AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# FEDERAL REGISTER

Vol. 90 Monday,

No. 205 October 27, 2025

Pages 48557–48704

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: 90 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.*

Printed on recycled paper.

# Contents

**Federal Register**

Vol. 90, No. 205

Monday, October 27, 2025

**Commerce Department**
*See* Patent and Trademark Office

**Environmental Protection Agency**
**NOTICES**
Hearings, Meetings, Proceedings, etc.:
FIFRA Scientific Advisory Panel, 48582

**Federal Communications Commission**
**RULES**
Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, 48648–48703
**PROPOSED RULES**
Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, 48557–48578

**Homeland Security Department**
**RULES**
Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States, 48604–48645
**NOTICES**
Determination Pursuant to Section 102 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, as Amended, 48582–48583

**Judicial Conference of the United States**
**NOTICES**
Hearings, Meetings, Proceedings, etc.:
Advisory Committee on Criminal Rules, 48584
Advisory Committee on Evidence Rules, 48583–48584

**National Credit Union Administration**
**NOTICES**
Staff Draft 2026-2027 Budget, 48584

**Patent and Trademark Office**
**NOTICES**
Streamlined Claim Set Pilot Program, 48579–48582

**Postal Regulatory Commission**
**NOTICES**
New Postal Products, 48584–48585

**State Justice Institute**
**NOTICES**
Grant Guideline, 48585–48600

**Transportation Department**
**NOTICES**
Agency Information Collection Activities; Proposals, Submissions, and Approvals:
Transportation Acquisition Regulation, 48600–48601

**Unified Carrier Registration Plan**
**NOTICES**
Meetings; Sunshine Act, 48601–48602

**Separate Parts In This Issue**

**Part II**
Homeland Security Department, 48604–48645

**Part III**
Federal Communications Commission, 48648–48703

**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.

**8 CFR**
215.....48604
235.....48604

**47 CFR**
0.....48648
1.....48648
43.....48648

**Proposed Rules:**
1.....48557

# Proposed Rules

Federal Register
Vol. 90, No. 205
Monday, October 27, 2025

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.

## FEDERAL COMMUNICATIONS COMMISSION

### 47 CFR Part 1

**[OI Docket No. 24–523, MD Docket No. 24–524; FCC 25–49; FR ID 311053]**

## Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks

**AGENCY:** Federal Communications Commission.

**ACTION:** Proposed rule.

**SUMMARY:** In this document, the Federal Communications Commission (Commission or FCC) adopted a Further Notice of Proposed Rulemaking (*FNPRM*) that proposes to prevent national security risks from current and potential foreign adversaries, while encouraging the use of trusted technology and measures to further accelerate the buildout of submarine cables. The *FNPRM* proposes a regulatory framework that would grant a blanket license to entities that own or operate Submarine Line Terminal Equipment (SLTEs), subject to certain exclusions and routine conditions, such as a tailored foreign adversary annual report. The *FNPRM* proposes new certifications and routine conditions related to foreign adversaries to further protect submarine cables from national security risks. The *FNPRM* also proposes an approach to expedite deployment of submarine cables that connect to the United States by presumptively excluding submarine cable applications from referral to the relevant Executive Branch agencies if they meet certain standards. The *FNPRM* seeks comment on requiring existing licensees to remove from their submarine cable system covered equipment or services, within a specified timeframe prior to the expiration of the license. The *FNPRM* also seeks comment on how the Commission can use its authority to incentivize and encourage the adoption and the use of trusted technologies produced and provided by the United States and its foreign allies.

**DATES:** Comments are due November 26, 2025; reply comments are due December 26, 2025.

**ADDRESSES:** Pursuant to §§ 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). You may submit comments, identified by OI Docket No. 24–523 or MD Docket No. 24–524, by any of the following methods:

- *Electronic Filers:* Comments may be filed electronically using the internet by accessing the ECFS: *https://www.fcc.gov/ecfs*.
- *Paper Filers:* Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by hand or messenger delivery, by commercial courier, or by the U.S. Postal Service. All filings must be addressed to the Secretary, Federal Communications Commission.
- Hand-delivered or messenger delivered paper filings for the Commission's Secretary are accepted between 8 a.m. and 4 p.m. by the FCC's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
- Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701. Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.
- *People with Disabilities.* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530.

**FOR FURTHER INFORMATION CONTACT:** Desiree Hanssen, Office of International Affairs, Telecommunications and Analysis Division, at *desiree.hanssen@fcc.gov* or at (202) 418–0887. For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, send an email to *PRA@fcc.gov* or contact Cathy Williams at 202–418–2918 or *Cathy.Williams@fcc.gov*.

**SUPPLEMENTARY INFORMATION:** This is a summary of the Commission's Further Notice of Proposed Rulemaking (*FNPRM*), in OI Docket No. 24–523, in MD Docket No. 24–524, FCC 25–49, adopted on August 7, 2025, and released on August, 13, 2025. The full text of this document is available online at *https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf*. The full text of this document is also available for public inspection and copying during business hours in the FCC Reference Center, 45 L Street NE, Washington, DC 20554. To request materials in accessible formats for people with disabilities, send an email to *FCC504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice), 202–418–0432 (TTY).

*Providing Accountability Through Transparency Act.* The Providing Accountability Through Transparency Act, Public Law 118–9, requires each agency, in providing notice of a rulemaking, to post online a brief plain-language summary of the proposed rule. The required summary of this FNPRM is available at *https://www.fcc.gov/proposed-rulemakings*. To request materials in accessible formats for people with disabilities (*e.g.* Braille, large print, electronic files, audio format), send an email to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at (202) 418–0530.

*Ex Parte Presentations.* The proceeding this Notice initiates shall be treated as a ''permit-but-disclose'' proceeding in accordance with the Commission's *ex parte* rules. *See* 47 CFR 1.1200 *et seq.* Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and

arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with § 1.1206(b). In proceedings governed by § 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.,* .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

*Regulatory Flexibility Act.* The Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning the potential impact of rule and policy change proposals on small entities in the Further Notice of Proposed Rulemaking. The Commission invites the general public, in particular small businesses, to comment on the IRFA. Comments must be filed by the deadlines for comments on the Further Notice of Proposed Rulemaking indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

*Paperwork Reduction Act.* This document may also contain proposed new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and OMB to comment on any information collection requirements contained in this document, as required by the PRA. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

**Synopsis**

**I. Introduction**

1. In this item, we modernize and streamline the Commission's submarine cable rules to facilitate faster and more efficient deployment of submarine cables, while at the same time ensuring the security and resilience of this critical infrastructure. We recognize that investment in such infrastructure is vital to American prosperity and economic dynamism. The rules that we adopt today will ensure that the United States remains ready and able to deploy submarine cable infrastructure with increasing amounts of capacity to meet current and future internet and data demands so that the United States remains ''the unrivaled world leader in critical and emerging technologies—such as artificial intelligence.'' With global competition for submarine cables increasing, connections to the United States should continue to be at the forefront of the submarine cable marketplace. Nonetheless, ''[i]nvestment at all costs is not always in the national interest,'' because of the potential for foreign adversary exploitation. We also recognize that ''[e]conomic security is national security,'' and thus protecting our communications networks against foreign threats is crucial. With these principles in mind today, we undertake the first major comprehensive update of our submarine cable rules since 2001. Since that time, technology, consumer expectations, international submarine cable traffic patterns, submarine cable infrastructure, and the foreign threat landscape have changed greatly.

2. To advance the Commission's comprehensive strategy to build a more secure and resilient communications supply chain, we adopt rules that place a strong emphasis on preventing and mitigating national security risks from foreign adversaries, while welcoming investment from United States allies and partners. We also lighten the regulatory burden on industry by modernizing and simplifying the submarine cable license approval process.

3. In the *FNPRM,* we propose to build upon the efforts adopted in the *Report and Order* to prevent national security risks from current and potential foreign adversaries, while encouraging the use of trusted technology and measures to further accelerate the buildout of submarine cables. We propose and seek comment on a regulatory framework that would require entities that own or operate SLTEs to become licensees. We propose granting SLTE owners and operators a blanket license, subject to certain exclusions and routine conditions, to reduce burdens on industry and encourage the investment in and deployment of submarine cable systems. As a condition of any grant of a blanket license, we also propose to require existing SLTE owners and operators that are owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, or other relevant criteria, to submit a tailored annual report (SLTE Foreign Adversary Annual Report) to ensure that the Commission maintains consistent oversight over their operations. We propose new certifications and routine conditions related to foreign adversaries to further protect submarine cables from national security risks.

4. While the *FNPRM* is pending, and to streamline the processing of submarine cable applications during this time, we will consistently implement our streamlined processing rules and not defer action on a submarine cable application unless the Executive Branch agencies, including the agencies that form the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee), provide specific and compelling national security, law enforcement, or other justifications to defer action. We propose an approach to expedite deployment of submarine cables that connect to the United States by presumptively excluding submarine cable applications from referral to the relevant Executive Branch agencies if they meet certain standards. To further protect U.S. submarine cable networks from national security and law enforcement threats, we seek comment on whether to require existing licensees to remove from their submarine cable system any and all covered equipment or services, within a specified timeframe prior to the expiration of the license. We also seek comment on how the Commission can use its authority pursuant to the Cable Landing License Act of 1921 (Cable Landing License Act or the Act) and Executive Order 10530 of 1954, to incentivize and encourage the adoption and the use of trusted technologies produced and provided by the United States and its foreign allies. Finally, we seek comment on whether under certain circumstances to streamline approval of domestic cables.

