, this investment agreement does not meet the definition of a covered data transaction and is not a restricted transaction.

§ 202.229 Iran.

The term *Iran* means the Islamic Republic of Iran, as well as any political

subdivision, agency, or instrumentality thereof.

§ 202.230 Knowingly.

(a) *Definition.* The term *knowingly*, with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or reasonably should have known, of the conduct, the circumstance, or the result.

(b) *Examples—*(1) *Example 1.* A U.S. company sells DNA testing kits to U.S. consumers and maintains bulk human genomic data collected from those consumers. The U.S. company enters into a contract with a foreign cloud-computing company (which is not a covered person) to store the U.S. company's database of human genomic data. The foreign company hires employees from other countries, including citizens of countries of concern who primarily reside in a country of concern, to manage databases for its customers, including the U.S. company's human genomic database. There is no indication of evasion, such as the U.S. company knowingly directing the foreign company's employment agreements with covered persons, or the U.S. company engaging in and structuring these transactions to evade the regulations. The cloud-computing services agreement between the U.S. company and the foreign company would not be prohibited or restricted, because that covered data transaction is between a U.S. person and a foreign company that does not meet the definition of a covered person. The employment agreements between the foreign company and the covered persons would not be prohibited or restricted because those agreements are between foreign persons.

(2) *Example 2.* A U.S. company transmits the bulk U.S. sensitive personal data of U.S. persons to a country of concern, in violation of this part, using a fiber optic cable operated by another U.S. company. The U.S. cable operator has not knowingly engaged in a prohibited transaction or a restricted transaction solely by virtue of operating the fiber optic cable because the U.S. cable operator does not know, and reasonably should not know, the content of the traffic transmitted across the fiber optic cable.

(3) *Example 3.* A U.S. service provider provides a software platform on which a U.S. company processes the bulk U.S. sensitive personal data of its U.S.-person customers. While the U.S. service provider is generally aware of the nature of the U.S. company's business, the U.S. service provider is not aware of the kind or volume of data that the U.S. company processes on the

platform, how the U.S. company uses the data, or whether the U.S. company engages in data transactions. The U.S. company also primarily controls access to its data on the platform, with the U.S. service provider accessing the data only for troubleshooting or technical support purposes, upon request by the U.S. company. Subsequently, without the actual knowledge of the U.S. service provider and without providing the U.S. service provider with any information from which the service provider should have known, the U.S. company grants access to the data on the U.S. service provider's software platform to a covered person through a covered data transaction, in violation of this part. The U.S. service provider itself, however, has not knowingly engaged in a restricted transaction by enabling the covered persons' access via its software platform.

(4) *Example 4.* Same as Example 3, but in addition to providing the software platform, the U.S. company's contract with the U.S. service provider also outsources the U.S. company's processing and handling of the data to the U.S. service provider. As a result, the U.S. service provider primarily controls access to the U.S. company's bulk U.S. sensitive personal data on the platform. The U.S. service provider employs a covered person and grants access to this data as part of this employment. Although the U.S. company's contract with the U.S. service provider is not a restricted transaction, the U.S. service provider's employment agreement with the covered person is a restricted transaction. The U.S. service provider has thus knowingly engaged in a restricted transaction by entering into an employment agreement that grants access to its employee because the U.S. service provider knew or should have known of its employee's covered person status and, as the party responsible for processing and handling the data, the U.S. service provider was aware of the kind and volume of data that the U.S. company processes on the platform.

(5) *Example 5.* A U.S. company provides cloud storage to a U.S. customer for the encrypted storage of the customer's bulk U.S. sensitive personal data. The U.S. cloud-service provider has an emergency back-up encryption key for all its customers' data, but the company is contractually limited to using the key to decrypt the data only at the customer's request. The U.S. customer's systems and access to the key become disabled, and the U.S. customer requests that the cloud-service provider use the back-up encryption key to decrypt the data and store it on a

backup server while the customer restores its own systems. By having access to and using the backup encryption key to decrypt the data in accordance with the contractual limitation, the U.S. cloud-service provider does not and reasonably should not know the kind and volumes of the U.S. customer's data. If the U.S. customer later uses the cloud storage to knowingly engage in a prohibited transaction, the U.S. cloud-service provider's access to and use of the backup encryption key does not mean that the U.S. cloud-service provider has also knowingly engaged in a restricted transaction.

(6) *Example 6.* A prominent human genomics research clinic enters into a cloud-services contract with a U.S. cloud-service provider that specializes in storing and processing healthcare data to store bulk human genomic research data. The cloud-service provider hires IT personnel in a country of concern, who are thus covered persons. While the data that is stored is encrypted, the IT personnel can access the data in encrypted form. The employment agreement between the U.S. cloud-service provider and the IT professionals in the country of concern is a prohibited transaction because the agreement involves giving the IT personnel access to the encrypted data and constitutes a transfer of human genomic data. Given the nature of the research institution's work and the cloud-service provider's expertise in storing healthcare data, the cloud-service provider reasonably should have known that the encrypted data is bulk U.S. sensitive personal data covered by the regulations. The cloud-service provider has therefore knowingly engaged in a prohibited transaction (because it involves access to human genomic data).

§ 202.231 Licenses; general and specific.

(a) *General license.* The term *general license* means a written license issued pursuant to this part authorizing a class of transactions and not limited to a particular person.

(b) *Specific license.* The term *specific license* means a written license issued pursuant to this part to a particular person or persons, authorizing a particular transaction or transactions in response to a written license application.

§ 202.232 Linked.

(a) *Definition.* The term *linked* means associated.

(b) *Examples*—(1) *Example 1.* A U.S. person transfers two listed identifiers in a single spreadsheet—such as a list of

names of individuals and associated MAC addresses for those individuals' devices. The names and MAC addresses would be considered linked.

(2) *Example 2.* A U.S. person transfers two listed identifiers in different spreadsheets—such as a list of names of individuals in one spreadsheet and MAC addresses in another spreadsheet—to two related parties in two different covered data transactions. The names and MAC addresses would be considered linked, provided that some correlation existed between the names and MAC addresses (e.g., associated employee ID number is also listed in both spreadsheets).

(3) *Example 3.* A U.S. person transfers a standalone list of MAC addresses, without any additional listed identifiers. The standalone list does not include covered personal identifiers. That standalone list of MAC addresses would not become covered personal identifiers even if the receiving party is capable of obtaining separate sets of other listed identifiers or sensitive personal data through separate covered data transactions with unaffiliated parties that would ultimately permit the association of the MAC addresses to specific persons. The MAC addresses would not be considered linked or linkable to those separate sets of other listed identifiers or sensitive personal data.

§ 202.233 Linkable.

The term *linkable* means reasonably capable of being linked.

Note to § 202.233. Data is considered linkable when the identifiers involved in a single covered data transaction, or in multiple covered data transactions or a course of dealing between the same or related parties, are reasonably capable of being associated with the same person(s). Identifiers are not linked or linkable when additional identifiers or data not involved in the relevant covered data transaction(s) would be necessary to associate the identifiers with the same specific person(s).

§ 202.234 Listed identifier.

The term *listed identifier* means any piece of data in any of the following data fields:

(a) Full or truncated government identification or account number (such as a Social Security number, driver's license or State identification number, passport number, or Alien Registration Number);

(b) Full financial account numbers or personal identification numbers associated with a financial institution or financial-services company;

(c) Device-based or hardware-based identifier (such as International Mobile Equipment Identity (“IMEI”), Media Access Control (“MAC”) address, or Subscriber Identity Module (“SIM”) card number);

(d) Demographic or contact data (such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers);

(e) Advertising identifier (such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising ID (“MAID”));

(f) Account-authentication data (such as account username, account password, or an answer to security questions);

(g) Network-based identifier (such as internet Protocol (“IP”) address or cookie data); or

(h) Call-detail data (such as Customer Proprietary Network Information (“CPNI”).

§ 202.235 National Security Division.

The term *National Security Division* means the National Security Division of the United States Department of Justice.

§ 202.236 North Korea.

The term *North Korea* means the Democratic People's Republic of North Korea, and any political subdivision, agency, or instrumentality thereof.

§ 202.237 Order.

The term *Order* means Executive Order 14117 of February 28, 2024 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern), 89 FR 15421 (March 1, 2024).

§ 202.238 Person.

The term *person* means an individual or entity.

§ 202.239 Personal communications.

The term *personal communications* means any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value, as set out under 50 U.S.C. 1702(b)(1).

§ 202.240 Personal financial data.

The term *personal financial data* means data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data in a bank, credit, or other financial statement, including assets, liabilities, debts, or trades in a securities portfolio; or data in a credit report or in a “consumer report” (as defined in 15 U.S.C. 1681a(d)).

§ 202.241 Personal health data.

The term *personal health data* means health information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. This term includes basic physical measurements and health attributes (such as bodily functions, height and weight, vital signs, symptoms, and allergies); social, psychological, behavioral, and medical diagnostic, intervention, and treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications.

§ 202.242 Precise geolocation data.

The term *precise geolocation data* means data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within 1,000 meters.

§ 202.243 Prohibited transaction.

The term *prohibited transaction* means a data transaction that is subject to one or more of the prohibitions described in subpart C of this part.

§ 202.244 Property; property interest.

The terms *property* and *property interest* include money; checks; drafts; bullion; bank deposits; savings accounts; debts; indebtedness; obligations; notes; guarantees; debentures; stocks; bonds; coupons; any other financial instruments; bankers acceptances; mortgages, pledges, liens, or other rights in the nature of security; warehouse receipts, bills of lading, trust receipts, bills of sale, or any other evidences of title, ownership, or indebtedness; letters of credit and any documents relating to any rights or obligations thereunder; powers of attorney; goods; wares; merchandise; chattels; stocks on hand; ships; goods on ships; real estate mortgages; deeds of trust; vendors' sales agreements; land contracts, leaseholds, ground rents, real estate and any other interest therein; options; negotiable instruments; trade acceptances; royalties; book accounts; accounts payable; judgments; patents; trademarks or copyrights; insurance policies; safe deposit boxes and their contents; annuities; pooling agreements; services of any nature whatsoever; contracts of any nature whatsoever; any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent.

§ 202.245 Recent former employees or contractors.

The terms *recent former employees* or *recent former contractors* mean employees or contractors who worked for or provided services to the United States Government, in a paid or unpaid status, within the past 2 years of a potential covered data transaction.

§ 202.246 Restricted transaction.

The term *restricted transaction* means a data transaction that is subject to subpart D of this part.

§ 202.247 Russia.

The term *Russia* means the Russian Federation, and any political subdivision, agency, or instrumentality thereof.

§ 202.248 Security requirements.

The term *security requirements* means the Cybersecurity and Infrastructure Agency ("CISA") Security Requirements for Restricted Transactions (incorporated by reference, *see* § 202.402).

§ 202.249 Sensitive personal data.

(a) *Definition.* The term *sensitive personal data* means covered personal identifiers, precise geolocation data, biometric identifiers, human genomic data, personal health data, personal financial data, or any combination thereof.

(b) *Exclusions.* The term *sensitive personal data* excludes:

(1) Public or nonpublic data that does not relate to an individual, including such data that meets the definition of a "trade secret" (as defined in 18 U.S.C. 1839(3)) or "proprietary information" (as defined in 50 U.S.C. 1708(d)(7));

(2) Data that is, at the time of the transaction, lawfully available to the public from a Federal, State, or local government record (such as court records) or in widely distributed media (such as sources that are generally available to the public through unrestricted and open-access repositories);

(3) Personal communications; and

(4) Information or informational materials.

§ 202.250 Special Administrative Region of Hong Kong.

The term *Special Administrative Region of Hong Kong* means the Special Administrative Region of Hong Kong, and any political subdivision, agency, or instrumentality thereof.

§ 202.251 Special Administrative Region of Macau.

The term *Special Administrative Region of Macau* means the Special

Administrative Region of Macau, and any political subdivision, agency, or instrumentality thereof.

§ 202.252 Telecommunications service.

The term *telecommunications service* means "telecommunications service" as defined in 47 U.S.C. 153(53).

§ 202.253 Transaction.

The term *transaction* means any acquisition, holding, use, transfer, transportation, exportation of, or dealing in any property in which a foreign country or national thereof has an interest.

§ 202.254 Transfer.

The term *transfer* means any actual or purported act or transaction, whether or not evidenced by writing, and whether or not done or performed within the United States, the purpose, intent, or effect of which is to create, surrender, release, convey, transfer, or alter, directly or indirectly, any right, remedy, power, privilege, or interest with respect to any property. Without limitation on the foregoing, it shall include the making, execution, or delivery of any assignment, power, conveyance, check, declaration, deed, deed of trust, power of attorney, power of appointment, bill of sale, mortgage, receipt, agreement, contract, certificate, gift, sale, affidavit, or statement; the making of any payment; the setting off of any obligation or credit; the appointment of any agent, trustee, or fiduciary; the creation or transfer of any lien; the issuance, docketing, filing, or levy of or under any judgment, decree, attachment, injunction, execution, or other judicial or administrative process or order, or the service of any garnishment; the acquisition of any interest of any nature whatsoever by reason of a judgment or decree of any foreign country; the fulfillment of any condition; the exercise of any power of appointment, power of attorney, or other power; or the acquisition, disposition, transportation, importation, exportation, or withdrawal of any security.

§ 202.255 United States.

The term *United States* means the United States, its territories and possessions, and all areas under the jurisdiction or authority thereof.

§ 202.256 United States person or U.S. person.