5. In short, we ''maintain[ ] the strong, open investment environment that benefits our economy and our people, while enhancing our ability to protect the United States from new and evolving threats'' in the submarine cable ecosystem.

## II. Background

6. In November 2024, the Commission adopted the *2024 Cable NPRM,* initiating a comprehensive review of the submarine cable rules to develop forward-looking rules to better protect submarine cables, identify and mitigate harms affecting national security and law enforcement, and facilitate the deployment of submarine cables and capacity to the market. As explained in the *2024 Cable NPRM,* the Commission's authority to grant, withhold, revoke, or condition submarine cable landing licenses derives from the Cable Landing License Act and Executive Order 10530. The Commission discussed in detail its rules and coordination of applications with the Executive Branch agencies, including the Committee, to assess applicants and licensees for assessment of any national security, law enforcement, foreign policy, and/or trade policy concerns. The Commission also discussed the existing procedures by which it coordinates with the State Department on all submarine cable applications and obtains approval of any proposed grant of an application or revocation of a cable landing license pursuant to the Cable Landing License Act and Executive Order 10530.

7. *Recent Commission Actions Regarding National Security.* The Commission has recognized that national security is built on both protecting the nation's communications infrastructure from foreign adversary threats and promoting the prosperity and robustness of the communications sector. The Commission in its recent rulemaking proceedings and actions is continuing its ongoing efforts to secure and protect communications networks from foreign adversaries, while recognizing that investment in U.S. communications networks bolsters national security. In December 2024, the Commission engaged with stakeholders in light of U.S. government confirmed reports that state-sponsored foreign actors tied to the People's Republic of China (PRC) infiltrated at least eight U.S. communications companies in a massive espionage effort, an incident known as Salt Typhoon. The Commission has continued to remain vigilant against this and other foreign adversary cyberthreats.

8. Earlier this year, shortly after President Trump announced in February 2025 the America First Investment Policy, which states that ''[e]conomic security is national security'' and discusses the need to limit certain investments in strategic sectors by six identified foreign adversaries, the Commission initiated a series of actions. In March 2025, the Commission responded to threats posed by the People's Republic of China and to the evolving threat environment more generally, by establishing a Council for National Security to bring together the Commission's regulatory, investigatory, and enforcement authorities to counter foreign adversaries. The Council was established with a three-part goal: ''(1) Reduce the American technology and telecommunications sectors' trade and supply chain dependencies on foreign adversaries; (2) Mitigate America's vulnerabilities to cyberattacks, espionage, and surveillance by foreign adversaries; and (3) Ensure the U.S. wins the strategic competition with China over critical technologies, such as 5G and 6G, AI, satellites and space, quantum computing, robotics and autonomous systems, and the Internet of Things.'' In the same month, the Commission opened a separate proceeding, the *Delete, Delete, Delete* proceeding, with an aim to remove outdated and unnecessary regulations to clear away obstacles to investment.

9. On May 22, 2025, the Commission took action in two distinct proceedings to protect our nation's communications infrastructure from foreign adversary threats. First, in the *Equipment Authorization Report and Order and FNPRM,* the Commission adopted new rules to help ensure that the telecommunication certification bodies (TCBs), measurement facilities (test labs), and laboratory accreditation bodies that participate in our equipment authorization program are not subject to ownership, direction, or control by untrustworthy actors, including foreign adversaries, that pose a risk to national security. The *Equipment Authorization Report and Order* prohibits Commission recognition of any TCB, test lab, or laboratory accreditation body owned by, controlled by, or subject to the direction of a prohibited entity, and prohibits such TCBs, test labs, and laboratory accreditation bodies from participating in the Commission's equipment authorization program.

10. Second, in the *Foreign Adversary NPRM,* the Commission proposed to adopt certification and information collection requirements that would fill gaps in the Commission's existing rules and give the Commission, and the public, a new and comprehensive view of threats from foreign adversaries in the communications sector. Specifically, the Commission proposed to apply new certification and disclosure requirements on entities holding every type of license, permit, or authorization, rather than only certain specific licenses, and to go beyond foreign adversary ownership to also cover all regulated entities controlled by or subject to the jurisdiction or direction of a foreign adversary. The Commission stated that, by focusing on foreign adversary ownership or control, rather than foreign influence more broadly, the proposed rules are tailored to avoid needless burden on regulated entities.

11. *2024 Cable NPRM.* On November 22, 2024, the Commission adopted the *2024 Cable NPRM,* which initiated the first major review of the submarine cable rules since 2001, and sought comment on how best to improve and streamline the rules to facilitate efficient deployment of submarine cables while ensuring the security, resilience, and protection of this critical infrastructure. Among other things, the Commission sought comment on codifying the scope of the Commission's licensing requirements under the Cable Landing License Act and Executive Order 10530 and other legal requirements, improving the Commission's oversight of submarine cable landing licenses, and adopting targeted requirements to protect submarine cables from national security and law enforcement risks. The Commission further sought comment on streamlining procedures to expedite submarine cable review processes and improving the quality of the circuit capacity data and facilitating the sharing of such information with other federal agencies. To address evolving national security, law enforcement, and other risks, the Commission sought comment on updating application requirements for national security purposes and ensuring the Commission has targeted and granular information regarding the ownership, control, and use of a submarine cable system, adopting new compliance certifications, and on any additional steps the Commission can take to protect this critical infrastructure, including activities in coordination with other federal agencies.

12. Earlier this year, the Commission received 18 comments, nine reply comments, and several ex partes pertaining to a wide range of topics discussed in the *2024 Cable NPRM.* Several commenters supported the proposal to codify a definition of a submarine cable system in the Commission's rules. Some commenters offered reservations about potentially duplicative requirements between the proposed periodic reporting, which sought updated ownership and other information, and similar requirements in mitigation agreements with the Committee, as well as concerns about requiring SLTE owners and operators to

be licensees. Other commenters offered generally critical views about the proposal to lower the ownership threshold for reportable interests from 10% to 5%, with some further refinements suggested. Some commenters expressed reservations about including capacity holders or IRU holders and lessees under a licensing requirement. Meanwhile, several commenters supported the effort to streamline applications and offered recommendations. As explained below, we have considered these and other comments in the thorough record received and either take action today or seek additional comment.

## III. Further Notice of Proposed Rulemaking

13. In this *FNPRM,* we propose concrete steps to build upon the *Report and Order* and recent proceedings to prevent national security risks from current and potential foreign adversaries. While this *FNPRM* is pending, and to streamline the processing of submarine cable applications during this time, we will consistently implement our streamlined processing rules and not defer action on a submarine cable application unless the Committee provides specific and compelling national security, law enforcement, or other justifications to defer action. We propose to require SLTE owners and operators to become licensees on a cable landing license and seek comment on a regulatory framework for SLTE owners and operators that balances national security concerns with the need to reduce regulatory burdens. In addition, we propose new certifications and routine conditions related to foreign adversaries to further protect submarine cables from national security risks. Moreover, we propose an approach to expedite deployment of submarine cables that connect to the United States by presumptively excluding submarine cable applications from referral to the Executive Branch agencies if they meet certain standards. Finally, we propose and broadly seek comment on additional measures to reform and streamline the submarine cable licensing rules and processes, with the goal of accelerating and enhancing the buildout of submarine cable infrastructure, and seek comment on the costs and benefits of the proposed rules and any alternatives.

### *A. Regulatory Framework for SLTEs*

14. In the *2024 Cable NPRM,* the Commission sought comment on whether to require entities that own or control the SLTE to be applicants for and licensees on a cable landing license. The Commission explained that ''[t]he SLTE is among the most important equipment associated with the submarine cable system and this modification to our rule would enable the Commission to know and assess any national security and law enforcement concerns related to the entities that will deploy SLTE and thus who can significantly affect the cable system's operations.'' The Commission also noted that a proposed cable system could have multiple locations where SLTE is deployed and therefore sought comment on whether and if so, how, to incorporate entities with ownership or control of SLTEs into our regulatory framework. The *2024 Cable NPRM* included an example of how the Commission would apply this licensing requirement, including certain IRU holders or grantees. Many commenters, including NASCA, Coalition, Microsoft, ICC, INCOMPAS, and ITI, disagree that the Commission should require SLTE owners and operators to become licensees. However, the Committee identified substantial national security risks associated with SLTE.

15. Although we decline in the *Report and Order* to require SLTE owners and operators to become licensees, we are taking steps to identify, through the one-time information collection adopted in the *Report and Order,* how many entities currently own or operate SLTEs on existing licensed cable systems. Through the one-time information collection, we will seek information from licensees regarding SLTEs to inform our decisions regarding the questions presented in this *FNPRM.*

#### 1. Requirements for SLTE Owners and Operators To Be a Licensee

16. We propose to adopt a rule that would require any entity that owns or operates SLTE to become a licensee (SLTE owner and operator) and also be subject to certain routine conditions. We propose to amend § 1.70003 of our newly adopted rules to include as licensees ''all entities that own or operate submarine line terminal equipment.'' To reduce the burden of requiring existing SLTE owners and operators to file an application to become a licensee, we propose to adopt a blanket license for existing owners and operators of SLTE subject to the conditions below. We use the term ''existing owners and operators of SLTE'' to refer to any entity that owns and/or operates SLTE on a Commissioned-licensed submarine cable system prior to the effective date of any new applicable rules subsequently adopted in this proceeding. We seek comment on this proposal or whether there are alternatives to this approach. We seek comment on whether our approach is properly tailored to reduce burdens on existing SLTE owners and operators and to limit any impacts of such proposal on existing licensees. We also seek comment on whether this proposal will disproportionately impact small entities that own or operate SLTE.

17. We tentatively conclude the Cable Landing License Act authorizes the Commission to regulate SLTE owners and operators. INCOMPAS and Microsoft state that there is no basis in the Cable Landing License Act for requiring these entities to become licensees because such entities do not ''land or operate'' a cable system, as required by the Act. We disagree with these commenters' assertions. Under the Cable Landing License Act, a license is required to land or operate a submarine cable connecting to the United States. An entity that owns or operates SLTE operates a significant component of the submarine cable system. In the *Report and Order,* we adopt a definition that ''a submarine cable system carries bidirectional data and voice telecommunications traffic consisting of one or more submarine cable(s) laid beneath the water, and all associated components that support the operation of the submarine cable system end-to-end, including the segments up to the system's terrestrial terminations at one or more SLTEs as well as the transponders that convert optical signals to electrical signals and vice versa.''

18. The ability to convert the telecommunications traffic optical signals to electrical signals and vice versa is simply not possible without equipment that performs that function. That is, the submarine cable system cannot be operated *without* the SLTE. We determine in the *Report and Order* that SLTE is a significant component of the system that may be owned separately from the other licensees who are required to comply with routine conditions and oversight under the Cable Landing Act and current Commission rules. Further, SLTE allows an entity to exercise control over its own fiber, capacity, or spectrum on the submarine cable system. With the advent of open cable systems, submarine cable owners and operators now have the ability to pass on an important responsibility of lighting the fiber to certain customers who wish to control their traffic and technology, *i.e.,* dark fiber IRU or lease holders.

19. The Committee explains that entities with dark fiber IRUs that deploy their own SLTE could be foreign

adversary-controlled landing parties, telecommunications companies, and governments with interest, access, and control over the fiber, capacity, or spectrum for the ''entire life of the cable.'' In essence, ''[a] foreign adversary-controlled non-licensee entity that owns, controls, or operates its own SLTE, or equivalent equipment, on a submarine cable landing in the United States may have connectivity comparable to operating their own communications cable to the United States without a license, or any regulatory review, mitigation, or monitoring for national security or law enforcement risk.'' The Committee further articulates that foreign adversary-affiliated entities that own or operate SLTE pursuant to an IRU or similar legal agreement, may effectively operate a submarine cable system that thereby ''allow[s] an adversary to intercept or misroute U.S. persons' communications and sensitive data transiting the cable, posing a serious counterintelligence risk.'' These concerns pose significant national security risks that would justify requiring SLTE owners or operators to be licensees on a cable landing license.

20. Based on the ownership of SLTE and ability to operate a significant component of the submarine cable system, we believe SLTE owners and operators fit within the Cable Landing License Act as operators of a submarine cable system. Therefore, we propose to require SLTE owners and operators to become licensees so that we can effectively carry out our duty to protect national security. Moreover, ''[t]he Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with [the Communications] Act, as may be necessary in the execution of its functions.'' Given that submarine cable systems are only functional with SLTE, regulating SLTE owners and operators seems necessary to execute the Commission's duties under the Cable Landing License Act and Executive Order 10530 to regulate submarine cable landing or operation, including withholding or revoking a cable landing license where such action would ''promote the security of the United States.'' We seek comment on our analysis.

2. Blanket License for SLTE Owners and Operators

21. To reduce burdens and ensure that the Commission tailors this requirement so that it does not interfere with the existing licensing process under our rules, we propose to adopt a blanket license for SLTE owners and operators. We understand that SLTE owners and operators may be different entities from the cable owners and operators that are required to be applicants/licensees under our rules, as amended in § 1.70003. We expect to have a better understanding of SLTEs after the completion of the one-time collection adopted today.

22. We believe that this blanket license approach for SLTE owners and operators is important to ensure the Commission is aware of all the entities that install their own SLTE to use fiber, capacity, or spectrum on the submarine cable system, while also not impacting those entities that are required to apply for a cable landing license pursuant to § 1.70003 of our newly adopted rules. Commenters voice concern that if the Commission requires SLTE owners and operators to become licensees, then it will take a very long time for such entities to obtain a license, resulting in backlog and harm to investment in the submarine cable industry. In addition, commenters are concerned that each time a new SLTE owner and operator is added to the submarine cable system, a modification application would be required in advance, which would exacerbate aforementioned harms. By proposing a blanket license for SLTE owners and operators, we believe that this approach will obviate the need for an initial application for a cable landing license or a modification application as contended by AWS and Coalition, and thus streamline the licensing process for this category of licensees.

23. To protect national security and law enforcement interests, we propose to exclude certain entities from the grant of this blanket license to the extent such entities seek to own or operate new SLTE on any current or future submarine cables landing in the United States. Specifically, we propose to exclude from the grant of this blanket license, any entity that would be subject to the foreign adversary and/or character presumptive disqualifying conditions that we adopt in the *Report and Order.*

24. We seek comment on whether this proposal is sufficient to ensure the protection and security of the submarine cable infrastructure. Should we instead exclude a larger or smaller category of entities from grant of the blanket license? We seek comment on how this proposal could affect existing licensees as well as the users of submarine cable systems. Are there any alternative approaches that may better achieve our objectives in a less burdensome way? For example, should we adopt regular reporting requirements instead?

25. We seek comment on whether we should allow entities that are excluded from the grant of a blanket license to file an application in accordance with our application rules, as amended in the *Report and Order,* if they seek to own or operate SLTE. Or should such entities provide an alternative showing, in lieu of an application, that they can overcome the adverse presumption set out in the disqualifying condition? We address in the *Report and Order* the written process that will apply where the Commission considers whether denial of an application or revocation and/or termination of a cable landing license is warranted. To the extent the Commission or OIA considers that a denial of an application is warranted or revocation and/or termination of a license is warranted, OIA pursuant to its delegated authority would determine appropriate procedures on a case by case basis as required by due process and applicable law and in light of the relevant facts and circumstances, including providing the applicant or licensee with notice and opportunity to cure noncompliance to the extent such an opportunity is required by the APA, and to respond to allegations and evidence in the record. We seek comment on whether the exclusion of certain SLTE owners and operators from the grant of a blanket license may disturb existing licensees' operations and interfere with investment-backed reliance interests of such licensees.

3. Routine Conditions for SLTE Owners and Operators

26. We seek comment on whether to apply distinct routine conditions to SLTE owners and operators as a separate category of licensees. Although SLTE owners and operators operate a significant portion of the submarine cable system as it pertains to an entity's control over a fiber, capacity, or spectrum, we understand that SLTE owners and operators may have distinct responsibilities from other submarine cable owners and operators, such as those licensees that own and maintain common infrastructure for the submarine cable system. Therefore, to satisfactorily tailor any regulatory obligations of SLTE owners and operators, we seek comment on appropriate routine conditions to apply to SLTE owners and operators, as set forth below.

27. With the understanding that certain existing routine conditions may not neatly apply to this category of cable landing licensees, we seek comment to examine whether we should specifically tailor routine conditions to apply to SLTE owners and operators, including for small providers. Are there national security or law enforcement reasons

why we may want to apply certain routine conditions to SLTE owners and operators? Are there any reasons why we should limit the number of routine conditions required for SLTE owners and operators? We seek comment on what routine conditions should apply to SLTEs generally. We seek comment on whether we should adopt the same routine conditions that currently apply to cable landing licensees. What routine conditions are appropriate for SLTE owners and operators so that the Commission may retain oversight of these entities and ensure compliance with the Cable Landing License Act and Commission rules?

28. Specifically, we propose that the Commission should require the following as routine conditions on the grant of a blanket license: (1) compliance with all rules and regulations of the Commission; (2) compliance with any treaties or conventions relating to communications to which the United States is or may hereafter become a party; (3) compliance with any action by the Commission or the Congress of the United States rescinding, changing, modifying or amending any rights accruing to any person by grant of the license; (4) the licensee, or any person or company controlling it, controlled by it, or under direct or indirect common control with it, does not enjoy and shall not acquire any right to handle traffic to or from the United States, its territories or its possessions unless such service is authorized by the Commission pursuant to section 214 of the Communications Act, as amended; (5) the licensee shall file a notification for prior approval to become affiliated with a foreign carrier; (6) the licensee shall file annual circuit capacity reports as required by § 43.82 of this chapter; (7) the cable landing license is revocable by the Commission after due notice and opportunity for hearing pursuant to section 2 of the Cable Landing License Act, 47 U.S.C. 35, or for failure to comply with the terms of the license or with the Commission's rules; and (8) the licensee must comply with proposed rule, § 1.70017, by filing the SLTE Foreign Adversary Annual Report, if one or more of the criteria under the proposed rule are met. We believe that the routine conditions will promote the statutory purposes under the Cable Landing License Act and better enable the Commission to carry out its licensing duties in furtherance of those purposes. We seek comment on this view.