(a) *Definition.* The terms *United States person* and *U.S. person* mean any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted

asylum under 8 U.S.C. 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States.

(b) *Examples*—(1) *Example 1.* An individual is a citizen of a country of concern and is in the United States. The individual is a U.S. person.

(2) *Example 2.* An individual is a U.S. citizen. The individual is a U.S. person, regardless of location.

(3) *Example 3.* An individual is a dual citizen of the United States and a country of concern. The individual is a U.S. person, regardless of location.

(4) *Example 4.* An individual is a citizen of a country of concern, is not a permanent resident alien of the United States, and is outside the United States. The individual is a foreign person.

(5) *Example 5.* A company is organized under the laws of the United States and has a foreign branch in a country of concern. The company, including its foreign branch, is a U.S. person.

(6) *Example 6.* A parent company is organized under the laws of the United States and has a subsidiary organized under the laws of a country of concern. The subsidiary is a foreign person regardless of the degree of ownership by the parent company; the parent company is a U.S. person.

(7) *Example 7.* A company is organized under the laws of a country of concern and has a branch in the United States. The company, including its U.S. branch, is a foreign person.

(8) *Example 8.* A parent company is organized under the laws of a country of concern and has a subsidiary organized under the laws of the United States. The subsidiary is a U.S. person regardless of the degree of ownership by the parent company; the parent company is a foreign person.

§ 202.257 U.S. device.

The term *U.S. device* means any device with the capacity to store or transmit data that is linked or linkable to a U.S. person.

§ 202.258 Vendor agreement.

(a) *Definition.* The term *vendor agreement* means any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.

(b) *Examples*—(1) *Example 1.* A U.S. company collects bulk precise geolocation data from U.S. users through an app. The U.S. company

enters into an agreement with a company headquartered in a country of concern to process and store this data. This vendor agreement is a restricted transaction.

(2) *Example 2.* A medical facility in the United States contracts with a company headquartered in a country of concern to provide IT-related services. The contract governing the provision of services is a vendor agreement. The medical facility has bulk personal health data on its U.S. patients. The IT services provided under the contract involve access to the medical facility's systems containing the bulk personal health data. This vendor agreement is a restricted transaction.

(3) *Example 3.* A U.S. company, which is owned by an entity headquartered in a country of concern and has been designated a covered person, establishes a new data center in the United States to offer managed services. The U.S. company's data center serves as a vendor to various U.S. companies to store bulk U.S. sensitive personal data collected by those companies. These vendor agreements are restricted transactions.

(4) *Example 4.* A U.S. company develops mobile games that collect bulk precise geolocation data and biometric identifiers of U.S.-person users. The U.S. company contracts part of the software development to a foreign person who is primarily resident in a country of concern and is a covered person. The contract with the foreign person is a vendor agreement. The software-development services provided by the covered person under the contract involve access to the bulk precise geolocation data and biometric identifiers. This is a restricted transaction.

(5) *Example 5.* A U.S. multinational company maintains bulk U.S. sensitive personal data of U.S. persons. This company has a foreign branch, located in a country of concern, that has access to this data. The foreign branch contracts with a local company located in the country of concern to provide cleaning services for the foreign branch's facilities. The contract is a vendor agreement, the foreign branch is a U.S. person, and the local company is a covered person. Because the services performed under this vendor agreement do not "involve access to" the bulk U.S. sensitive personal data, the vendor agreement would not be a covered data transaction.

§ 202.259 Venezuela.

The term *Venezuela* means the Bolivarian Republic of Venezuela, and

any political subdivision, agency, or instrumentality thereof.

Subpart C—Prohibited Transactions and Related Activities

§ 202.301 Prohibited data-brokerage transactions.

(a) *Prohibition.* Except as otherwise authorized pursuant to subparts E or H of this part or any other provision of this part, no U.S. person, on or after the effective date, may knowingly engage in a covered data transaction involving data brokerage with a country of concern or covered person.

(b) *Examples*—(1) *Example 1.* A U.S. subsidiary of a company headquartered in a country of concern develops an artificial intelligence chatbot in the United States that is trained on the bulk U.S. sensitive personal data of U.S. persons. While not its primary commercial use, the chatbot is capable of reproducing or otherwise disclosing the bulk sensitive personal health data that was used to train the chatbot when responding to queries. The U.S. subsidiary knowingly licenses subscription-based access to that chatbot worldwide, including to covered persons such as its parent entity. Although licensing use of the chatbot itself may not necessarily "involve access" to bulk U.S. sensitive personal data, the U.S. subsidiary knows or should know that the license can be used to obtain access to the U.S. persons' bulk sensitive personal training data if prompted. The licensing of access to this bulk U.S. sensitive personal data is data brokerage because it involves the transfer of data from the U.S. company (*i.e.*, the provider) to licensees (*i.e.*, the recipients), where the recipients did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. Even though the license did not explicitly provide access to the data, this is a prohibited transaction because the U.S. company knew or should have known that the use of the chatbot pursuant to the license could be used to obtain access to the training data, and because the U.S. company licensed the product to covered persons.

(2) [Reserved]

§ 202.302 Other prohibited data-brokerage transactions involving potential onward transfer to countries of concern or covered persons.

(a) *Prohibition.* Except as otherwise authorized pursuant to this part, no U.S. person, on or after the effective date, may knowingly engage in a covered data transaction involving data brokerage with any foreign person that is not a covered person unless the U.S. person:

(1) Contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving data brokerage of the same data with a country of concern or covered person; and

(2) Reports any known or suspected violations of this contractual requirement in accordance with paragraph (b) of this section.

(b) *Reporting known or suspected violations*—(1) *When reports are due.* U.S. persons shall file reports within 14 days of the U.S. person becoming aware of a known or suspected violation.

(2) *Contents of reports.* Reports on known or suspected violations shall include the following, to the extent the information is known and available to the person filing the report at the time of the report:

(i) The name and address of the U.S. person reporting the known or suspected violation of the contractual requirement in accordance with paragraph (b) of this section;

(ii) A description of the known or suspected violation, including:

(A) Date of known or suspected violation;

(B) Description of the data-brokerage transaction referenced in paragraph (a) of this section;

(C) Description of the contractual provision prohibiting the onward transfer of the same data to a country of concern or covered person;

(D) Description of the known or suspected violation of the contractual obligation prohibiting the foreign person from engaging in a subsequent covered data transaction involving the same data with a country of concern or a covered person;

(E) Any persons substantively participating in the transaction referenced in paragraph (a) of this section;

(F) Information about the known or suspected persons involved in the onward data transfer transaction, including the name and location of any covered persons or countries of concern;

(G) A copy of any relevant documentation received or created in connection with the transaction; and

(iii) Any other information that the Department of Justice may require or any other information that the U.S. person filing the report believes to be pertinent to the known or suspected violation or the implicated covered person.

(3) *Additional contents; format and method of submission.* Reports required by this section must be submitted in accordance with this section and with subpart L of this part.

(c) *Examples*—(1) *Example 1.* A U.S. business knowingly enters into an agreement to sell bulk human genomic data to a European business that is not a covered person. The U.S. business is required to include in that agreement a limitation on the European business' right to resell or otherwise engage in a covered data transaction involving data brokerage of that data to a country of concern or covered person. Otherwise, the agreement would be a prohibited transaction.

(2) *Example 2.* A U.S. company owns and operates a mobile app for U.S. users with available advertising space. As part of selling the advertising space, the U.S. company provides the bulk precise geolocation data, IP address, and advertising IDs of its U.S. users' devices to an advertising exchange based in Europe that is not a covered person. The U.S. company's provision of this data to the advertising exchange is data brokerage and a prohibited transaction unless the U.S. company obtains a contractual commitment from the advertising exchange not to engage in any covered data transactions involving data brokerage of that same data with a country of concern or covered person.

§ 202.303 Prohibited human genomic data and human biospecimen transactions.

Except as otherwise authorized pursuant to this part, no U.S. person, on or after the effective date, may knowingly engage in any covered data transaction with a country of concern or covered person that involves access by that country of concern or covered person to bulk U.S. sensitive personal data that involves bulk human genomic data, or to human biospecimens from which bulk human genomic data could be derived.

§ 202.304 Prohibited evasions, attempts, causing violations, and conspiracies.

(a) *Prohibition.* Any transaction on or after the effective date that has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this part is prohibited. Any conspiracy formed to violate the prohibitions set forth in this part is prohibited.

(b) *Examples*—(1) *Example 1.* A U.S. data broker seeks to sell bulk U.S. sensitive personal data to a foreign person who primarily resides in China. With knowledge that the foreign person is a covered person and with the intent to evade the regulations, the U.S. data broker invites the foreign person to travel to the United States to consummate the data transaction and transfer the bulk U.S. sensitive personal data in the United States. After

completing the transaction, the person returns to China with the bulk U.S. sensitive personal data. The transaction in the United States is not a covered data transaction because the person who resides in China is a U.S. person while in the United States (unless that person was individually designated as a covered person pursuant to § 202.211(a)(5), in which case their covered person status would remain, even while in the United States, and the transaction would be a covered data transaction). However, the U.S. data broker has structured the transaction to evade the regulation's prohibitions on covered data transactions with covered persons. As a result, this transaction has the purpose of evading the regulations and is prohibited.

(2) *Example 2.* A Russian national, who is employed by a corporation headquartered in Russia, travels to the United States to conduct business with the Russian company's U.S. subsidiary, including with the purpose of obtaining bulk U.S. sensitive personal data from the U.S. subsidiary. The U.S. subsidiary is a U.S. person, the Russian corporation is a covered person, and the Russian employee is a covered person while outside the United States but a U.S. person while temporarily in the United States (unless that Russian employee was individually designated as a covered person pursuant to § 202.211(a)(5), in which case their covered person status would remain, even while in the United States, and the transaction would be a covered data transaction). With knowledge of these facts, the U.S. subsidiary licenses access to bulk U.S. sensitive personal data to the Russian employee while in the United States, who then returns to Russia. This transaction has the purpose of evading the regulations and is prohibited.

(3) *Example 3.* A U.S. subsidiary of a company headquartered in a country of concern collects bulk precise geolocation data from U.S. persons. The U.S. subsidiary is a U.S. person, and the parent company is a covered person. With the purpose of evading the regulations, the U.S. subsidiary enters into a vendor agreement with a foreign company that is not a covered person. The vendor agreement provides the foreign company access to the data. The U.S. subsidiary knows (or reasonably should know) that the foreign company is a shell company, and knows that it subsequently outsources the vendor agreement to the U.S. subsidiary's parent company. This transaction has the purpose of evading the regulations and is prohibited.

(4) *Example 4.* A U.S. company collects bulk personal health data from U.S. persons. With the purpose of evading the regulations, the U.S. company enters into a vendor agreement with a foreign company that is not a covered person. The agreement provides the foreign company access to the data. The U.S. company knows (or reasonably should know) that the foreign company is a front company staffed primarily by covered persons. The U.S. company has not complied with either the security requirements in § 202.248 or other applicable requirements for conducting restricted transactions as detailed in subpart J of this part. This transaction has the purpose of evading the regulations and is prohibited.

(6) *Example 6.* A U.S. online gambling company uses an artificial intelligence algorithm to analyze collected bulk covered personal identifiers to identify users based on impulsivity for targeted advertising. For the purpose of evasion, a U.S. subsidiary of a company headquartered in a country of concern licenses the derivative algorithm from the U.S. online gambling company for the purpose of accessing bulk sensitive personal identifiers from the training data contained in the algorithm that would not otherwise be accessible to the parent company and shares the algorithm with the parent company so that the parent company can obtain the bulk covered personal identifiers. The U.S. subsidiary's licensing transaction with the parent company has the purpose of evading the regulations and is prohibited.

§ 202.305 Knowingly directing prohibited or restricted transactions.

(a) *Prohibition.* Except as otherwise authorized pursuant to this part, no U.S. person, on or after the effective date, may knowingly direct any covered data transaction that would be a prohibited transaction or restricted transaction that fails to comply with the requirements of subpart D and all other applicable requirements under this part, if engaged in by a U.S. person.

(b) *Examples—*(1) *Example 1.* A U.S. person is an officer, senior manager, or equivalent senior-level employee at a foreign company that is not a covered person, and the foreign company undertakes a covered data transaction at that U.S. person's direction or with that U.S. person's approval when the covered data transaction would be prohibited if performed by a U.S. person. The U.S. person has knowingly directed a prohibited transaction.

(2) *Example 2.* Several U.S. persons launch, own, and operate a foreign company that is not a covered person,

and that foreign company, under the U.S. persons' operation, undertakes covered data transactions that would be prohibited if performed by a U.S. person. The U.S. persons have knowingly directed a prohibited transaction.

(3) *Example 3.* A U.S. person is employed at a U.S.-headquartered multinational company that has a foreign affiliate that is not a covered person. The U.S. person instructs the U.S. company's compliance unit to change (or approve changes to) the operating policies and procedures of the foreign affiliate with the specific purpose of allowing the foreign affiliate to undertake covered data transactions that would be prohibited if performed by a U.S. person. The U.S. person has knowingly directed prohibited transactions.

(4) *Example 4.* A U.S. bank processes a payment from a U.S. person to a covered person, or from a covered person to a U.S. person, as part of that U.S. person's engagement in a prohibited transaction. The U.S. bank has not knowingly directed a prohibited transaction, and its activity would not be prohibited (although the U.S. person's covered data transaction would be prohibited).

(5) *Example 5.* A U.S. financial institution underwrites a loan or otherwise provides financing for a foreign company that is not a covered person, and the foreign company undertakes covered data transactions that would be prohibited if performed by a U.S. person. The U.S. financial institution has not knowingly directed a prohibited transaction, and its activity would not be prohibited.

(6) *Example 6.* A U.S. person, who is employed at a foreign company that is not a covered person, signs paperwork approving the foreign company's procurement of real estate for its operations. The same foreign company separately conducts data transactions that use or are facilitated by operations at that real estate location and that would be prohibited transactions if performed by a U.S. person, but the U.S. employee has no role in approving or directing those separate data transactions. The U.S. person has not knowingly directed a prohibited transaction, and the U.S. person's activity would not be prohibited.

(7) *Example 7.* A U.S. company owns or operates a submarine telecommunications cable with one landing point in a foreign country that is not a country of concern and one landing point in a country of concern. The U.S. company leases capacity on the cable to U.S. customers that transmit

bulk U.S. sensitive personal data to the landing point in the country of concern, including transmissions as part of prohibited transactions. The U.S. company's ownership or operation of the cable does not constitute knowingly directing a prohibited transaction, and its ownership or operation of the cable would not be prohibited (although the U.S. customers' covered data transactions would be prohibited).

(8) *Example 8.* A U.S. person engages in a vendor agreement involving bulk U.S. sensitive personal data with a foreign person who is not a covered person. Such vendor agreement is not a restricted or prohibited transaction. The foreign person then employs an individual who is a covered person and grants them access to bulk U.S. sensitive personal data without the U.S. person's knowledge or direction. There is no covered data transaction between the U.S. person and the covered person, and there is no indication that the parties engaged in these transactions with the purpose of evading the regulations (such as the U.S. person having knowingly directed the foreign person's employment agreement with the covered person or the parties knowingly structuring a restricted transaction into these multiple transactions with the purpose of evading the prohibition). The U.S. person has not knowingly directed a restricted transaction.

(9) *Example 9.* A U.S. company sells DNA testing kits to U.S. consumers and maintains bulk human genomic data collected from those consumers. The U.S. company enters into a contract with a foreign cloud-computing company (which is not a covered person) to store the U.S. company's database of human genomic data. The foreign company hires employees from other countries, including citizens of countries of concern who primarily reside in a country of concern, to manage databases for its customers, including the U.S. company's human genomic database. There is no indication of evasion, such as the U.S. company knowingly directing the foreign company's employment agreements or the U.S. company knowingly engaging in and structuring these transactions to evade the regulations. The cloud-computing services agreement between the U.S. company and the foreign company would not be prohibited or restricted because that transaction is between a U.S. person and a foreign company that does not meet the definition of a covered person. The employment agreements between the foreign company and the covered persons would not be prohibited or restricted

because those agreements are between foreign persons.

Subpart D—Restricted Transactions

§ 202.401 Authorization to conduct restricted transactions.

(a) *Restricted transactions.* Except as otherwise authorized pursuant to subparts E or H of this part or any other provision of this part, no U.S. person, on or after the effective date, may knowingly engage in a covered data transaction involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person unless the U.S. person complies with the security requirements required by subpart D of this part and all other applicable requirements under this part.

(b) This subpart does not apply to covered data transactions involving access to bulk human genomic data or human biospecimens from which such data can be derived that is subject to the prohibition in § 202.303 of this part.

(c) *Examples—(1) Example 1.* A U.S. company engages in an employment agreement with a covered person to provide information technology support. As part of their employment, the covered person has access to personal financial data. The U.S. company implements and complies with the security requirements. The employment agreement is authorized as a restricted transaction because the company has complied with the security requirements.

(2) *Example 2.* A U.S. company engages in a vendor agreement with a covered person to store bulk personal health data. Instead of implementing the security requirements as identified by reference in this subpart, the U.S. company implements different controls that it believes mitigate the covered person's access to the bulk personal health data. Because the U.S. person has not complied with the security requirements, the vendor agreement is not authorized and thus is a prohibited transaction.

(3) *Example 3.* A U.S. person engages in a vendor agreement involving bulk U.S. sensitive personal data with a foreign person who is not a covered person. The foreign person then employs an individual who is a covered person and grants them access to bulk U.S. sensitive personal data without the U.S. person's knowledge or direction. There is no covered data transaction between the U.S. person and the covered person, and there is no indication that the parties engaged in these transactions with the purpose of evading the regulations (such as the U.S.

person having knowingly directed the foreign person's employment agreement with the covered person or the parties knowingly structuring a prohibited transaction into these multiple transactions with the purpose of evading the prohibition). As a result, neither the vendor agreement nor the employment agreement would be a restricted transaction.

§ 202.402 Incorporation by reference.

(a) *Incorporation by reference.* Certain material is incorporated by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. This incorporation by reference ("IBR") material is available for inspection at the Department of Justice and at the National Archives and Records Administration ("NARA"). Please contact the Foreign Investment Review Section, National Security Division, U.S. Department of Justice, 175 N St. NE, Washington, DC 20002, telephone: 202-514-8648, NSD.FIRS.datasecurity@usdoj.gov. You may also obtain the material from the National Security Division at <https://www.justice.gov/nsd>. For information on the availability of this material at NARA, visit www.archives.gov/federal-register/cfr/ibr-locations.html or email fr.inspection@nara.gov. The material may also be obtained from the sources in the following paragraphs of this section.

(b) *Other sources.* The Cybersecurity and Infrastructure Security Agency, Mail Stop 0380, Department of Homeland Security, 245 Murray Lane, Washington, DC 20528-0380, central@cisa.gov, 888-282-0870, <http://www.cisa.gov>. You may also obtain the material from the Cybersecurity and Infrastructure Security Agency at <https://www.cisa.gov/>.

(1) The Cybersecurity and Infrastructure Security Agency ("CISA"), Security Requirements for Restricted Transactions; (Final edition 202X Draft), IBR approved for §§ 202.248; 202.304(b)(4); 202.401(a); 202.401(c)(1); 202.401(c)(2); 202.508(b)(8); 202.508(b)(10); 202.508(b)(11); 202.1001(b)(4); 202.1002(b)(1); 202.1002(e)(4); 202.1002(f)(2)(iv); 202.1002(f)(2)(v); 202.1002(f)(2)(vi); 202.1101(b)(2); 202.1101(b)(3).

(2) [Reserved]

Subpart E—Exempt Transactions

§ 202.501 Personal communications.

Subparts C and D of this part do not apply to data transactions to the extent that they involve any postal, telegraphic, telephonic, or other

personal communication that does not involve the transfer of anything of value.

§ 202.502 Information or informational materials.

Subparts C and D of this part do not apply to data transactions to the extent that they involve the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials.

§ 202.503 Travel.

Subparts C and D of this part do not apply to data transactions to the extent that they are ordinarily incident to travel to or from any country, including importation of accompanied baggage for personal use; maintenance within any country, including payment of living expenses and acquisition of goods or services for personal use; and arrangement or facilitation of such travel, including nonscheduled air, sea, or land voyages.

§ 202.504 Official business of the United States Government.

(a) *Exemption.* Subparts C and D of this part do not apply to data transactions to the extent that they are for the conduct of the official business of the United States Government by its employees, grantees, or contractors; any authorized activity of any United States Government department or agency (including an activity that is performed by a Federal depository institution or credit union supervisory agency in the capacity of receiver or conservator); or transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government.

(b) *Examples—(1) Example 1.* A U.S. hospital receives a Federal grant to conduct human genomic research on U.S. persons. As part of that federally funded human genomic research, the U.S. hospital contracts with a foreign laboratory that is a covered person, hires a researcher that is a covered person, and gives the laboratory and researcher access to the human biospecimens and human genomic data in bulk. The contract with the foreign laboratory and the employment of the researcher are exempt transactions but would be prohibited transactions if they were not part of the federally funded research.

(2) [Reserved]

§ 202.505 Financial services.

(a) *Exemption.* Subparts C and D of this part do not apply to data transactions, to the extent that they are ordinarily incident to and part of the

provision of financial services, including:

(1) Banking, capital-markets (including investment-management services), or financial-insurance services;

(2) A financial activity authorized for national banks by 12 U.S.C. 24 (Seventh) and rules and regulations and written interpretations of the Office of the Comptroller of the Currency thereunder;

(3) An activity that is “financial in nature or incidental to such financial activity” or “complementary to a financial activity,” section (k)(1), as set forth in section (k)(4) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)) and rules and regulations and written interpretations of the Board of Governors of the Federal Reserve System thereunder;

(4) The transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces);

(5) The provision or processing of payments or funds transfers (such as person-to-person, business-to-person, and government-to-person funds transfers) involving the transfer of personal financial data or covered personal identifiers, or the provision of services ancillary to processing payments and funds transfers (such as services for payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention, and payment-related loyalty point program administration); and

(6) The provision of investment-management services that manage or provide advice on investment portfolios or individual assets for compensation (such as devising strategies and handling financial assets and other investments for clients) or provide services ancillary to investment-management services (such as broker-dealers executing trades within a securities portfolio based upon instructions from an investment advisor).

(b) *Examples*—(1) *Example 1.* A U.S. company engages in a data transaction to transfer personal financial data in bulk to a financial institution that is incorporated in, located in, or subject to the jurisdiction or control of a country of concern to clear and settle electronic payment transactions between U.S. individuals and merchants in a country of concern where both the U.S. individuals and the merchants use the

U.S. company’s infrastructure, such as an e-commerce platform. Both the U.S. company’s transaction transferring bulk personal financial data and the payment transactions by U.S. individuals are exempt transactions.

(2) *Example 2.* As ordinarily incident to and part of securitizing and selling asset-backed obligations (such as mortgage and nonmortgage loans) to a covered person, a U.S. bank provides bulk U.S. sensitive personal data to the covered person. The data transfers are exempt transactions.

(3) *Example 3.* A U.S. bank or other financial institution, as ordinarily incident to and part of facilitating payments to U.S. persons in a country of concern, stores and processes the customers’ bulk financial data using a data center operated by a third-party service provider in the country of concern. The use of this third-party service provider is a vendor agreement, but it is an exempt transaction that is ordinarily incident to and part of facilitating payment.

(4) *Example 4.* Same as Example 3, but the underlying payments are between U.S. persons in the United States and do not involve a country of concern. The use of this third-party service provider is a vendor agreement, but it is not an exempt transaction because it is not ordinarily incident to facilitating this type of financial activity.

(5) *Example 5.* As part of operating an online marketplace for the purchase and sale of goods, a U.S. company, as ordinarily incident to and part of U.S. consumers’ purchase of goods on that marketplace, transfers bulk contact information, payment information (e.g., credit-card account number, expiration data, and security code), and delivery address to a merchant in a country of concern. The data transfers are exempt transactions because they are ordinarily incident to and part of U.S. consumers’ purchase of goods.

(6) *Example 6.* A U.S. investment adviser purchases securities of a company incorporated in a country of concern for the accounts of its clients. The investment adviser engages a broker-dealer located in a country of concern to execute the trade, and, as ordinarily incident to and part of the transaction, transfers to the broker-dealer its clients’ covered personal identifiers and financial account numbers in bulk. This provision of data is an exempt transaction because it is ordinarily incident to and part of the provision of investment-management services.

(7) *Example 7.* A U.S. company that provides payment-processing services

sells bulk U.S. sensitive personal data to a covered person. This sale is prohibited data brokerage and is not an exempt transaction because it is not ordinarily incident to and part of the payment-processing services provided by the U.S. company.

(8) *Example 8.* A U.S. bank facilitates international funds transfers to foreign persons not related to a country of concern, but through intermediaries or locations subject to the jurisdiction or control of a country of concern. These transfers result in access to bulk financial records by some covered persons to complete the transfers and manage associated risks. Providing this access as part of these transfers is ordinarily incident to the provision of financial services and is exempt.

(9) *Example 9.* A U.S. insurance company underwrites personal insurance to U.S. persons residing in foreign countries in the same region as a country of concern. The insurance company relies on its own business infrastructure and personnel in the country of concern to support its financial activity in the region, which results in access to the bulk sensitive personal data of some U.S.-person customers residing in the region, to covered persons at the insurance company supporting these activities. Providing this access is ordinarily incident to the provision of financial services and is exempt.

(10) *Example 10.* A U.S. bank operates a foreign branch in a country of concern and provides financial services to U.S. persons living within the country of concern. The bank receives a lawful request from the regulator in the country of concern to review the financial activity conducted in the country, which includes providing access to the bulk sensitive personal data of U.S. persons resident in the country or U.S. persons conducting transactions through the foreign branch. Responding to the regulator’s request, including providing access to this bulk sensitive personal data, is ordinarily incident to the provision of financial services and is exempt.

(11) *Example 11.* A U.S. bank voluntarily shares information, including relevant bulk sensitive personal data, with financial institutions organized under the laws of a country of concern for the purposes of, and consistent with industry practices for, fraud identification, combatting money laundering and terrorism financing, and U.S. sanctions compliance. Sharing this data for these purposes is ordinarily incident to the provision of financial services and is exempt.

(12) *Example 12.* A U.S. company provides wealth-management services and collects bulk personal financial data on its U.S. clients. The U.S. company appoints a citizen of a country of concern, who is located in a country of concern, to its board of directors. In connection with the board's data security and cybersecurity responsibilities, the director could access the bulk personal financial data. The appointment of the director, who is a covered person, is a restricted employment agreement and is not exempt because the board member access to the bulk personal financial data is not ordinarily incident to the U.S. company's provision of wealth-management services.

§ 202.506 Corporate group transactions.