29. Licensees under § 1.70003 of our newly adopted rules that seek to consummate a transaction, such as a transfer of control or assignment of the cable landing license, must seek prior approval from the Commission or provide a post-consummation notification consistent with §§ 1.70012 and 1.70013. We seek comment on whether, and if so, how, to apply the Commission's new rules at §§ 1.70012 and 1.70013 to transactions by SLTE owners and operators. If SLTE is sold or transferred to another entity that resumes operation of the SLTE connected to the licensed submarine cable system, the Commission cannot maintain oversight of the SLTE without this information. We seek comment on whether the Commission should be made aware if the SLTE and/or SLTE owner and operator is transferred or assigned to another entity. We seek comment on the impact of such a reporting requirement on small SLTE owners and operators. For transactions involving transfers of control or assignments of the SLTE itself or the SLTE owner and operator, how should the Commission frame its rules? For both scenarios, should the existing SLTE owner and operator be obligated to file an application seeking prior approval of the transaction? Or should the existing SLTE owner and operator file a notification including basic information about the transaction? We seek comment on how the Commission should handle *pro forma* transactions, such as whether it should merely apply the transaction rules set forth in our newly adopted rules to this category of licensees. We seek comment on methods the Commission can employ to ensure its records remain up-to-date, but that do not unduly delay or interfere with the ability of an SLTE owner and operator to sell, purchase, transfer, or take a similar action that is consistent with the SLTE owner's and operator's business needs. Our existing rules require that ''[t]he licensee, or in the case of multiple licensees, the licensees collectively, shall maintain *de jure* and *de facto* control of the U.S. portion of the cable system, including the cable landing stations in the United States, sufficient to comply with the requirements of the Commission's rules and any specific conditions of the license.'' We consider that this routine condition may be difficult to impose on SLTE owners and operators who may not have ownership interests in common infrastructure in the submarine cable system and may instead hold interests in a fiber, capacity, or spectrum that they must light themselves. Should we adopt a routine condition requiring that SLTE owners and operators must maintain *de jure* and *de facto* control of the SLTE? We seek comment on other alternatives that we should consider.

30. In the *Report and Order,* we adopt routine conditions for existing licensees and future licensees with regard to cybersecurity and physical security risk management, the Covered List, and foreign adversary-related disclosures and prohibitions. We seek comment on whether to adopt these new routine conditions for SLTE owners and operators. For example, should we adopt routine conditions requiring all SLTE owners and operators to certify that they have created, updated, and implemented a cybersecurity and physical security risk management plan and to certify that they will not add to the submarine cable systems, covered equipment or services that are currently identified or newly identified in the future? We seek comment on whether to require SLTE owners and operators to disclose whether or not their submarine cable systems use equipment or services identified on the Covered List. Consistent with the proposal under section IV.B.1.–2. of this *FNPRM,* we also seek comment on whether to require an applicant for a cable landing license to certify, as a condition of the potential grant of an application, that it will not use any equipment in the operation of the submarine cable system that is produced or provided by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g). Should we also require this certification if an entity seeks to own or operate new SLTE on any current or future submarine cables landing in the United States?

31. In the *Report and Order,* we also adopt routine conditions to ensure we receive timely updates from licensees when there are certain changes requiring the Commission's attention. Consistent with those adopted routine conditions, we propose and seek comment on adopting the following additional routine conditions for all SLTE owners and operators. We propose that SLTE owners and operators must file a notification updating the Commission within thirty (30) days of any change in: (1) the point of contact of the SLTE owner and operator; (2) the name of the SLTE owner and operator or the submarine cable system; (3) ownership of the SLTE owner and operator resulting in the entity becoming owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g), to the extent such change does not require prior Commission approval under our rules; and (4) location of SLTE such as a change of

address or coordinates of the SLTE. We seek comment on whether any SLTE owners or operators should be exempt from these routine conditions. We seek comment on whether there are any other changes that the Commission should be aware of and what method of reporting would be the least burdensome to SLTE owners and operators while ensuring that the Commission is timely notified of important new or updated information. We seek comment on whether there should be any exceptions to the (30) day requirement.

32. Lastly, we seek comment on whether to adopt any other new rules applicable to SLTE owners and operators, or apply any other existing rules to such entities. Should SLTE owners and operators be subject to certain certification requirements such as cybersecurity certifications? Should we attach additional routine conditions to the blanket license for SLTE owners and operators that would require certain notifications to the Commission? Should the Commission be aware if there is a change in the third-party entity that operates the SLTE to the extent the SLTE owner itself does not operate the SLTE? We seek comment on whether there are national security and law enforcement concerns that we should consider in adopting rules that may be applicable and warranted in the case of SLTE owners and operators. Additionally, we seek comment on whether SLTE and/or SLTE owners and operators are more vulnerable to physical exploitation or attack by foreign adversaries, given their presence on land. Are there are additional measures we should require of SLTE owners and operators to ensure physical security of SLTE and the submarine cable system?

4. SLTE Owner and Operator Foreign Adversary Annual Report

33. Similar to the Foreign Adversary Annual Report that we adopt in the *Report and Order,* we propose to adopt an annual reporting requirement for existing SLTE owners and operators that meet any of the criteria below (SLTE Foreign Adversary Annual Report). We propose a tailored approach under which SLTE owners and operators that do not meet the foreign adversary criteria will not be subject to such reporting requirements. Instead, we propose to limit the reporting requirements to SLTE owners and operators that meet our foreign adversary criteria and thus present potential national security and law enforcement concerns. To the extent SLTE owners and operators demonstrate any of the proposed criteria, it would be indicative of heighted national security and law enforcement concerns and warrant providing relevant information to the Commission on a consistent basis.

34. We propose that SLTE owners and operators that meet one or more of the following criteria must submit an SLTE Foreign Adversary Annual Report to the Commission on an annual basis:

(1) That is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g);

(2) That is identified on the Covered List that the Commission maintains pursuant to the Secure Networks Act; [1]

(3) That has purchased, rented, leased, or otherwise obtained equipment or services on the Commission's Covered List and is using in the submarine cable infrastructure;

(4) Whose authorization, license, or other Commission approval, whether or not related to operation of a submarine cable, was denied or revoked and/or terminated or is denied or revoked and/or terminated in the future on national security and law enforcement grounds, as well as the current and future affiliates or subsidiaries of any such entity; and/or

(5) The submarine cable system for which the SLTE owner and operator is licensed to operate in the United States lands in a foreign adversary country or the SLTE is located or operated from a foreign adversary country, as defined in § 1.70001(f).

The Commission must be able to receive on a regular basis information necessary to ascertain foreign adversary control or ownership of SLTE owners and operators, which is directly relevant to the Commission's oversight role of cable landing licensees. We propose to adopt a requirement for SLTE owners and operators, that meet one or more of the criteria described above, to provide the SLTE Foreign Adversary Annual Report on an annual basis. This will ensure that the Commission has the information it needs to timely monitor and continually assess evolving national security and other risks.

35. The Commission currently does not know the identity of every single owner and operator of SLTE. In the *Report and Order,* the Commission adopted a one-time information collection for the purpose of ascertaining the identities of SLTE owners and operators and location information of the SLTE. We intend to use the information collected to better understand the size of this category of potential licensees so that we can regulate in a reasonably-tailored manner. At this time, however, the Commission also has incomplete information regarding SLTE owners and operators that are owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g). We propose to require SLTE owners and operators to self-identify and fulfill the reporting requirements for the SLTE Foreign Adversary Annual Report.

36. *Content of SLTE Foreign Adversary Annual Report.* For existing SLTE owners and operators that meet the above criteria, we propose to require them to file the STLE Foreign Adversary Annual Report that must include the following information that is current as of thirty (30) days prior to the date of the submission: (1) the information of the SLTE owner and operator as required in § 1.70005(a) through (d), (g), (j)(1); (2) the location(s) of the SLTE(s) that the SLTE owner and operator owns or operates; (3) identify and describe whether the SLTE(s) is managed or operated by a third party; (4) identify and describe whether the SLTE owner and operator leases, sells, shares, or swaps fiber, capacity, or spectrum on a Commission-licensed submarine cable system, including the name of the specific submarine cable system; and (5) certifications as set forth under § 1.70006. We tentatively conclude that requiring this SLTE Foreign Adversary Annual Report will improve the Commission's oversight of certain high-risk SLTE owners and operators. We further propose that SLTE owners and operators must provide a copy of the Foreign Adversary Annual Report directly to the Committee at the time of filing with the Commission. We seek comment on this. In an effort to ease burdens on SLTE owners and operators

[1] Pursuant to sections 2(a) and (d) of the Secure and Trusted Communications Networks Act, and §§ 1.50002 and 1.50003 of the Commission's rules, the Public Safety and Homeland Security Bureau (PSHSB) publishes a list of communications equipment and services that have been determined by one of the sources specified in that statute to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons (''covered'' equipment and services). *See* Secure and Trusted Communications Networks Act of 2019, Public Law 116–124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. 1601–1609 (Secure Networks Act); *see also* 47 CFR 1.50002 and 1.50003; Federal Communications Commission, *List of Equipment and Services Covered by Section 2 of the Secure Networks Act, https://www.fcc.gov/supplychain/coveredlist* (last updated June 5, 2025) (*List of Covered Equipment and Services*). An entity is placed on the Covered List based on a determination made by, among others, an appropriate national security agency that the entity's equipment and/or services pose an unacceptable risk to the national security of the United States or the security and safety of United States persons pursuant to the Secure and Trusted Communications Networks Act of 2019. *See* Secure Networks Act. *See also* 47 CFR 1.50000 *et seq.; List of Covered Equipment and Services.*

that do not meet the above criteria, we seek comment on whether to adopt routine conditions to ensure SLTE owners and operators provide updated information to the Commission as circumstances change.