(a) Subparts C and D of this part do not apply to data transactions to the extent they are:

(1) Between a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control of) a country of concern; and

(2) Ordinarily incident to and part of administrative or ancillary business operations, including:

- (i) Human resources;
- (ii) Payroll, expense monitoring and reimbursement, and other corporate financial activities;
- (iii) Paying business taxes or fees;
- (iv) Obtaining business permits or licenses;
- (v) Sharing data with auditors and law firms for regulatory compliance;
- (vi) Risk management;
- (vii) Business-related travel;
- (viii) Customer support;
- (ix) Employee benefits; and
- (x) Employees' internal and external communications.

(b) *Examples—*(1) *Example 1.* A U.S. company has a foreign subsidiary located in a country of concern, and the U.S. company's U.S.-person contractors perform services for the foreign subsidiary. As ordinarily incident to and part of the foreign subsidiary's payments to the U.S.-person contractors for those services, the U.S. company engages in a data transaction that gives the subsidiary access to the U.S.-person contractors' bulk personal financial data and covered personal identifiers. This is an exempt corporate group transaction.

(2) *Example 2.* A U.S. company aggregates bulk personal financial data. The U.S. company has a subsidiary that is a covered person because it is headquartered in a country of concern. The subsidiary is subject to the country of concern's national security laws requiring it to cooperate with and assist

the country's intelligence services. The exemption for corporate group transactions would not apply to the U.S. parent's grant of a license to the subsidiary to access the parent's databases containing the bulk personal financial data for the purpose of complying with a request or order by the country of concern under those national security laws to provide access to that data because granting of such a license is not ordinarily incident to and part of administrative or ancillary business operations.

(3) *Example 3.* A U.S. company's affiliate operates a manufacturing facility in a country of concern for one of the U.S. company's products. The affiliate uses employee fingerprints as part of security and identity verification to control access to that facility. To facilitate its U.S. employees' access to that facility as part of their job responsibilities, the U.S. company provides the fingerprints of those employees in bulk to its affiliate. The transaction is an exempt corporate group transaction.

(4) *Example 4.* A U.S. company has a foreign subsidiary located in a country of concern that conducts research and development for the U.S. company. The U.S. company sends bulk personal financial data to the subsidiary for the purpose of developing a financial software tool. The transaction is not an exempt corporate group transaction because it is not ordinarily incident to and part of administrative or ancillary business operations.

(5) *Example 5.* Same as Example 4, but the U.S. company has a foreign branch located in a country of concern instead of a foreign subsidiary. Because the foreign branch is a U.S. person as part of the U.S. company, the transaction occurs within the same U.S. person and is not subject to the prohibitions or restrictions. If the foreign branch allows employees who are covered persons to access the bulk personal financial data to develop the financial software tool, the foreign branch has engaged in restricted transactions.

§ 202.507 Transactions required or authorized by Federal law or international agreements, or necessary for compliance with Federal law.

(a) *Required or authorized by Federal law or international agreements.* Subparts C and D of this part do not apply to data transactions to the extent they are required or authorized by Federal law or pursuant to an international agreement to which the United States is a party, including relevant provisions in the following:

(1) Annex 9 to the Convention on International Civil Aviation, International Civil Aviation Organization Doc. 7300 (2022);

(2) Section 2 of the Convention on Facilitation of International Maritime Traffic (1965);

(3) Articles 1, 12, 14, and 16 of the Postal Payment Services Agreement (2021);

(4) Articles 63, 64, and 65 of the Constitution of the World Health Organization (1946);

(5) Article 2 of the Agreement Between the Government of the United States of America and the Government of the People's Republic of China Regarding Mutual Assistance in Customs Matters (1999);

(6) Article 7 of the Agreement Between the Government of the United States of America and the Government of the People's Republic of China on Mutual Legal Assistance in Criminal Matters (2000);

(7) Article 25 of the Agreement Between the Government of the United States of America and the Government of the People's Republic of China for the Avoidance of Double Taxation and the Prevention of Tax Evasion with Respect to Taxes on Income (1987);

(8) Article 2 of the Agreement Between the United States of America and the Macao Special Administrative Region of the People's Republic of China for Cooperation to Facilitate the Implementation of FATCA (2021);

(9) Articles II, III, VII of the Protocol to Extend and Amend the Agreement Between the Department of Health and Human Services of the United States of America and the National Health and Family Planning Commission of the People's Republic of China for Cooperation in the Science and Technology of Medicine and Public Health (2013);

(10) Article III of the Treaty Between the United States and Cuba for the Mutual Extradition of Fugitives from Justice (1905);

(11) Articles 3, 4, 5, 7 of the Agreement Between the Government of the United States of America and the Government of the Russian Federation on Cooperation and Mutual Assistance in Customs Matters (1994);

(12) Articles 1, 2, 5, 7, 13, and 16 of the Treaty Between the United States of America and the Russian Federation on Mutual Legal Assistance in Criminal Matters (1999);

(13) Articles I, IV, IX, XV, and XVI of the Treaty Between the Government of the United States of America and the Government of the Republic of Venezuela on Mutual Legal Assistance in Criminal Matters (1997); and

(14) Articles 5, 6, 7, 9, 11, 19, 35, and 45 of the International Health Regulations (2005).

(b) *Global health and pandemic preparedness.* Subparts C and D of this part do not apply to data transactions to the extent they are required or authorized by the following:

(1) The Pandemic Influenza Preparedness and Response Framework;

(2) The Global Influenza Surveillance and Response System; and

(3) The Agreement between the Government of the United States of America and the Government of the People's Republic of China on Cooperation in Science and Technology (1979).

(c) *Compliance with Federal law.* Subparts C and D of this part do not apply to data transactions to the extent that they are ordinarily incident to and part of ensuring compliance with any Federal laws and regulations, including the Bank Secrecy Act, 12 U.S.C. 1829b, 1951 through 1960, 31 U.S.C. 310, 5311 through 5314, 5316 through 5336; the Securities Act of 1933, 15 U.S.C. 77a *et seq.*; the Securities Exchange Act of 1934, 15 U.S.C. 78a *et seq.*; the Investment Company Act of 1940, 15 U.S.C. 80a–1 *et seq.*; the Investment Advisers Act of 1940, 15 U.S.C. 80b–1 *et seq.*; the International Emergency Economic Powers Act, 50 U.S.C. 1701 *et seq.*; the Export Administration Regulations, 15 CFR 730 *et seq.*; or any notes, guidance, orders, directives, or additional regulations related thereto.

(d) *Examples*—(1) *Example 1.* A U.S. bank or other financial institution engages in a covered data transaction with a covered person that is ordinarily incident to and part of ensuring compliance with U.S. laws and regulations (such as OFAC sanctions and anti-money laundering programs required by the Bank Secrecy Act). This is an exempt transaction.

(2) [Reserved]

§ 202.508 Investment agreements subject to a CFIUS action.

(a) *Exemption.* Subparts C and D of this part do not apply to data transactions to the extent that they involve an investment agreement that is subject to a CFIUS action.

(b) *Examples*—(1) *Example 1.* A U.S. software provider is acquired in a CFIUS covered transaction by a foreign entity in which the transaction parties sign a mitigation agreement with CFIUS. The agreement has provisions governing the acquirer's ability to access the data of the U.S. software provider and their customers. The mitigation agreement contains a provision stating that it is a CFIUS action for purposes of this part.

Before the effective date of the CFIUS mitigation agreement, the investment agreement is not subject to a CFIUS action and remains subject to these regulations to the extent otherwise applicable. Beginning on the effective date of the CFIUS mitigation agreement, the investment agreement is subject to a CFIUS action and exempt from this part.

(2) *Example 2.* Same as Example 1, but CFIUS issues an interim order before entering a mitigation agreement. The interim order states that it constitutes a CFIUS action for purposes of this part. Before the effective date of the interim order, the investment agreement is not subject to a CFIUS action and remains subject to these regulations to the extent otherwise applicable. Beginning on the effective date of the interim order, the investment agreement is subject to a CFIUS action and is exempt from this part. The mitigation agreement also states that it constitutes a CFIUS action for purposes of this part. After the effective date of the mitigation agreement, the investment agreement remains subject to a CFIUS action and is exempt from this part.

(3) *Example 3.* A U.S. biotechnology company is acquired by a foreign multinational corporation. CFIUS reviews this acquisition and concludes action without mitigation. This acquisition is not subject to a CFIUS action, and the acquisition remains subject to this part to the extent otherwise applicable.

(4) *Example 4.* A U.S. manufacturer is acquired by a foreign owner in which the transaction parties sign a mitigation agreement with CFIUS. The mitigation agreement provides for supply assurances and physical access restrictions but does not address data security, and it does not contain a provision explicitly designating that it is a CFIUS action. This acquisition is not subject to a CFIUS action, and the acquisition remains subject to this part to the extent otherwise applicable.

(5) *Example 5.* As a result of CFIUS's review and investigation of a U.S. human genomic company's acquisition by a foreign healthcare company, CFIUS refers the transaction to the President with a recommendation to require the foreign acquirer to divest its interest in the U.S. company. The President issues an order prohibiting the transaction and requiring divestment of the foreign healthcare company's interests and rights in the human genomic company. The presidential order itself does not constitute a CFIUS action. Unless CFIUS takes action, such as by entering into an agreement or imposing conditions to address risk prior to completion of the

divestment, the transaction remains subject to this part to the extent otherwise applicable for as long as the investment agreement remains in existence following the presidential order and prior to divestment.

(6) *Example 6.* A U.S. healthcare company and foreign acquirer announce a transaction that they believe will be subject to CFIUS jurisdiction and disclose that they intend to file a joint voluntary notice soon. No CFIUS action has occurred yet, and the transaction remains subject to this part to the extent otherwise applicable.

(7) *Example 7.* Same as Example 6, but the transaction parties file a joint voluntary notice with CFIUS. No CFIUS action has occurred yet, and the transaction remains subject to this part to the extent otherwise applicable.

(8) *Example 8.* Company A, a covered person, acquires 100% of the equity and voting interest of Company B, a U.S. business that maintains bulk U.S. sensitive personal data of U.S. persons. After completing the transaction, the parties fail to implement the security requirements and other conditions required under this part. Company A and Company B later submit a joint voluntary notice to CFIUS with respect to the transaction. Upon accepting the notice, CFIUS determines that the transaction is a covered transaction and takes measures to mitigate interim risk that may arise as a result of the transaction until such time that the Committee has completed action, pursuant to 50 U.S.C. 4565(l)(3)(A)(iii). The interim order states that it constitutes a CFIUS action for purposes of this part. Beginning on the effective date of these measures imposed by the interim order, the security requirements and other applicable conditions under this part no longer apply to the transaction. The Department of Justice, however, may take enforcement action under this part, in coordination with CFIUS, with respect to the violations that occurred before the effective date of the interim order issued by CFIUS.

(9) *Example 9.* Same as Example 8, but before engaging in the investment agreement for the acquisition, Company A and Company B submit the joint voluntary notice to CFIUS. CFIUS determines that the transaction is a CFIUS covered transaction. CFIUS identifies a risk related to data security arising from the transaction, and CFIUS negotiates and enters into a mitigation agreement with the parties to resolve that risk. The mitigation agreement contains a provision stating that it is a CFIUS action for purposes of this part. Because a CFIUS action has occurred before the parties engage in the

investment agreement, the acquisition is exempt from this part.

(10) *Example 10.* Same as Example 8, but before engaging in the investment agreement for the acquisition, the parties implement the security requirements and other conditions required under these regulations. Company A and Company B then submit a joint voluntary notice to CFIUS, which determines that the transaction is a CFIUS covered transaction. CFIUS identifies a risk related to data security arising from the transaction but determines that the regulations in this part adequately resolve the risk. CFIUS concludes action with respect to the transaction without taking any CFIUS action. Because no CFIUS action has occurred, the transaction remains subject to this part.

(11) *Example 11.* Same facts as Example 10, but CFIUS determines that the security requirements and other conditions applicable under this part are inadequate to resolve the national security risk identified by CFIUS. CFIUS negotiates a mitigation agreement with the parties to resolve the risk, which contains a provision stating that it is a CFIUS action for purposes of this part. The transaction is exempt from this part beginning on the effective date of the CFIUS mitigation agreement.

§ 202.509 Telecommunications services.

(a) *Exemption.* Subparts C and D of this part do not apply to data transactions, other than those involving data brokerage, to the extent that they are ordinarily incident to and part of the provision of telecommunications services, including international calling, mobile voice, and data roaming.

(b) *Examples*—(1) *Example 1.* A U.S. telecommunications service provider collects covered personal identifiers from its U.S. subscribers. Some of those subscribers travel to a country of concern and use their mobile phone service under an international roaming agreement. The local telecommunications service provider in the country of concern shares these covered personal identifiers with the U.S. service provider for the purposes of either helping provision service to the U.S. subscriber or receiving payment for the U.S. subscriber's use of the country of concern service provider's network under that international roaming agreement. The U.S. service provider provides the country of concern service provider with network or device information for the purpose of provisioning services and obtaining payment for its subscribers' use of the local telecommunications service provider's network. Over the course of

12 months, the volume of network or device information shared by the U.S. service provider with the country of concern service provider for the purpose of provisioning services exceeds the applicable bulk threshold. These transfers of bulk U.S. sensitive personal data are ordinarily incident to and part of the provision of telecommunications services and are thus exempt transactions.

(2) *Example 2.* A U.S. telecommunications service provider collects precise geolocation data on its U.S. subscribers. The U.S. telecommunications service provider sells this precise geolocation data in bulk to a covered person for the purpose of targeted advertising. This sale is not ordinarily incident to and part of the provision of telecommunications services and remains a prohibited transaction.