37. We seek comment on whether an entity that meets one or more of the criteria to file a Foreign Adversary Annual Report and an SLTE Foreign Adversary Annual Report (as both a licensee under § 1.70003(a) or (b) and an SLTE owner and operator) should file both reports every year. If both reports should be required, what timing or reporting deadlines should we consider? Should such entity be permitted to seek a waiver of a requirement to file the SLTE Foreign Adversary Annual Report if it incorporates necessary information about its SLTE ownership and location in the Foreign Adversary Annual Report? Should the Commission instead use a single form for both the SLTE Foreign Adversary Annual Report and the Foreign Adversary Annual Report and require the filer to indicate which annual report it is submitting? We seek comment on our proposed approach and whether there are any other approaches that would reduce burdens on licensees.

*B. New Applicant Certifications and Routine Conditions*

38. Below, we propose to further amend our newly adopted rules by adopting new certification requirements for submarine cable applications and new routine conditions. Generally, we propose to require applicants for a cable landing license or modification, assignment, transfer of control, or renewal or extension of a cable landing license, to certify in their application that they will comply with all of the routine conditions set out in our rules, as amended. We seek comment on these proposals and any burdens on applicants and licensees.

1. Use of Foreign Adversary Entity Equipment

39. We seek comment on whether to require an applicant for a cable landing license to certify, as a condition of the potential grant of an application, that it will not use any equipment in the operation of the submarine cable system that is produced by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g). We propose that notifications of *pro forma* assignments and transfers of control involving cable landing licenses that are granted after the effective date of this *Report and Order* and *FNPRM* must contain a certification that the assignee or the licensee subject to the transfer of control will not use any equipment in the operation of the submarine cable system that is produced by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g). As the Committee notes, in its ''experience, foreign adversaries use a host of seemingly innocuous corporate entities to advance their strategic goals,'' while ''[t]he FCC's 'Covered List' is limited and identifies only a handful of those entities.'' The Committee therefore offers an option, which we propose to adopt, ''going beyond lists [of entities], and instead requir[ing] licensees to certify that they will not use vendors for equipment or services who meet certain qualifications found in other existing national security related regulations.'' After all, ''static lists can be too rigid to account for the full spectrum of actors that may pose risks.'' As the Committee suggests, ''the Commission could require licensees to certify that they will not use vendors for equipment or services who meet the definition of a 'person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary' found in the Department of Commerce's Information and Communications Technology Services rule, 15 CFR 791.2.'' Given our reliance on this definition in this *Report and Order* and in related contexts, we propose to adopt this proposal as to equipment. We seek comment on this proposal.

40. We also seek comment on whether we should apply this certification requirement solely to (1) all equipment; (2) only logic-bearing hardware or software; or (3) only ''communications equipment'' as defined in § 1.50001(d) of the Commission's rules, which includes most equipment with Bluetooth or Wi-Fi connectivity, as reflected in the 2022 *Equipment Authorization Program Report and Order*. This proposed certification could provide the Commission with flexibility to mitigate against evolving or unseen threats from foreign adversaries. In addition, we seek comment on whether to codify this requirement as a routine condition of any cable landing license. Should we apply this routine condition to cable landing licenses held by all licensees, or only those licenses that are granted after the effective date of any new applicable rules we adopt in this proceeding? The Cable Landing License Act authorizes the Commission to ''withhold or revoke'' a license or attach terms and conditions as necessary to serve the statutory purposes, which include promoting national security. Furthermore, the Commission may ''grant such license upon such terms as shall be necessary to assure just and reasonable rates and service in the operation and use of cables so licensed,'' and we believe that all cable landing licenses granted to date have been understood as being subject to the Commission's reservation of regulatory authority. The Commission tentatively concludes that it would have the legal authority to apply such requirements to all licenses, even those granted prior to the adoption of new rules. We seek comment on this tentative conclusion.

2. Prohibition on the Use of Foreign Adversary Entity or Entity Identified on the Covered List as Third-Party Service Providers

41. We propose to adopt a routine condition prohibiting the use of certain third-party service providers to ensure the security, integrity, and resilience of submarine cable systems. The operation of a submarine cable system involves many vendors and contractors, and supply chain integrity is an important priority. We propose to prohibit cable landing licensees from using any third-party service provider in the operation of the submarine cable that is (1) an entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g) of our newly adopted rules, as suggested by the Committee; (2) an entity identified on the Covered List; and/or (3) an entity that can access the submarine cable system from a foreign adversary country, as defined in § 1.70001(f) of our newly adopted rules. We do not apply a strict liability standard, but we expect licensees to conduct substantial due diligence to ensure compliance with FCC requirements. To the extent a licensee conducts substantial due diligence to verify all relevant information and reasonably believes the entity is not owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined herein, such licensee would not be subject to enforcement sanctions. We would consider all of the facts and circumstances raised in an individual case and take into consideration the steps a licensee took in conducting substantial due diligence to ensure compliance with the rule. We believe these measures will further protect critical submarine cable infrastructure from vulnerabilities presented by national security threats. We also propose to require applicants for a cable landing license or modification, assignment, transfer of control, or renewal or extension of a cable landing

license, to certify in the application that they will not use the aforementioned third-party service providers in the operation of the submarine cable. We also propose that notifications of *pro forma* assignments and transfers of control involving cable landing licenses that are granted after the effective date of this *Report and Order* and *FNPRM* must contain this certification for the assignee or the licensee subject to the transfer of control. We also propose to exempt licensees that are themselves owned by, controlled by, or operated by an entity identified on the Covered List, because the Commission assesses that there are few national security benefits in applying this condition to such licensees, given that such entities have themselves already been determined to produce or provide equipment or services that pose an unacceptable risk to national security.

42. We seek comment on these proposals. What would be the potential impact on licensees that currently use the aforementioned third-party service providers? Will this increase costs for licensees significantly? What is the length of time that licensees would need to choose alternative third-party service providers? Should the Commission provide additional guidance on how licensees can verify whether third-party service providers are owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary? For example, should the Commission merely require that licensees exercise their reasonable due diligence in detecting whether third-party service providers meet the definition? If so, what actions by licensees would be necessary and sufficient to support their verification? How would the Commission monitor to ensure that licensees will not use prohibited third-party service providers? Should the Commission adopt specific monitoring, auditing, or verification procedures? What should these look like? For example, should the Commission require third-party auditing of licensees? Should the Commission require annual reporting on all of licensees' contracts with third-party service providers? How can the Commission best ensure compliance while minimizing burdens. Does mitigating the risks presented by untrustworthy third-party service providers outweigh any burdens involved in complying with this prohibition? Should we solely prohibit licensees from entering into new or an extension of existing contracts with the aforementioned third-party service providers, or should we also apply this prohibition to existing contracts that licensees currently may have with such third-party service providers? We seek comment on the costs and benefits of implementing this proposal.

43. In the alternative, should we only prohibit licensees from using a narrower category of third-party service providers, and require licensees to report whether or not they use other third-party service providers, including any of the entities discussed above, in the operation of the submarine cable system? Would this approach strike a balance between our objective to mitigate foreign adversary control and interference in critical submarine cable infrastructure and the burdens on licensees? We seek detailed comments on which third-party service providers we should prohibit or which third-party service providers we should allow licensees to simply disclose to the Commission, as well as justification for any proposed approaches. To the extent we incorporate a reporting requirement under this approach, how frequently should we require licensees to disclose their third-party service providers and what additional information should we require licensees to provide so that we have the necessary visibility into potential threats to submarine cable systems? We seek comment on the costs and benefits of any approaches.

44. *Exception for Repair and Maintenance.* Additionally, we propose an exception to this prohibition where third-party services involve providing repair and maintenance to the wet segment of submarine cables. The Committee noted that if the Commission adopts a broad prohibition on equipment or services produced or provided by entities owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, ''the Committee acknowledges that the Commission might need to allow carve-outs or waivers to address certain circumstances, such as to allow for timely maintenance or restoration of service in the event of outage.'' We propose to simply exempt third-party repair and maintenance services for the wet segment of the cable from the types of third-party services that would be included in this prohibition. We seek comment on this approach. The Commission understands there is heavy industry reliance on Chinese repair and maintenance ships, so not allowing this exception may impose risks of long-term outages. Is this exception necessary, or can industry find vendors for third-party repair and maintenance services without substantial delay, even without this exception? We seek comment on how we should define repair and maintenance services for the wet segment of the cable for the purposes of this exception. Additionally, we seek comment on whether there are other third-party services that we should exempt from the prohibition.

45. *Incentivizing the Use of Non-Foreign Adversary Ships and Repair and Maintenance Services.* In the event that the Commission adopts this exception, or does not adopt the prohibition at all, we seek comment on ways that the Commission can incentivize the use of non-foreign adversary ships and repair and maintenance services. How can the Commission incentivize use of U.S./non-foreign adversary flagged or crewed repair ships, in lieu of reliance on repair ships flagged or crewed by foreign adversaries? Submarine cables, no matter where they are deployed, ''face complex and challenging risks from natural, accidental, and malicious threats.'' When a submarine cable experiences a fault, this causes a disruption that can have ''immediate and far-reaching effects, given the overwhelming reliance our global communication network has on these systems.'' One way to reduce disruption from a cable fault is to increase resiliency to ensure there are many submarine cables deployed that can be used to reroute the traffic to ensure it arrives at its intended destination. Regardless of location, the repairs needed to restore submarine cable service usually require the availability of a specialized repair ship, a cable repair crew that is typically diverse in skill and nationality and may therefore require numerous visas and/or permits due to national cabotage laws, and a window of good weather for the repair work period to ensure safety of the vessel and crew.

46. Submarine cable repair and maintenance services, when conducted by entities subject to the exploitation of foreign adversaries, also present potential opportunities for foreign adversary sabotage, interference, or surveillance of U.S. submarine cables. A recent report from the Center for Strategic and International Studies noted, ''the overreliance on Chinese repair ships due to limited alternatives in the marketplace is another vulnerability if, during a time of military conflict, the Chinese government prohibits access to its repair ships and subsea cables are left damaged without timely repair.'' Cable repair ships are in limited supply, and as a result, this is a growing stressor to the submarine cable industry. Approximately 22 such ships in the

world are dedicated solely to repair, of which only two are U.S.-flagged, and that fleet is aging. If the two U.S.-flagged vessels are unavailable, ''the United States may have to rely on ships outside of its trusted vendor networks, which could introduce security concerns if the ship operators are'' owned by, controlled by, or subject to the jurisdiction of direction of a foreign adversary, as defined in § 1.70001(g) of our newly adopted rules. We seek further information regarding how many existing repair ships are in the trusted vendor network, *i.e.,* outside the ownership, control, jurisdiction, or direction of a foreign adversary.

47. We also seek comment on how the Commission may support or promote the expansion of additional U.S./non-foreign adversary repair ships. Should the Commission also use its submarine cable licensing authority to promote the restoration of U.S. shipbuilding capacity, thus helping to facilitate the recently-announced ''policy of the United States to revitalize and rebuild domestic maritime industries and workforce to promote national security and economic prosperity''? Should the Commission, for example, impose similar requirements for ships that engage in cable repair and maintenance as the Merchant Marine Act of 1920, better known as the Jones Act, imposes on ships that transport cargo between American ports? Should the Commission also give priority to allied-built or owned ships? If so, how should the Commission define ''allied''? Should the Commission rely on the State Department's list of U.S. treaty allies? Should the Commission rely on some combination of ownership, location of the ship was built in, and citizenship of the crew members? Should the Commission instead simply distinguish between those ships owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary as defined in § 1.70001(g) of our newly adopted rules, and those ships that are not? To what extent should the Commission consider broader industrial policy goals, alongside its traditional role in protecting the security of submarine cable infrastructure?

3. Prohibition From Entering Into IRU and Leasing Capacity Arrangements With Entities Identified on the Covered List

48. To further protect U.S. communications networks from national security and law enforcement threats, and consistent with our actions today, we seek comment on adopting a routine condition that would prohibit cable landing licensees from entering into new or an extension of existing arrangements for IRUs or leases for capacity on submarine cable systems landing in the United States, with any entity identified on the Covered List. In the *Report and Order,* we adopt a routine condition that prohibits licensees from entering into new or an extension of existing arrangements for IRUs or leases for capacity on submarine cable systems landing in the United States, where such arrangement for IRUs or lease for capacity would give an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g), the ability to install, own, or manage SLTE on a submarine cable landing in the United States. We believe there are additional national security and law enforcement risks if cable landing licensees enter into such arrangements with entities identified on the Covered List. The entities identified on the Covered List have been found to produce or provide equipment and services that have been deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. We also seek comment on whether to require applicants for a cable landing license or modification, assignment, transfer of control, or renewal or extension of a cable landing license, to certify in the application that they will not enter into new or extension of existing arrangements for IRUs or leases for capacity on submarine cable systems landing in the United States, with any entity identified on the Covered List.

49. This approach is consistent with the actions taken today to prohibit the use of covered equipment and services in new submarine cable systems, to apply a disqualifying condition that will presumptively preclude the grant of a cable landing license filed by any applicant that is identified on the Covered List, and to require existing licensees to certify they will not *add* in their submarine cable systems any equipment or services currently included on the Covered List or any equipment or services subsequently added to the Covered List. We seek comment on whether this routine condition should be subject to any exception granted by the Commission. Should we allow a licensee to petition the Commission for waiver of the condition? To the extent we allow a licensee to petition for a waiver, we propose that any waiver would be granted only to the extent the licensee demonstrates by clear and convincing evidence that a new or extension of an existing arrangement with an entity identified on the Covered List presents no national security nor other threats and would serve the public interest.

4. Notification of Change of Address or Coordinates

50. We also propose to require licensees to notify the Commission of any change of address or geographic coordinates concerning information provided under § 1.70005(e)(7) and (f), within thirty (30) days of the change. In the *Report and Order,* we adopt § 1.70005(e)(7) and (f) requiring an applicant for a cable landing license or modification, assignment, transfer of control, and renewal or extension of a license to provide detailed geographic information about the submarine cable system in the application, including a map and geographic data in generally accepted GIS formats that specifies the location of information described under 1.70005(e)(7) such as each beach manhole, cable landing station, PFE, SLTE, NOC and backup NOC, and SOC and backup SOC, if distinct from the NOC, and the route position list including the wet segment of the submarine cable system. Consistent with this application requirement, we propose to adopt a routine condition requiring a cable landing licensee to notify the Commission within thirty (30) days of any change with respect to any of the information required under § 1.70005(e)(7) and (f). We propose to require licensees to submit a specific description of the updated information, including an updated map and geographic data in generally accepted GIS formats. We propose to delegate authority to OIA, in coordination with OEA, to determine the specific file formats and data fields which will be collected. Consistent with our action in the *Report and Order,* we will provide confidential treatment of the exact location information.

5. Notification of Intent of Non-Renewal of License

51. The Commission currently does not have a formal process, other than outreach to individual licensees, to confirm whether a licensee intends to renew a cable landing license that is nearing the date of expiration. We propose to adopt a routine condition requiring a licensee to notify the Commission within sixty (60) days prior to the date of license expiration if the licensee does not intend to renew or extend the license. If a licensee has already submitted an application to renew or extend the license or requested an STA to continue operating a

submarine cable system, this routine condition will not be applicable as such licensee has expressed an intent to renew or extend the license. Regardless of the timing of any notice of intent not to renew a license, all rights under the license shall terminate upon expiration of the license term unless the licensee has previously filed a renewal application or request for an STA.

6. Notification of Submarine Cable System Retirement

52. We propose to adopt a routine condition requiring a cable landing licensee to notify the Commission within sixty (60) days prior to any retirement of its submarine cable system. Our rules require a licensee to notify the Commission within 30 days of the date the cable is placed into service, whereupon the license will expire 25 years from the in-service date. However, the Commission's rules do not require a licensee to notify the Commission if the submarine cable will be retired and taken out of service. It is important that the Commission maintain up-to-date records of the operational status of licensed submarine cable systems for national security and emergency preparedness and response purposes (for example, in the event of a natural disaster or conflict) and to verify that a licensee is in compliance with Commission rules and the terms of its license. We seek comment on this proposal and whether we should require a licensee to provide any additional information in such notification.

7. Change in Foreign Adversary Ownership

53. We seek comment on whether we should adopt a routine condition requiring cable landing licensees to submit a certification within thirty (30) days of any changes in the licensee's status (*e.g.,* ownership, change in board seats, etc.) that results in the licensee becoming owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g), to the extent such change does not require prior Commission approval under our rules.

8. Change to List of Foreign Adversary Countries

54. We seek comment on whether we should adopt a routine condition requiring cable landing licensees to submit a foreign adversary certification within thirty (30) days of any new additions to the list of foreign adversaries identified in the Department of Commerce's rule, 15 CFR 791.4, or the removal of any countries from this list. Specifically, we seek comment on whether to require licensees to submit a certification that they are or are not owned by controlled by, or subject to the jurisdiction or direction of the foreign adversary newly identified in the Department of Commerce's rule, 15 CFR 791.4. Alternatively, should we only require licensees to submit a certification acknowledging the new addition to the list of foreign adversaries identified in the Department of Commerce's rule, 15 CFR 791.4?

9. Change to the Commission's Covered List

55. We propose to adopt a routine condition that requires licensees, irrespective of when the license was granted, to certify, within sixty (60) days of a **Federal Register** publication announcing any new addition of equipment or services to the Covered List, if they use such Covered List equipment or services in their respective submarine cable system and a brief description of how such equipment or services are used. Is 60 days the right length of time? Should we instead adopt a longer or shorter time length? In the *Report and Order,* we adopt a routine condition for Covered List equipment and services for licenses granted after the effective date of the new rules. In this *FNPRM,* we believe that this proposed routine condition for all licensees, irrespective of when the license was granted, would enable the Commission to account for circumstances where the Covered List evolves and is updated to protect against national security threats and to verify the extent to which such threats exist in critical submarine cable infrastructure. In the alternative, should we require all licensees to report annually if they use any Covered List equipment or services, including any equipment or services newly added prior to the annual reporting deadline? For example, would changes to the Commission's Covered List published in the **Federal Register** before the annual reporting deadline be an appropriate way to define newly added Covered List equipment or services? Should we consider a fixed annual reporting deadline? We seek comment on this approach. To the extent we adopt a certification requirement or an annual reporting requirement, we seek comment on whether to also require licensees to disclose each covered equipment or services that they use in the submarine cable system. What type of information disclosure should we require about the Covered List equipment or service from licensees? Should we require more detailed information? We seek comment on these approaches.