§ 202.510 Drug, biological product, and medical device authorizations.

(a) *Exemption.* Subparts C and D of this part do not apply to a data transaction that

(1) Involves “regulatory approval data” as defined in this section and

(2) Is necessary to obtain or maintain regulatory approval to market a drug, biological product, device, or a combination product in a country of concern, provided that the U.S. person complies with the recordkeeping and reporting requirements set forth in §§ 202.1101(a) and 202.1102 with respect to such transaction.

(b) *Regulatory approval data.* For purposes of this section, the term *regulatory approval data* means de-identified sensitive personal data that is required to be submitted to a country of concern regulatory entity to obtain or maintain authorization or approval to research or market a drug, biological product, device, or combination product, including in relation to post-marketing studies and post-marketing product surveillance activities, and supplemental product applications for additional uses. The term excludes sensitive personal data not reasonably necessary for a regulatory entity to assess the safety and effectiveness of the drug, biological product, device, or combination product.

(c) *Other terms.* For purposes of this section, the terms “drug,” “biological product,” “device,” and “combination product” have the meanings given to them in 21 U.S.C. 321(g)(1), 42 U.S.C. 262(i)(1), 21 U.S.C. 321(h)(1), and 21 CFR 3.2(e), respectively.

(d) *Examples*—(1) *Example 1.* A U.S. pharmaceutical company seeks to market a new drug in a country of

concern. The company submits a marketing application to the regulatory entity in the country of concern with authority to approve the drug in the country of concern. The marketing application includes the safety and effectiveness data reasonably necessary to obtain regulatory approval in that country. The transfer of data to the country of concern's regulatory entity is exempt from the prohibitions in this part.

(2) *Example 2.* Same as Example 1, except the regulatory entity in the country of concern requires that the data be de-anonymized. The transfer of data is not exempt under this section, because the data includes sensitive personal data that is identified to an individual.

(3) *Example 3.* Same as Example 1, except the U.S. company enters a vendor agreement with a covered person located in the country of concern to store, organize, and prepare the bulk U.S. sensitive personal data for submission to the regulatory agency. The transaction is not exempt under this section, because the use of a covered person to prepare the regulatory submission is not necessary to obtain regulatory approval.

§ 202.511 Other clinical investigations and post-marketing surveillance data.

(a) *Exemption.* Subparts C and D of this part do not apply to data transactions to the extent that those transactions are:

(1) Ordinarily incident to and part of clinical investigations regulated by the U.S. Food and Drug Administration (“FDA”) under sections 505(i) and 520(g) of the Federal Food, Drug, and Cosmetic Act (“FD&C Act”) or clinical investigations that support applications to the FDA for research or marketing permits for drugs, biological products, devices, combination products, or infant formula; or

(2) Ordinarily incident to and part of the collection or processing of clinical care data indicating real-world performance or safety of products, or the collection or processing of post-marketing surveillance data (including pharmacovigilance and post-marketing safety monitoring), and necessary to support or maintain authorization by the FDA, provided the data is deidentified.

(b) [Reserved]

Subpart F—Determination of Countries of Concern

§ 202.601 Determination of countries of concern.

(a) *Countries of concern.* Solely for purposes of the Order and this part, the

Attorney General has determined, with the concurrence of the Secretaries of State and Commerce, that the following foreign governments have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of U.S. persons and pose a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or security and safety of U.S. persons:

- (1) China;
- (2) Cuba;
- (3) Iran;
- (4) North Korea;
- (5) Russia; and
- (6) Venezuela.

(b) *Effective date of amendments.* Any amendment to the list of countries of concern will apply to any covered data transaction that is initiated, pending, or completed on or after the effective date of the amendment.

Subpart G—Covered Persons

§ 202.701 Designation of covered persons.

(a) *Designations.* The Attorney General may designate any person as a covered person for purposes of this part if, after consultation with other agencies as the Attorney General deems appropriate, the Attorney General determines the person meets any of the criteria set forth in § 202.211(a)(5) of this part.

(b) *Information considered.* In determining whether to designate a person as a covered person, the Attorney General may consider any information or material the Attorney General deems relevant and appropriate, classified or unclassified, from any Federal department or agency or from any other source.

(c) *Covered Persons List.* The names of persons designated as a covered person for purposes of this part, transactions with whom are prohibited or restricted pursuant to this part, are published in the **Federal Register** and incorporated into the National Security Division's Covered Persons List. The Covered Persons List is accessible through the following page on the National Security Division's website at <https://www.justice.gov/nsd>.

(d) *Non-exhaustive.* The list of designated covered persons described in this section is not exhaustive of all covered persons and supplements the categories in the definition of covered persons in § 202.211.

(e) *Effective date; actual and constructive knowledge.* (1) Designation as a covered person will be effective

from the date of any public announcement by the Department. Except as otherwise authorized in this part, a U.S. person with actual knowledge of a designated person's status is prohibited from knowingly engaging in a covered data transaction with that person on or after the date of the Department's public announcement.

(2) Publication in the **Federal Register** is deemed to provide constructive knowledge of a person's status as a covered person.

§ 202.702 Procedures governing removal from the Covered Persons List.

(a) *Requests for removal from the Covered Persons List.* A person may petition to seek administrative reconsideration of their designation, or may assert that the circumstances resulting in the designation no longer apply, and thus seek to be removed from the Covered Persons List pursuant to the following administrative procedures:

(b) *Content of requests.* A covered person designated under paragraph (a) of this section may submit arguments or evidence that the person believes establish that insufficient basis exists for the designation. Such a person also may propose remedial steps on the person's part, such as corporate reorganization, resignation of persons from positions in a listed entity, or similar steps, that the person believes would negate the basis for designation.

(c) *Additional content; form and method of submission.* Requests for removal from the Covered Persons List must be submitted in accordance with this section and with subpart L of this part.

(d) *Requests for more information.* The information submitted by the listed person seeking removal will be reviewed by the Attorney General, who may request clarifying, corroborating, or other additional information.

(e) *Meetings.* A person seeking removal may request a meeting with the Attorney General; however, such meetings are not required, and the Attorney General may, in the Attorney General's discretion, decline to conduct such a meeting prior to completing a review pursuant to this section.

(f) *Decisions.* After the Attorney General has conducted a review of the request for removal, and after consultation with other agencies as the Attorney General deems appropriate, the Attorney General will provide a written decision to the person seeking removal. A covered person's status as a covered person—including its associated prohibitions and restrictions under this part—remains in effect during the pendency of any request to

be removed from the Covered Persons List.

Subpart H—Licensing

§ 202.801 General licenses.

(a) *General course of procedure.* The Department may, as appropriate, issue general licenses to authorize, under appropriate terms and conditions, transactions that are subject to the prohibitions or restrictions in this part. In determining whether to issue a general license, the Attorney General may consider any information or material the Attorney General deems relevant and appropriate, classified or unclassified, from any Federal department or agency or from any other source.

(b) *Relationship with specific licenses.* It is the policy of the Department not to grant applications for specific licenses authorizing transactions to which the provisions of a general license are applicable.

(c) *Reports.* Persons availing themselves of certain general licenses may be required to file reports and statements in accordance with the instructions specified in those licenses, this part or the Order. Failure to file timely all required information in such reports or statements may nullify the authorization otherwise provided by the general license and result in apparent violations of the applicable prohibitions that may be subject to enforcement action.

§ 202.802 Specific licenses.

(a) *General course of procedure.* Transactions subject to the prohibitions or restrictions in this part or the Order, and that are not otherwise permitted under this part or a general license, may be permitted only under a specific license, under appropriate terms and conditions.

(b) *Content of applications for specific licenses.* Applications for specific licenses shall include, at a minimum, a description of the nature of the transaction, including each of the following requirements:

(1) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transactions;

(2) The identity of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals;

(3) The end-use of the data and the method of data transfer; and

(4) Any other information that the Attorney General may require.

(c) *Additional content; form and method of submissions.* Requests for

specific licenses must be submitted in accordance with this section and with subpart L of this part.

(d) *Additional conditions.* Applicants should submit only one copy of a specific license application to the Department; submitting multiple copies may result in processing delays. Any person having an interest in a transaction or proposed transaction may file an application for a specific license authorizing such a transaction.

(e) *Further information to be supplied.* Applicants may be required to furnish such further information as the Department deems necessary to assist in making a determination. Any applicant or other party-in-interest desiring to present additional information concerning a specific license application may do so at any time before or after the Department makes its decision with respect to the application. In unique circumstances, the Department may determine, in its discretion, that an oral presentation regarding a license application would assist in the Department's review of the issues involved. Any requests to make such an oral presentation must be submitted electronically by emailing the National Security Division at NSD.FIRS.datasecurity@usdoj.gov or using another official method to make such requests, in accordance with any instructions on the National Security Division's website.

(f) *Decisions.* In determining whether to issue a specific license, the Attorney General may consider any information or material the Attorney General deems relevant and appropriate, classified or unclassified, from any Federal department or agency or from any other source. The Department will advise each applicant of the decision respecting the applicant's filed application. The Department's decision with respect to a license application shall constitute final agency action.

(g) *Time to issuance.* The Department shall endeavor to respond to any request for a specific license within 45 days after receipt of the request and of any requested additional information and documents.

(h) *Scope.* (1) Unless otherwise specified in the license, a specific license authorizes the transaction:

(i) Only between the parties identified in the license;

(ii) Only with respect to the data described in the license; and

(iii) Only to the extent the conditions specified in the license are satisfied. The applicant must inform any other parties identified in the license of the license's scope and of the specific conditions applicable to them.

(2) The Department will determine whether to grant specific licenses in reliance on representations the applicant made or submitted in connection with the license application, letters of explanation, and other documents submitted. Any license obtained based on a false or misleading representation in the license application, in any document submitted in connection with the license application, or during an oral presentation under this section shall be deemed void as of the date of issuance.

(i) *Reports under specific licenses.* As a condition for the issuance of any specific license, the licensee may be required to file reports or statements with respect to the transaction or transactions authorized by the specific license in such form and at such times as may be prescribed in the license. Failure to file timely all required information in such reports or statements may nullify the authorization otherwise provided by the specific license and result in apparent violations of the applicable prohibitions that may be subject to enforcement action.

(j) *Effect of denial.* The denial of a specific license does not preclude the reconsideration of an application or the filing of a further application. The applicant or any other party-in-interest may at any time request, by written correspondence, reconsideration of the denial of an application based on new facts or changed circumstances.

§ 202.803 General provisions.

(a) *Effect of license.* (1) No license issued under this subpart, or otherwise issued by the Department, authorizes or validates any transaction effected prior to the issuance of such license or other authorization, unless specifically provided for in such license or authorization.

(2) No license issued under this subpart authorizes or validates any transaction prohibited under or subject to this part unless the license is properly issued by the Department and specifically refers to this part.

(3) Any license authorizing or validating any transaction that is prohibited under or otherwise subject to this part has the effect of removing or amending those prohibitions or other requirements from the transaction, but only to the extent specifically stated by the terms of the license. Unless the license otherwise specifies, such an authorization does not create any right, duty, obligation, claim, or interest in, or with respect to, any property that would not otherwise exist under ordinary principles of law.

(4) Nothing contained in this part shall be construed to supersede the requirements established under any other provision of law or to relieve a person from any requirement to obtain a license or authorization from another department or agency of the United States Government in compliance with applicable laws and regulations subject to the jurisdiction of that department or agency. For example, issuance of a specific license authorizing a transaction otherwise prohibited by this part does not operate as a license or authorization to conclude the transaction that is otherwise required from the U.S. Department of Commerce, U.S. Department of State, U.S. Department of the Treasury, or any other department or agency of the United States Government.

(b) *Amendment, modification, or rescission.* Except as otherwise provided by law, any licenses (whether general or specific), authorizations, instructions, or forms issued thereunder may be amended, modified, or rescinded at any time.

(c) *Consultation.* The Department will issue, amend, modify, or rescind a general or specific license in concurrence with the Departments of State, Commerce, and Homeland Security and in consultation with other relevant agencies.

(d) *Exclusion from licenses and other authorizations.* The Attorney General reserves the right to exclude any person, property, or transaction from the operation of any license or from the privileges conferred by any license. The Attorney General also reserves the right to restrict the applicability of any license to particular persons, property, transactions, or classes thereof. Such actions are binding upon all persons receiving actual or constructive notice of the exclusions or restrictions.

Subpart I—Advisory Opinions

§ 202.901 Inquiries concerning application of this part.

(a) *General.* Any U.S. person party to a transaction potentially regulated under the Order and this part, or an agent of the party to such a transaction on the party's behalf, may request from the Attorney General a statement of the present enforcement intentions of the Department of Justice under the Order with respect to that transaction that may be subject to the prohibitions or restrictions in the Order and this part ("advisory opinion").

(b) *Anonymous, hypothetical, non-party and ex post facto review requests excluded.* The entire transaction that is the subject of the advisory opinion

request must be an actual, as opposed to hypothetical, transaction and involve disclosed, as opposed to anonymous, parties to the transaction. Advisory opinion requests must be submitted by a U.S. person party to the transaction or that party's agent and have no application to a party that does not join the request. The transaction need not involve only prospective conduct, but an advisory opinion request will not be considered unless that portion of the transaction for which an opinion is sought involves only prospective conduct.