56. This is a continuation of the *Report and Order* adopted today to collect from licensees information about Covered List equipment or services on their respective submarine cable and to certify as to their use of Covered List equipment or services on their respective cable system. Because the information collection or certification will be based on known information as of the time licensees submit these materials, here, we seek comment on our approach to maintain visibility and awareness of Covered List equipment or services used in the licensed submarine cables after there are changes to the Covered List. The potential for a national security risk or threat from newly added entries to the Commission's Covered List in the future may be great and we seek comment on this approach or other approaches to mitigate against these potential risks or threats. Moreover, we seek comment on whether the routine condition should require a licensee to disclose if the licensee does not use the equipment or service that is newly added to the Covered List and if so, whether the licensee should be required to certify that it will not use the equipment or service in the future.

10. Sharing Information From Applications With Federal Agencies

57. We seek comment on adopting a rule which would allow the Commission to share with relevant federal government agencies, including the Committee, information submitted in an application for a cable landing license or modification, assignment, transfer of control, or renewal or extension of a license on a confidential basis without the pre-notification requirements of § 0.442(d) of the Commission's rules. We seek comment, for example, on sharing such information required in § 1.70005 and other rules that reference § 1.70005. Under this approach, the Commission would be able to share the confidential information with federal agencies that have a legitimate need for the information consistent with their functions without the delay attendant to providing parties an opportunity to object to the sharing. The sharing of confidential information would, however, continue to be subject to the requirement that each of the other federal agencies comply with the confidentiality protections applicable both to the Commission and the other agencies relating to the unlawful disclosure of information, and we

would provide notice to the parties whose information is being shared.

58. We tentatively find that Executive Order 13913 provides a basis to share such information with the Committee by establishing that the members and advisors of the Committee have a legitimate need for such information. The policy of Executive Order 13913 is to ensure the ''[t]he security, integrity, and availability of the United States telecommunications networks [that] are vital to United States national security and law enforcement interests.'' Further, in this regard, Executive Order 13913 authorizes the Committee to review not only license applications but also existing licenses. We seek comment on this tentative conclusion.

*C. Presumptively Exempting Applications From Referral to the Executive Branch Agencies*

59. We propose adopting a national security standard that would exclude a submarine cable application from Commission referral to the Executive Branch agencies, if *all* of the qualifications are met that will ensure the security, integrity, and resilience of the submarine cable system. We also note that the Commission would retain the discretion to refer a submarine cable application to the Executive Branch agencies for review for national security, law enforcement, foreign policy, and/or trade policy concerns as circumstances warrant. We seek comment on whether we should establish further guidance on when we will exercise such discretion. We believe that reducing the number of applications that are referred to the Committee would reduce burdens on applicants and enable the Commission and the Committee to prioritize resources on reviewing foreign adversary applications that present significant national security and law enforcement risks warranting closer scrutiny and will allow for expedited review of applications generally. We will continue to work closely with the Committee to assess how we can reduce the number of applications that are referred to the Committee and to streamline the review of those applications that are referred to the Committee, while taking into consideration the U.S. government's equities in national security and law enforcement.

60. Currently, § 1.40001 of the rules states that ''[t]he Commission will generally refer to the [Executive Branch] applications filed for . . . submarine cable landing license[s] as well as an application[s] to assign, transfer control of, or modify those authorizations and licenses where the applicant has reportable foreign ownership . . . .'' Subject to certain exceptions, including the presumptive disqualifications that we adopt today, we currently refer submarine cable applications where an applicant has a foreign owner that directly or indirectly owns 10% or more of the equity interests and/or voting interests, or a controlling interest, of the applicant. The Commission received several comments raising concerns about the lengthy duration of the submarine cable licensing process and encouraging the Commission to use the existing streamlining process and to exercise its discretion in determining which applications to refer to the Committee.

61. The Commission tentatively concludes that extensive delays to submarine cable applications that do not threaten national security or law enforcement interests are not in the public interest. Such delays impose economic costs without national security benefits. Furthermore, not only do such delays not benefit national security; in fact, they may undermine national security by deterring investment in submarine cables and thus reducing the resilience of America's submarine cable network. This is not consistent with the America First Investment Policy or the goals of the Commission. We seek comment on whether this analysis is correct.

62. Specifically, we propose to adopt a national security standard that is a list of qualifications for a submarine cable application—including an application for a cable landing license or modification, assignment, transfer of control, or renewal or extension of such license—to qualify the applicant for exemption from Commission referral to the Committee. We seek comment on the list of qualifications and whether there are other standards that we should adopt to ensure the applicant has met qualifications to ensure the national security of the United States if its application is granted. We propose to require applicants to certify to all of the qualifications below to enable the Commission to verify whether or not the application qualifies for exclusion from Commission referral to the Committee. We propose that our determination of whether an applicant meets each qualification would be considered on a case-by-case basis and in light of the relevant facts and circumstances. We are particularly interested in comments from both the affected industry and the Committee on what qualifications would serve the public interest and protect national security. Additionally, we seek comment on the impact of the Committee's application and license review prioritization based on section 3(a) of Executive Order 14117 on our proposed rules and interaction with the Committee.

1. Recurring Applicants in Good Standing

63. We propose that, to presumptively qualify for exemption, an applicant must be a licensee of a submarine cable licensed by the Commission and has operated its licensed submarine cable(s) without any incident. An applicant in good standing would be, for example, one that has complied with the terms of the license(s) and has no pending or adjudicated enforcement action by the Commission and/or national security, law enforcement, or other concerns brought to the Commission's attention in the course of operating the submarine cable(s) and has no history of false statements or certifications in its dealings before the Commission related to its cable landing license(s). For instance, should we consider that an application meets this qualification if there was no referral of any issue to the Commission's Enforcement Bureau and/or no issuance of a Letter of Inquiry or subpoena at any point in the history of the cable landing license(s) or within a certain timeframe? What would be an appropriate standard or timeframe to ensure that the applicant has demonstrated good standing with the Commission with respect to its licensing obligations in the past? We seek comment on an appropriate timeframe in assessing any history of incidents involving a licensee's operation of its submarine cable.

64. We also seek comment on other incidents, or lack thereof, that we should consider for purposes of assessing an applicant's qualification for exclusion from referral. We note that several commenters support expediting review for applicants whose prior applications were approved, and propose relying on certifications in conjunction with a streamlined process for a ''frequent filer.'' In considering the record, we seek further comment on whether an application should qualify for exclusion from referral if a prior submarine cable application filed by the applicant was recently cleared by the Executive Branch agencies, including the Committee, and granted by the Commission. For instance, should we consider whether a prior application that was filed by the same applicant was cleared by the Executive Branch agencies, with or without mitigation, within the past 18 months from the filing of a new application? Does the timeframe of 18 months following any clearance by the Executive Branch

agencies of such prior application sufficiently account for changed circumstances and an evolving national security and law enforcement environment? Should the timeframe be shorter or longer than 18 months? Should we also consider whether the applicant and/or its existing submarine cable system have no reportable foreign ownership, or no new reportable foreign ownership, as of the Executive Branch agencies' most recent review? We seek comment on these and any other considerations.

65. We seek comment on how we should apply this qualification for recurring applicants in good standing where an applicant is or has previously been a part of a consortium. For example, if multiple joint licensees on a cable landing license hold equal ownership and controlling interests in the submarine cable and operated it without any incident, and one of the licensees files an application for a new cable landing license, should we consider that the applicant has met this standard? Should we require that a licensee must hold a specific threshold of ownership and/or controlling interests in its licensed submarine cable to meet this standard for any submarine cable application it subsequently files? How should we apply this standard if an applicant(s) is a joint licensee of another submarine cable where one of the joint licensees holding less than a majority of the ownership and controlling interests violated the Commission's rules or a condition of the license in the course of operating the submarine cable? We seek comment generally on how we should apply a ''in good standing'' standard where an application is filed by multiple parties, such as an application for a new cable landing license filed by joint applicants or an application filed by any or all of the joint licensees of a submarine cable. To the extent multiple parties file an application, if one applicant meets the qualification but others do not, how should we apply the ''in good standing'' standard with respect to those other applicants? Are there other combinations of scenarios that we should consider?

2. No History of Character Condition Violations

66. We propose that, to presumptively qualify for exemption, an applicant must have consistently demonstrated the requisite character qualifications. Specifically, should we consider an applicant qualifies for the exclusion if in the last 20 years it has not (1) materially violated the Cable Landing License Act where the violation (a) was not remediated with an adjudication involving a consent decree and/or compliance plan, (b) resulted in a loss of Commission license or authorization, or (c) was found by the Commission to be intentional; (2) committed national security-related violations of the Communications Act or Commission rules as identified in Commission orders, including but not limited to violations of rules concerning the Covered List that the Commission maintains pursuant to the Secure Networks Act; (3) made materially false statements or engaged in fraudulent conduct concerning national security or the Cable Landing License Act; (4) been subject to an adjudicated finding of making false statements or engaging in fraudulent conduct concerning national security before another U.S. government agency; or (5) materially failed to comply with the terms of a cable landing license, including but not limited to a condition requiring compliance with a mitigation agreement with the Executive Branch agencies, including the Committee, where the violation (a) was not remediated with an adjudication involving a consent decree and/or compliance plan, (b) resulted in a loss of Commission license or authorization, or (c) was found by the Commission to be intentional? We seek comment on this approach.