(c) *Contents.* Each advisory opinion request shall be specific and must be accompanied by all material information bearing on the conduct for which an advisory opinion is requested, and on the circumstances of the prospective conduct, including background information, complete copies of any and all operative documents, and detailed statements of all collateral or oral understandings, if any. Each request must include, at a minimum:

(1) The identities of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals;

(2) A description of the nature of the transaction, including the types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction, the end-use of the data, the method of data transfer, and any restrictions or requirements related to a party's right or ability to control, access, disseminate, or dispose of the data; and

(3) Any potential basis for exempting or excluding the transaction from the prohibitions or restrictions imposed in the Order and this part.

(d) *Additional contents; format and method of submissions.* Requests for advisory opinions must be submitted in accordance with this section and with subpart L of this part.

(e) *Further information to be supplied.* Each party shall provide any additional information or documents that the Department of Justice may thereafter request in its review of the matter. Any information furnished orally shall be confirmed promptly in writing; signed by or on behalf of the party that submitted the initial review request; and certified to be a true, correct, and complete disclosure of the requested information. A request will not be deemed complete until the Department of Justice receives such additional information. In connection with an advisory opinion request, the Department of Justice may conduct any

independent investigation it believes appropriate.

(f) *Outcomes.* After submission of an advisory opinion request, the Department, in its discretion, may state its present enforcement intention under the Order and this part with respect to the proposed conduct; may decline to state its present enforcement intention; or, if circumstances warrant, may take such other position or initiate such other action as it considers appropriate. Any requesting party or parties may withdraw a request at any time prior to issuance of an advisory opinion. The Department remains free, however, to submit such comments to the requesting party or parties as it deems appropriate. Failure to take action after receipt of a request, documents, or information, whether submitted pursuant to this procedure or otherwise, shall not in any way limit or stop the Department from taking any action at such time thereafter as it deems appropriate. The Department reserves the right to retain any advisory opinion request, document, or information submitted to it under this procedure or otherwise, to disclose any advisory opinion and advisory opinion request, including the identities of the requesting party and foreign parties to the transaction, the general nature and circumstances of the proposed conduct, and the action of the Department in response to any advisory opinion request, consistent with applicable law, and to use any such request, document, or information for any governmental purpose.

(g) *Time for response.* The Department shall endeavor to respond to any advisory opinion request within 30 days after receipt of the request and of any requested additional information and documents.

(h) *Written decisions only.* The requesting party or parties may rely only upon a written advisory opinion signed by the Attorney General.

(i) *Effect of advisory opinion.* Each advisory opinion can be relied upon by the requesting party or parties to the extent the disclosures made pursuant to this subpart were accurate and complete and to the extent the disclosures continue accurately and completely to reflect circumstances after the date of the issuance of the advisory opinion. An advisory opinion will not restrict enforcement actions by any agency other than the Department of Justice. It will not affect a requesting party's obligations to any other agency or under any statutory or regulatory provision other than those specifically discussed in the advisory opinion.

(j) *Amendment or revocation of advisory opinion.* An advisory opinion

may be amended or revoked at any time after it has been issued. Notice of such will be given in the same manner as notice of the advisory opinion was originally given or in the **Federal Register**. Whenever possible, a notice of amendment or revocation will state when the Department will consider a party's reliance on the superseded advisory opinion to be unreasonable, and any transition period that may be applicable.

(k) *Compliance.* Neither the submission of an advisory opinion request, nor its pendency, shall in any way alter the responsibility or obligation of a requesting party to comply with the Order, this part, or any other applicable law.

Subpart J—Due Diligence and Audit Requirements

§ 202.1001 Due diligence for restricted transactions.

(a) *Data compliance program.* By the effective date of this part, U.S. persons engaging in any restricted transactions shall develop and implement a data compliance program.

(b) *Requirements.* The data compliance program shall include, at a minimum, each of the following requirements:

(1) Risk-based procedures for verifying data flows involved in any restricted transaction, including procedures to verify and log, in an auditable manner, the following:

(i) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;

(ii) The identity of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals; and

(iii) The end-use of the data and the method of data transfer;

(2) For restricted transactions that involve vendors, risk-based procedures for verifying the identity of vendors;

(3) A written policy that describes the data compliance program and that is annually certified by an officer, executive, or other employee responsible for compliance;

(4) A written policy that describes the implementation of the security requirements as defined in § 202.248 of this part and that is annually certified by an officer, executive, or other employee responsible for compliance; and

(5) Any other information that the Attorney General may require.

§ 202.1002 Audits for restricted transactions.

(a) *Audit required.* U.S. persons that engage in any restricted transactions under § 202.401 of this part shall conduct an audit that complies with the requirements of this section.

(b) *Who may conduct the audit.* The auditor:

(1) Must be qualified and competent to examine, verify, and attest to the U.S. person's compliance with and the effectiveness of the security requirements, as defined in § 202.248 of this part, and all other applicable requirements, as defined in § 202.401 of this part, implemented for restricted transactions;

(2) Must be independent and external; and

(3) Cannot be a covered person or a country of concern.

(c) *When required.* The audit must be performed once for each calendar year in which the U.S. person engages in any restricted transactions.

(d) *Timeframe.* The audit must cover the preceding 12 months.

(e) *Scope.* The audit must:

(1) Examine the U.S. person's data transactions;

(2) Examine the U.S. person's data compliance program required under § 202.1001 of this part and its implementation;

(3) Examine relevant records required under § 202.1101 of this part;

(4) Examine the U.S. person's security requirements, as defined by § 202.248 of this part; and

(5) Use a reliable methodology to conduct the audit.

(f) *Report.* (1) The auditor must prepare and submit a written report to the U.S. person within 60 days of the completion of the audit.

(2) The audit report must:

(i) Describe the nature of any prohibited transactions, restricted transactions, and exempt transactions engaged in by the U.S. person;

(ii) Describe the methodology undertaken, including the policies and other documents reviewed, personnel interviewed, and any facilities, equipment, networks, or systems examined;

(iii) Describe the effectiveness of the U.S. person's data compliance program and its implementation;

(iv) Describe any vulnerabilities or deficiencies in the implementation of the security requirements that have affected or could affect access to government-related data or bulk U.S. sensitive personal data by a country of concern or covered person;

(v) Describe any instances in which the security requirements failed or were

otherwise not effective in mitigating access to government-related data or bulk U.S. sensitive personal data by a country of concern or covered person; and

(vi) Recommend any improvements or changes to policies, practices, or other aspects of the U.S. person's business to ensure compliance with the security requirements.

(3) U.S. persons engaged in restricted transactions must retain the audit report for a period of at least 10 years, consistent with the recordkeeping requirements in § 202.1101.

Subpart K—Reporting and Recordkeeping Requirements**§ 202.1101 Records and recordkeeping requirements.**

(a) *Records.* Except as otherwise provided, U.S. persons engaging in any transaction subject to the provisions of this part shall keep a full and accurate record of each such transaction engaged in, and such record shall be available for examination for at least 10 years after the date of such transaction.

(b) *Additional recordkeeping requirements.* U.S. persons engaging in any restricted transaction shall create and maintain, at a minimum, the following records in an auditable manner:

(1) A written policy that describes the data compliance program and that is certified annually by an officer, executive, or other employee responsible for compliance;

(2) A written policy that describes the implementation of any applicable security requirements as defined in § 202.248 of this part and that is certified annually by an officer, executive, or other employee responsible for compliance;

(3) The results of any annual audits that verify the U.S. person's compliance with the security requirements and any conditions on a license;

(4) Documentation of the due diligence conducted to verify the data flow involved in any restricted transaction, including:

(i) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;

(ii) The identity of the transaction parties, including any direct and indirect ownership of entities or citizenship or primary residence of individuals; and

(iii) A description of the end-use of the data;

(5) Documentation of the method of data transfer;

(6) Documentation of the dates the transaction began and ended;

(7) Copies of any agreements associated with the transaction;

(8) Copies of any relevant licenses or advisory opinions;

(9) The document reference number for any original document issued by the Attorney General, such as a license or advisory opinion;

(10) A copy of any relevant documentation received or created in connection with the transaction; and

(11) An annual certification by an officer, executive, or other employee responsible for compliance of the completeness and accuracy of the records documenting due diligence.

§ 202.1102 Reports to be furnished on demand.

(a) *Reports.* Every person is required to furnish under oath, in the form of reports or otherwise, from time to time and at any time as may be required by the Department of Justice, complete information relative to any act or transaction or covered data transaction, regardless of whether such act, transaction, or covered data transaction is effected pursuant to a license or otherwise, subject to the provisions of this part. The Department of Justice may require that such reports include the production of any books, contracts, letters, papers, or other hard copy or electronic documents relating to any such act, transaction, or covered data transaction, in the custody or control of the persons required to make such reports. Reports may be required either before, during, or after such acts, transactions, or covered data transactions. The Department of Justice may, through any person or agency, conduct investigations, hold hearings, administer oaths, examine witnesses, receive evidence, take depositions, and require by subpoena the attendance and testimony of witnesses and the production of any books, contracts, letters, papers, and other hard copy or electronic documents relating to any matter under investigation, regardless of whether any report has been required or filed in connection therewith.

(b) *Definition of the term "document."* For purposes of paragraph (a) of this section, the term *document* includes any written, recorded, or graphic matter or other means of preserving thought or expression (including in electronic format), and all tangible things stored in any medium from which information can be processed, transcribed, or obtained directly or indirectly, including correspondence, memoranda, notes, messages, contemporaneous communications such as text and instant messages, letters, emails, spreadsheets, metadata, contracts,

bulletins, diaries, chronological data, minutes, books, reports, examinations, charts, ledgers, books of account, invoices, air waybills, bills of lading, worksheets, receipts, printouts, papers, schedules, affidavits, presentations, transcripts, surveys, graphic representations of any kind, drawings, photographs, graphs, video or sound recordings, and motion pictures or other film.

(c) *Format.* Persons providing documents to the Department of Justice pursuant to this section must produce documents in a usable format agreed upon by the Department of Justice. For guidance, see the Department of Justice's data delivery standards available on the National Security Division's website at <https://www.justice.gov/nsd>.

§ 202.1103 Annual reports.

(a) *Who must report.* An annual report must be filed by any U.S. person that is engaged in a restricted transaction involving cloud-computing services, and that has 25% or more of the U.S. person's equity interests owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a country of concern or covered person.

(b) *Primary responsibility to report.* A report may be filed on behalf of a U.S. person engaging in the data transaction described in § 202.1103(a) by an attorney, agent, or other person. Primary responsibility for reporting, however, rests with the actual U.S. person engaging in the data transaction. No U.S. person is excused from filing a report by reason of the fact that another U.S. person has submitted a report with regard to the same data transaction, except where the U.S. person has actual knowledge that the other U.S. person filed the report.

(c) *When reports are due.* A report on the data transactions described in § 202.1103(a) engaged in as of December 31 of the previous year shall be filed annually by March 1 of the subsequent year.

(d) *Contents of reports.* Annual reports on the data transactions described in § 202.1103(a) shall include the following:

(1) The name and address of the U.S. person engaging in the covered data transaction, and the name, telephone number, and email address of a contact from whom additional information may be obtained;

(2) A description of the covered data transaction, including:

(i) The date of the transaction;

(ii) The types and volumes of government-related data or bulk U.S.

sensitive personal data involved in the transaction;

(iii) The method of data transfer; and

(iv) Any persons participating in the data transaction and their respective locations, including the name and location of each data recipient, the ownership of entities or citizenship or primary residence of individuals, the name and location of any covered persons involved in the transaction, and the name of any countries of concern involved in the transaction;

(3) A copy of any relevant documentation received or created in connection with the transaction; and

(4) Any other information that the Department of Justice may require.

(e) *Additional contents; format and method of submission.* Reports required by this section must be submitted in accordance with this section and with subpart L of this part.

§ 202.1104 Reports on rejected prohibited transactions.

(a) *Who must report.* A report must be filed by any U.S. person that has received and affirmatively rejected (including automatically rejected using software, technology, or automated tools) an offer from another person to engage in a prohibited transaction involving data brokerage.

(b) *When reports are due.* U.S. persons shall file reports within 14 days of rejecting a transaction prohibited by this part.

(c) *Contents of reports.* Reports on rejected transactions shall include the following, to the extent known and available to the person filing the report at the time the transaction is rejected:

(1) The name and address of the U.S. person that rejected the prohibited transaction, and the name, telephone number, and email address of a contact from whom additional information may be obtained;

(2) A description of the rejected transaction, including:

(i) The date the transaction was rejected;

(ii) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;

(iii) The method of data transfer;

(iv) Any persons attempting to participate in the transaction and their respective locations, including the name and location of each data recipient, the ownership of entities or citizenship or primary residence of individuals, the name and location of any covered persons involved in the transaction, and the name of any countries of concern involved in the transaction;

(v) A copy of any relevant documentation received or created in connection with the transaction; and

(vi) Any other information that the Department of Justice may require.

(d) *Additional contents; format and method of submission.* Reports required by this section must be submitted in accordance with this section and with subpart L of this part.

Subpart L—Submitting Applications, Requests, Reports, and Responses

§ 202.1201 Procedures.

(a) *Application of this subpart.* This subpart applies to any submissions required or permitted by this part, including reports of known or suspected violations submitted pursuant to § 202.302, requests for removal from the Covered Persons List submitted pursuant to subpart G of this part, requests for specific licenses submitted pursuant to § 202.802, advisory opinion requests submitted pursuant to subpart I of this part, annual reports submitted pursuant to § 202.1103, reports on rejected prohibited transactions submitted pursuant to § 202.1104, and responses to pre-penalty notices and findings of violations submitted pursuant to § 202.1306 (collectively, "submissions").

(b) *Form of submissions.* Submissions must follow the instructions in this part and any instructions on the National Security Division's website. With the exception of responses to pre-penalty notices or findings of violations submitted pursuant to subpart M of this part, submissions must use the forms on the National Security Division's website or another official reporting option as specified by the National Security Division.

(c) *Method of submissions.* Submissions must be made to the National Security Division electronically by emailing the National Security Division at NSD.FIRS.datasecurity@usdoj.gov or using another official electronic reporting option, in accordance with any instructions on the National Security Division's website.

(d) *Certification.* If the submitting party is an individual, the submission must be signed by the individual or the individual's attorney. If the submitting party is not an individual, the submission must be signed on behalf of each submitting party by an officer, director, a person performing the functions of an officer or a director of, or an attorney for, the submitting party. Annual reports submitted pursuant to § 202.1103, and reports on rejected transactions submitted pursuant to

§ 202.1104, must be signed by an officer, a director, a person performing the functions of an officer or a director, or an employee responsible for compliance. In appropriate cases, the Department of Justice may require the chief executive officer of a requesting party to sign the request. Each such person signing a submission must certify that the submission is true, accurate, and complete.

Subpart M—Penalties and Finding of Violation

§ 202.1301 Penalties for violations.

(a) *Civil and criminal penalties.* Section 206 of IEEPA, 50 U.S.C. 1705, is applicable to violations of the provisions of any license, ruling, regulation, order, directive, or instruction issued by or pursuant to the direction or authorization of the Attorney General pursuant to this part or otherwise under IEEPA.

(1) A civil penalty not to exceed the amount set forth in section 206 of IEEPA may be imposed on any person who violates, attempts to violate, conspires to violate, or causes a violation of any license, order, regulation, or prohibition issued under IEEPA.

(2) IEEPA provides for a maximum civil penalty not to exceed the greater of \$368,136 or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed.

(3) A person who willfully commits, willfully attempts to commit, willfully conspires to commit, or aids or abets in the commission of a violation of any license, order, regulation, or prohibition issued under IEEPA shall, upon conviction, be fined not more than \$1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both.

(b) *Adjustment of civil penalties.* The civil penalties provided in IEEPA are subject to adjustment pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990 (Public Law 101–410, as amended, 28 U.S.C. 2461 note).

(c) *Adjustment of criminal penalties.* The criminal penalties provided in IEEPA are subject to adjustment pursuant to 18 U.S.C. 3571.

(d) *False statements.* Pursuant to 18 U.S.C. 1001, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact; or makes any materially false, fictitious, or fraudulent statement or representation;

or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry shall be fined under title 18, United States Code, imprisoned, or both.

(e) *Other applicable laws.* Violations of this part may also be subject to other applicable laws.

§ 202.1302 Process for pre-penalty notice.

(a) *When and how issued.* (1) If the Department of Justice has reason to believe that there has occurred a violation of any provision of this part or a violation of the provisions of any license, ruling, regulation, order, directive, or instruction issued by or pursuant to the direction or authorization of the Attorney General pursuant to this part or otherwise under IEEPA and determines that a civil monetary penalty is warranted, the Department of Justice will issue a pre-penalty notice informing the alleged violator of the agency's intent to impose a monetary penalty.

(2) The pre-penalty notice shall be in writing.

(3) The pre-penalty notice may be issued whether or not another agency has taken any action with respect to the matter.

(4) The Department shall provide the alleged violator with the relevant information that is not privileged, classified, or otherwise protected, and that forms the basis for the pre-penalty notice, including a description of the alleged violation and proposed penalty amount.

(b) *Opportunity to respond.* An alleged violator has the right to respond to a pre-penalty notice in accordance with § 202.1306 of this part.

(c) *Settlement.* Settlement discussion may be initiated by the Department of Justice, the alleged violator, or the alleged violator's authorized representative.

(d) *Representation.* A representative of the alleged violator may act on behalf of the alleged violator, but any oral communication with the Department of Justice prior to a written submission regarding the specific allegations contained in the pre-penalty notice must be preceded by a written letter of representation, unless the pre-penalty notice was served upon the alleged violator in care of the representative.

§ 202.1303 Penalty imposition.

If, after considering any written response to the pre-penalty notice and any relevant facts, the Department of Justice determines that there was a violation by the alleged violator named in the pre-penalty notice and that a civil

monetary penalty is appropriate, the Department of Justice may issue a penalty notice to the violator containing a determination of the violation and the imposition of the monetary penalty. The Department shall provide the violator with any relevant, non-classified information that forms the basis of the penalty. The issuance of the penalty notice shall constitute final agency action. The violator has the right to seek judicial review of that final agency action in Federal district court.

§ 202.1304 Administrative collection and litigation.

In the event that the violator does not pay the penalty imposed pursuant to this part or make payment arrangements acceptable to the Department of Justice, the Department of Justice may refer the matter to the Department of the Treasury for administrative collection measures or take appropriate action to recover the penalty in any civil suit in Federal district court.

§ 202.1305 Finding of violation.

(a) *When and how issued.* (1) The Department of Justice may issue an initial finding of violation that identifies a violation if the Department of Justice:

(i) Determines that there has occurred a violation of any provision of this part, or a violation of the provisions of any license, ruling, regulation, order, directive, or instruction issued by or pursuant to the direction or authorization of the Attorney General pursuant to this part or otherwise under IEEPA;

(ii) Considers it important to document the occurrence of a violation; and

(iii) Concludes that an administrative response is warranted but that a civil monetary penalty is not the most appropriate response.

(2) An initial finding of violation shall be in writing and may be issued whether or not another agency has taken any action with respect to the matter.

(3) The Department shall provide the alleged violator with the relevant information that is not privileged, classified, or otherwise protected, that forms the basis for the finding of violation, including a description of the alleged violation.

(b) *Opportunity to respond.* An alleged violator has the right to contest an initial finding of violation in accordance with § 202.1306 of this part.

(c) *Determination.*—(1) *Determination that a finding of violation is warranted.* If, after considering the response, the Department of Justice determines that a final finding of violation should be issued, the Department of Justice will

issue a final finding of violation that will inform the violator of its decision. The Department shall provide the violator with the relevant information that is not privileged, classified, or otherwise protected, that forms the basis for the finding of violation. A final finding of violation shall constitute final agency action. The violator has the right to seek judicial review of that final agency action in Federal district court.

(2) *Determination that a finding of violation is not warranted.* If, after considering the response, the Department of Justice determines a finding of violation is not warranted, then the Department of Justice will inform the alleged violator of its decision not to issue a final finding of violation. A determination by the Department of Justice that a final finding of violation is not warranted does not preclude the Department of Justice from pursuing other enforcement actions.

(d) *Representation.* A representative of the alleged violator may act on behalf of the alleged violator, but any oral

communication with the Department of Justice prior to a written submission regarding the specific alleged violations contained in the initial finding of violation must be preceded by a written letter of representation, unless the initial finding of violation was served upon the alleged violator in care of the representative.

§ 202.1306 Opportunity to respond to a pre-penalty notice or finding of violation.

(a) *Right to respond.* An alleged violator has the right to respond to a pre-penalty notice or finding of violation by making a written presentation to the Department of Justice.

(b) *Deadline for response.* A response to a pre-penalty notice or finding of violation must be electronically submitted within 30 days of electronic service of the notice or finding. The failure to submit a response within 30 days shall be deemed to be a waiver of the right to respond.

(c) *Extensions of time for response.* Any extensions of time will be granted,

at the discretion of the Department of Justice, only upon specific request to the Department of Justice.

(d) *Contents of response.* Any response should set forth in detail why the alleged violator either believes that a violation of the regulations did not occur or why a finding of violation or penalty is otherwise unwarranted under the circumstances. The response should include all documentary or other evidence available to the alleged violator that supports the arguments set forth in the response. The Department of Justice will consider all relevant materials submitted in the response.

Subpart N—Government-Related Location Data List

§ 202.1401 Government-Related Location Data List.

For each Area ID listed in this section, each of the latitude/longitude coordinate pairs forms a corner of the geofenced area.

Area ID	Latitude/longitude coordinates of geofenced area			
1	38.935624, – 77.207888	38.931674, – 77.199387	38.929289, – 77.203229	38.932939, – 77.209328
2	38.950446, – 77.125592	38.952077, – 77.120947	38.947468, – 77.120060	38.947135, – 77.122809
3	38.953191, – 77.372792	38.953174, – 77.369764	38.951148, – 77.369759	38.951152, – 77.372781
4	39.113546, – 76.777053	39.131086, – 76.758527	39.100086, – 76.749715	39.093304, – 76.760882
5	33.416299, – 82.172772	33.416666, – 82.164366	33.406350, – 82.163645	33.406261, – 82.172947
6	21.525093, – 158.019139	21.525362, – 158.002575	21.518161, – 158.002233	21.518010, – 158.018364
7	21.475012, – 158.061844	21.483357, – 158.057568	21.479226, – 158.049881	21.472695, – 158.052371
8	29.449322, – 98.646174	29.452872, – 98.637623	29.448069, – 98.637303	29.444547, – 98.640607

Dated: October 18, 2024.

Matthew G. Olsen,

Assistant Attorney General for National Security, U.S. Department of Justice.

[FR Doc. 2024–24582 Filed 10–22–24; 4:15 pm]

BILLING CODE 4410–PF–P



FEDERAL REGISTER

Vol. 89

Tuesday,

No. 209

October 29, 2024

Part III

Department of Defense

Chinese Military Companies; Notices

DEPARTMENT OF DEFENSE**Office of the Secretary****Notice of Removal of Designated Chinese Military Companies and Notice of Designation of Chinese Military Company; Supplemental Notice**

AGENCY: Office of the Under Secretary of Defense (Acquisition and Sustainment), Department of Defense (DoD).

ACTION: Notice of removal of a company from the 2023 Section 1260H List of Chinese Military Companies Operating in the United States and notice of designation of Chinese Military Company; supplemental notice.

SUMMARY: On Wednesday, October 23, 2024, the DoD published two notices entitled “Notice of Removal of Designated Chinese Military Companies” and “Notice of Designation of Chinese Military Company.” The notices were inadvertently published in the wrong order. Please see the **SUPPLEMENTARY INFORMATION** section for details.

DATES: This correction is effective October 29, 2024.

FOR FURTHER INFORMATION CONTACT: Patricia Toppings, 571–372–0485.

SUPPLEMENTARY INFORMATION: On Wednesday, October 23, 2024, the DoD published two notices entitled “Notice of Removal of Designated Chinese Military Companies” and “Notice of Designation of Chinese Military Company.”

The notice titled “Notice of Designation of Chinese Military Company” appeared at 89 FR 84547–84548. The notice titled “Notice of Removal of Designated Chinese Military Companies” appeared at 89 FR 84555.

On Wednesday, October 23, 2024, the DoD published two notices entitled “Notice of Removal of Designated Chinese Military Companies” and “Notice of Designation of Chinese Military Company.” The notices were inadvertently published in the wrong order. The notice titled “Notice of Removal of Designated Chinese Military Companies” should have published in the **Federal Register** before the notice titled “Notice of Designation of Chinese Military Company,” to publicly reflect that Hesai Technology Co., Ltd. (Hesai), the designated company, was removed from the Chinese Military Companies list on the basis of the original listing

record and then added to the list on a new record based on the latest information available. This supplemental notice is necessary to clearly identify that Hesai is currently included on the Chinese Military Companies list. The Department is reprinting both notices in the correct order.

Dated: October 24, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2024–25167 Filed 10–28–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE**Office of the Secretary****Notice of Removal of Designated Chinese Military Companies**

AGENCY: Office of the Under Secretary of Defense (Acquisition and Sustainment), Department of Defense.

ACTION: Notice of removal of a company from the 2023 Section 1260H List of Chinese Military Companies Operating in the United States.

SUMMARY: The Deputy Secretary of Defense has decided to delist the entity listed in the **SUPPLEMENTARY INFORMATION** section of this notice from the list of “Chinese military companies” in accordance with the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, without prejudice to relisting the company on additional or supplementary grounds.

FOR FURTHER INFORMATION CONTACT: Mr. Devante Brown (GIES), (703) 695–8545.

SUPPLEMENTARY INFORMATION: Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Pub. L. 116–283) requires the Secretary of Defense to list “Chinese military companies” that meet the statutory criteria annually until December 31, 2030. Paragraph (b)(2) of this section requires the Secretary of Defense to publish the unclassified portion of such list in the **Federal Register**.

The Deputy Secretary of Defense has decided to delist the following entity from the list of “Chinese military companies” in accordance with section 1260H, without prejudice to relisting the entity on additional or supplementary grounds:

Hesai Technology Co., Ltd. (Hesai)

Dated: October 24, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2024–25168 Filed 10–28–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE**Office of the Secretary****Notice of Designation of Chinese Military Company**

AGENCY: Office of the Under Secretary of Defense (Acquisition and Sustainment), Department of Defense.

ACTION: Notice of addition of a company to the Section 1260H List of Chinese Military Companies Operating in the United States.

SUMMARY: The Deputy Secretary of Defense has determined that the entity listed in the **SUPPLEMENTARY INFORMATION** section of this notice qualifies as a “Chinese military company” in accordance with the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.

FOR FURTHER INFORMATION CONTACT: Mr. Devante Brown (GIES), (703) 695–8545.

SUPPLEMENTARY INFORMATION: Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Pub. L. 116–283) requires the Secretary of Defense to make additions or deletions to the most recent list of “Chinese military companies” on an ongoing basis based on the latest information. Paragraph (b)(2) of this section requires the Secretary of Defense to publish the unclassified portion of such list in the **Federal Register**.

The Deputy Secretary of Defense has determined that the following entity qualifies as a “Chinese military company” in accordance with section 1260H:

Hesai Technology Co., Ltd. (Hesai)

Dated: October 24, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2024–25169 Filed 10–28–24; 8:45 am]

BILLING CODE 6001–FR–P

Reader Aids

Federal Register

Vol. 89, No. 209

Tuesday, October 29, 2024

CUSTOMER SERVICE AND INFORMATION

Federal Register/Code of Federal Regulations

General Information, indexes and other finding aids **202-741-6000****Laws** **741-6000**

Presidential Documents

Executive orders and proclamations **741-6000****The United States Government Manual** **741-6000**

Other Services

Electronic and on-line services (voice) **741-6020**Privacy Act Compilation **741-6050**

ELECTRONIC RESEARCH

World Wide Web

Full text of the daily Federal Register, CFR and other publications is located at: www.govinfo.gov.Federal Register information and research tools, including Public Inspection List and electronic text are located at: www.federalregister.gov.

E-mail

FEDREGTOC (Daily Federal Register Table of Contents Electronic Mailing List) is an open e-mail service that provides subscribers with a digital form of the Federal Register Table of Contents. The digital form of the Federal Register Table of Contents includes HTML and PDF links to the full text of each document.To join or leave, go to <https://public.govdelivery.com/accounts/USGPOOFR/subscriber/new>, enter your email address, then follow the instructions to join, leave, or manage your subscription.**PENS** (Public Law Electronic Notification Service) is an e-mail service that notifies subscribers of recently enacted laws.To subscribe, go to <http://listserv.gsa.gov/archives/publaws-l.html> and select *Join or leave the list (or change settings)*; then follow the instructions.**FEDREGTOC** and **PENS** are mailing lists only. We cannot respond to specific inquiries.**Reference questions.** Send questions and comments about the Federal Register system to: fedreg.info@nara.gov

The Federal Register staff cannot interpret specific documents or regulations.

FEDERAL REGISTER PAGES AND DATE, OCTOBER

79731-80054.....	1
80055-80360.....	2
80361-80714.....	3
80715-80992.....	4
80993-81286.....	7
81287-81814.....	8
81815-82158.....	9
82159-82452.....	10
82453-82930.....	11
82931-83420.....	15
83421-83600.....	16
83601-83760.....	17
83761-84064.....	18
84065-84254.....	21
84255-84450.....	22
84451-84798.....	23
84799-85034.....	24
85035-85420.....	25
85421-85850.....	28
85851-86230.....	29

CFR PARTS AFFECTED DURING OCTOBER

At the end of each month the Office of the Federal Register publishes separately a List of CFR Sections Affected (LSA), which lists parts and sections affected by documents published since the revision date of each title.

2 CFR

170.....	79731
184.....	79731
200.....	79731
300.....	80055

3 CFR

Proclamations:

10773 (amended by Proc. 10817)	80351
10817.....	80351
10818.....	80355
10819.....	80357
10820.....	80359
10821.....	80361
10822.....	80363
10823.....	80365
10824.....	80367
10825.....	80369
10826.....	80371
10827.....	80375
10828.....	80377
10829.....	81287
10830.....	81815
10831.....	81817
10832.....	81821
10833.....	81823
10834.....	82925
10835.....	83411
10836.....	83413
10837.....	83601
10838.....	83603
10839.....	83605
10840.....	83609
10841.....	84451
10842.....	84453
10843.....	84455
10844.....	85421

Executive Orders:

14127.....	80345

Administrative Orders:

Memorandums:

Memorandum of September 25, 2024	83761

Memorandum of

September 26, 2024	83763

Memorandum of

September 29, 2024	83765

Notices:

Notice of October 10, 2024	82929

Notice of October 11, 2024	83417

Notice of October 11, 2024	83419

Notice of October 25, 2024	85849

Presidential

Determinations:

No. 2024-13 of September 30, 2024	83767

No. 2024-14 of September 30, 2024	83769

No. 2024-15 of September 30, 2024	83773

Presidential Permits:

Presidential Permit of October 3, 2024	81289

5 CFR

890.....	85012
1321.....	82453

Proposed Rules:

532.....	82874

6 CFR

37.....	85340

7 CFR

2.....	80073
305.....	79733
319.....	79733
1775.....	82482
3434.....	81293
3550.....	82484
3555.....	82484
3560.....	85035

Proposed Rules:

800.....	81396, 83437
927.....	84828
982.....	82190

8 CFR

208.....	81156
235.....	81156
1208.....	81156

9 CFR

Proposed Rules:

201.....	82519

10 CFR

2.....	80715
72.....	83775
429.....	81994
430.....	81295, 83611, 83990, 84028, 84065, 84076
431.....	81994

Proposed Rules:

50.....	85889
51.....	80797, 83632
52.....	85889

12 CFR

30.....	84255
34.....	82931
201.....	80075
213.....	82934

226.....82931, 82938
Ch. X.....80075
328.....84261
1006.....80715
1013.....82934
1026.....82931, 82938

Proposed Rules:

303.....82537, 84108
337.....82537
375.....80135
1227.....79785
1277.....80422

13 CFR

120.....79734

Proposed Rules:

120.....84831
125.....85072

14 CFR

1.....80310
3.....81305
11.....80020, 80310
25.....81313, 83617
39.....80077, 80379, 80724,
80729, 80734, 80993, 80995,
81314, 81320, 81324, 81326,
81329, 81333, 81336, 82486,
82488, 82491, 82493, 82496,
84077, 84262, 84264, 84267,
84272, 84274, 84277, 84457,
84799, 84801, 84803, 84806,
84808, 85037, 85040
61.....80020, 80310
63.....80020
65.....80020
71.....80382, 80383, 80739,
81338, 81339, 82159, 82944,
83776, 83777, 84810, 84812,
85851
73.....84814, 85423
91.....80310, 80384, 81313,
83421
95.....80997
97.....79741, 79742, 83778,
83780
121.....81313
125.....81313
141.....80020
250.....84815
254.....84815

Proposed Rules:

39.....79789, 80155, 80427,
80827, 81403, 82190, 83437,
84836, 84838, 85890
71.....79792, 80157, 80430,
80432, 80433, 81406, 81408,
82538, 84304, 84305, 84307,
84308, 84309, 84311, 84313,
84841, 85455
259.....80435
261.....80435

15 CFR

734.....84770
740.....83427, 84770
742.....84766
744.....83428, 84460, 84770
746.....84460, 84770
748.....80080
764.....83619
774.....84766, 84770
922.....83554

Proposed Rules:

740.....84784
774.....84784

16 CFR

1112.....85388
1130.....85388
1215.....81825
1242.....85388

Proposed Rules:

1.....81871
1220.....85077
1221.....85077
1240.....80159
1421.....80831

17 CFR

38.....83378
232.....84280
242.....81620

18 CFR

50.....84465
380.....84465

Proposed Rules:

40.....79794
342.....84475

19 CFR

Ch. I.....83620

21 CFR

Ch. I.....84819
16.....83781
510.....85423
516.....85423
520.....85423
522.....85423
524.....85423
529.....85423
556.....85423
558.....85423
820.....82945
1308.....84281, 85047

Proposed Rules:

1310.....85459

22 CFR

92.....85429

Proposed Rules:

120.....84482
121.....84482
126.....84482

23 CFR**Proposed Rules:**

772.....83801

25 CFR**Proposed Rules:**

1194.....85078

26 CFR

1.....81341, 82160, 84732,
85798
31.....84079

Proposed Rules:

1.....81871, 85099
54.....85750
301.....81871, 83825

27 CFR

9.....83431, 85852

Proposed Rules:

24.....80160

28 CFR

106.....83621

Proposed Rules:

202.....86116

29 CFR

1910.....81829

Proposed Rules:

1602.....82540
2590.....85750
4902.....84314

30 CFR

250.....85050

31 CFR

33.....85431
501.....81358
587.....80740, 80741, 80742,
84820
588.....84472
594.....84821
1010.....82499
1010.380.....83782

32 CFR

49.....80390
170.....83092

Proposed Rules:

220.....79804
310.....85892

33 CFR

100.....80396, 81004, 81006,
81361, 82506, 83621, 85855
117.....82945, 83435, 85051
165.....80093, 80396, 80398,
80400, 80742, 80743, 81008,
82170, 83783, 83785, 84286,
85053, 85432, 85434, 85855

Proposed Rules:

117.....80436, 85117
147.....84316

36 CFR

242.....83622

37 CFR

2.....85435
7.....85435
42.....79744, 82172
201.....80743, 85437
229.....80743

Proposed Rules:

380.....82543

38 CFR

14.....85055
38.....82179
39.....82179

Proposed Rules:

3.....79815
14.....82546
81.....80172

39 CFR**Proposed Rules:**

111.....82948
3050.....83632

40 CFR

51.....84286
52.....79752, 80402, 80745,
80749, 81008, 81361, 82508,
82510, 84083, 84085, 84286,
84288, 85064, 85857
60.....83296

62.....82513
63.....84291
84.....82682
82.....82414
139.....82074
170.....80767
180.....81010, 85067, 85859
261.....82515, 82682, 83787
262.....82682
266.....82682
270.....82682
271.....82682
281.....79756
282.....79756, 80788

Proposed Rules:

51.....80833
52.....79828, 80439, 80445,
81036, 81409, 82550, 82553,
82560, 82948, 82953, 83338,
84322, 84842, 85119
62.....82564
81.....81409
180.....80446
281.....79850
282.....79850, 80853
372.....81776

41 CFR

51.....83788

42 CFR

38.....80055
50.....80055
51.....80055
51a.....80055
51b.....80055
51c.....80055
51d.....80055
52.....80055
52a.....80055
52b.....80055
52c.....80055
52d.....80055
52e.....80055
55a.....80055
56.....80055
57.....80055
59.....80055
59a.....80055
62.....80055
63a.....80055
64.....80055
65.....80055
65a.....80055
66.....80055
67.....80055
124.....80055
136.....80055
405.....80098, 83240
412.....80095, 80098, 80131,
80405
413.....80098, 80132
417.....80055
418.....79764
430.....80055
431.....80098, 85070
433.....80055
434.....80055
435.....85431
436.....80055
438.....80055
440.....80055
441.....80055
456.....80055
457.....80055, 85070
476.....83240

482.....80098	1328.....80055	305.....80634	Proposed Rules:
485.....80098	1336.....80055	306.....80634	40.....82957
488.....80132	1355.....80055	308.....80634	107.....85590
489.....83240	1357.....80055	309.....80634	171.....85590
495.....80098	2584.....85867	311.....80634	172.....85590
512.....80098	Proposed Rules:	312.....80634	173.....85590
600.....85431	147.....85750	313.....80634	174.....85590
1001.....80055	153.....82308	314.....80634	176.....85590
1007.....80055	155.....82308	315.....80634	177.....85590
Proposed Rules:	156.....82308	316.....80634	178.....85590
600.....82308	158.....82308	318.....80634	179.....85590
44 CFR	47 CFR	319.....80634	180.....85590
9.....82182	8.....84086	322.....80634	199.....82957
45 CFR	9.....81013, 83628	323.....80634	211.....85895
16.....80055	15.....83789	324.....80634	213.....84845
46.....84822	64.....82518	325.....80634	236.....85462
63.....80055	73.....84096	326.....80634	
75.....80055	74.....83789	327.....80634	
87.....80055	Proposed Rules:	330.....80634	
95.....80055	64.....80449	331.....80634	50 CFR
98.....80055, 85071	48 CFR	332.....80634	13.....83629
153.....85431	205.....82182	333.....80634	17.....81388, 85294
155.....85431	206.....82183	334.....80634	22.....83629
156.....85431	212.....82182, 82183	335.....80634	100.....83622
261.....80055	214.....82182	336.....80634	217.....79777, 81848, 84674
262.....80055	215.....82182	337.....80634	223.....81867
263.....80055	237.....82182	341.....80634	622.....81031, 84105
265.....80055	252.....82183, 82188	342.....80634	635.....81032, 85452, 85879
286.....80055	270.....82183	343.....80634	648.....79778, 80795, 81869,
287.....80055	Ch. 4.....81014	344.....80634	84106, 85885
301.....80055	Proposed Rules:	345.....80634	660.....84296, 84302, 85453
302.....80055	25.....84505	347.....80634	679.....79783, 81034, 81394
303.....80055	234.....82193	352.....80634	Proposed Rules:
304.....80055	242.....82193	370.....80634	17.....79857, 79880, 85909
309.....80055	252.....82193, 82196	3025.....79851	217.....85686
400.....80055	301.....80634	3052.....79851	223.....84510
1000.....80055	302.....80634	49 CFR	224.....84510
1303.....80055	303.....80634	225.....79767, 85450	648.....83440
1321.....80055	304.....80634	571.....81836	660.....81878, 84511
		674.....83956	679.....84514

LIST OF PUBLIC LAWS Note: No public bills which have become law were received by the Office of the Federal Register for inclusion	in today's List of Public Laws. Last List October 8, 2024	Public Laws Electronic Notification Service (PENS) PENS is a free email notification service of newly	enacted public laws. To subscribe, go to https://portalguard.gsa.gov/__layouts/PG/register.aspx. Note: This service is strictly for email notification of new laws. The text of laws is not available through this service. PENS cannot respond to specific inquiries sent to this address.