3. Enhanced Cybersecurity Standards

67. We propose that, to presumptively qualify for exemption, an applicant must submit a cybersecurity certification consistent with §§ 1.70005(m) and 1.70006(c) of our newly adopted rules, which sets out the requirements of an initial applications for a cable landing license, if such applicant is to qualify for exclusion from Commission referral to the Committee. Should we require a more stringent standard in order to meet this presumptive qualification? Should a requirement of this qualification involve the structuring of a licensee's cybersecurity and physical risk management plans in accordance with higher cybersecurity standards such as the NIST CSF, and a set of established cybersecurity best practices, such as the standards and controls set forth in the CISA CPGs or the CIS Controls? We seek comment on what other cybersecurity standards would be reasonable to require that a licensee implement, if any submarine cable application that it subsequently files is to qualify for exclusion from referral.

4. Physical Security Standards

68. We propose that, to presumptively qualify for exemption, an applicant must certify that it will meet appropriate physical security standards, such as taking all practicable measures to physically secure the submarine cable system (including the cable landing stations, beach manholes and related sites, and SLTEs), if such applicant is to qualify for exclusion from Commission referral to the Committee. We also propose that, in order to qualify for exclusion from referral, applicants must certify they will ensure that individuals who have access to the submarine cable system (including cable landing stations, beach manholes and related sites, and SLTEs) will be screened in accordance with the applicant's security policies. In addition, we propose that, in order to qualify for exclusion from referral, the applicant must certify that it will exclude any company personnel, including contractors, that is a citizen of a foreign adversary country, as defined in § 1.70001(f) of our newly adopted rules, from physical or logical access to the submarine cable system. Finally, we seek comment on the physical security requirements and best practices (*e.g.,* perimeter security, physical barriers, surveillance, environmental controls, security personnel, audit and vulnerability assessments, security awareness training, etc.) that should be required in order for an applicant to meet this presumptive qualification. What other physical security standards should we require in order for an application to qualify for exclusion from referral?

5. No Logic-Bearing Hardware or Software Component Produced by Persons Owned by, Controlled by, or Subject to the Jurisdiction or Direction of a Foreign Adversary

69. We propose that, to presumptively qualify for exemption, an applicant must certify that it will not include any logic-bearing hardware (*e.g.,* readable, writable, and/or programable hardware components) or software in the submarine cable system that is produced by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001 of our newly adopted rules, in order to qualify for exclusion from Commission referral to the Committee. We seek comment on whether we should define what constitutes logic-bearing hardware or software, and if so, what components deployed in a submarine cable system would constitute logic-bearing hardware or software. Alternatively, should we use a slightly narrower definition of ''communications equipment or services,'' as proposed above?

6. No Ownership Below 5% Is Held by Persons Owned, Controlled by, or Subject to the Jurisdiction or Direction of a Foreign Adversary

70. In the *Report and Order,* we retain the requirement that an entity owning or controlling a 5% or greater interest in the submarine cable system and using the U.S. points of the cable system, and any entity that controls a U.S. cable landing station, must be an applicant for a cable landing license. We propose that, to presumptively qualify for exemption, an applicant must certify that no entity holding less than 5% interest in the cable system is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g) of our newly adopted rules. An applicant would meet this standard if no owner of the submarine cable is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g). We seek comment on this proposal. Should we also require that an applicant meets this qualification if any entity that *owns* the U.S. cable landing station also is not owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g)? What other qualifications should we adopt to ensure the cables do not have foreign adversary ownership or control of the infrastructure?

7. Expansion of IRUs and/or Leases of Capacity Prohibitions

71. In the *Report and Order,* we adopt a routine condition that prohibits cable landing licensees from entering into new or an extension of existing arrangements for IRUs or leases for capacity on submarine cable systems landing in the United States, where such arrangement for IRUs or lease for capacity would give an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g) of our newly adopted rules, the ability to install, own, or manage SLTE on a submarine cable landing in the United States. We propose that, to presumptively qualify for exemption, an applicant would need to certify that it will prohibit its customers from entering into new arrangements or extending existing arrangements that would be prohibited for the applicant itself. The applicant would have to adopt contractual provisions that prohibit its buyers or lessors from selling to, leasing out, or swapping the capacity with an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g). We seek comment on this standard.

72. To what extent should we consider whether the capacity sold or leased out by an applicant to another entity is, in turn, sold to, leased out, or swapped with an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g)? Instead of relying solely on contract terms, should we assess whether applicants have taken measures to enforce any such contractual provisions? Should we also require applicants to file with the Commission copies of any arrangements for IRUs or leases of capacity, and if so, should we treat this information as presumptively confidential?

8. No Interconnection With Foreign Adversary Cables

73. We propose that, to presumptively qualify for exemption, an applicant must certify that the submarine cable system will not connect directly or via a branching unit with a submarine cable owned or operated by an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g) of our newly adopted rules, or that lands in a foreign adversary country, as defined in § 1.70001(f). We seek comment on whether this qualification should include other types of connections to submarine cable systems that could present national security risks.

9. No Submarine Cable Repair Ships Operated by Foreign Adversaries

74. We propose to require that, in order to qualify for exclusion from Commission referral to the Committee, an applicant must certify that it will not use a ship for submarine cable installation or repair and maintenance of the submarine cable system that is owned or operated by an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g) of our newly adopted rules, or that is flagged in a foreign adversary country, as defined in § 1.70001(f). We seek comment on whether it is reasonable to require that applicants must meet this qualification in order to qualify for exclusion from referral, or whether restricting the use of such cable installation or repair and maintenance ships would have any adverse impact on owners and operators of submarine cable systems as well as the submarine cable system itself. Alternatively, rather than a prohibition, should we merely require that, an applicant certify that it will implement adequate security measures if it uses any such cable installation or repair and maintenance ships, regardless of whether the ship is operated by an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g)? We seek comment on how applicants will know if a given ship is restricted. Should we rely on applicants' due diligence, require the Commission publish a white list of permissible ships, or use some other method? We seek comment on ways to ensure that this qualification would not curtail or otherwise adversely impact the ability of submarine cable owners and operators to quickly deploy or repair submarine cable systems connecting to the United States.

10. No Senior Officials Owned by, Controlled by, or Subject to the Jurisdiction or Direction of a Foreign Adversary

75. We propose to require that, to presumptively qualify for exemption, an applicant must certify that no senior official of the applicant or the applicant's parent company(ies) is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g) of our newly adopted rules. For purposes of such requirement, we propose to define a senior official as a board member or executive-level management, such as a Chief Executive Officer or Chief Operating Officer. We seek comment on this proposal. Should we adopt a different definition of ''senior official'' for purposes of the proposed requirement? Should we only apply this proposed requirement with respect to the board members or executives of the applicant or the applicant's parent company(ies)?

11. Other Standards

76. We seek comment on whether we should also require that, to presumptively qualify for exemption, an applicant must certify to other measures that are common features of national security agreements with the Committee that concern submarine cables. For example, national security agreements often require that licensees provide the Committee with notice for certain third party access to the submarine cable infrastructure. Should we require that, to presumptively qualify for exemption, an applicant must certify that it will not provide any individual or entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g), or that is identified on the Covered List

with access to certain parts of the submarine cable system, such as the cable landing station(s), NOC(s), and beach manhole(s)? Which parts of the submarine cable system should we include in such a certification? Should we similarly require certification as to access to sensitive U.S. data or domestic communications? How would we define the data that licensees would be prohibited from sharing? Should we also require applicants to certify that they will adopt personnel screening measures to ensure adherence to these requirements? If we required personnel screening measures, what would such a requirement consist of? National security agreements also often contain requirements around incident and breach reporting. Should we require that, to presumptively qualify for exemption, an applicant must certify that it will report certain incidents or breaches to the Commission, such as cyberattacks, unauthorized access, or service disruptions to the Commission? If we adopted such a standard, how would we define the universe of incidents and breaches that would need to be reported? What would be the deadline for incident or breach reporting? 48 hours? More? Fewer? Would the national security benefits of such a reporting requirement outweigh any burden to licensees of providing these reports? What would be the costs and benefits of all of these proposals?

77. We seek comment generally on whether there are any other standards that the Commission should consider to qualify an application for exemption from Commission referral to the Executive Branch agencies. In the alternative, we seek comment on whether we should not refer any applications to the Executive Branch in light of the strong national security measures we adopt in the *Report and Order* and further propose in this *FNPRM,* and whether we should revise § 1.40001 of the rules accordingly.

### *D. Timeframe for Removing Covered Equipment and Services From Submarine Cable System*

78. To further protect U.S. submarine cable networks from national security and law enforcement threats, we seek comment on whether to require existing licensees to remove from their submarine cable system any and all covered equipment or services, within a specified timeframe prior to the expiration of the license. In the *Report and Order,* we find that covered equipment and services that have been deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. Accordingly, we take action to prohibit the use of covered equipment and services identified on the Covered List in new submarine cable systems. We also apply a disqualifying condition that will presumptively preclude the grant of a cable landing license filed by any applicant that is identified on the Covered List. Moreover, we require existing licensees to certify that they will not *add* to their submarine cable systems any current covered equipment or services. However, we believe there remains a critical vulnerability where existing licensees use covered equipment and services in current or future operations of existing submarine cable systems. While we recognize that removal of covered equipment and services from these submarine cable systems may be burdensome to licensees, we believe that allowing the continued use of equipment and services that present unacceptable national security risks is contrary to our objectives to protect this critical U.S. submarine cable networks. We seek comment on this analysis.

79. We seek comment on whether to require a gradual transition away from the use of covered equipment and services in current submarine cable infrastructure, and if so, we seek comment on the appropriate timeframe for the transition. For example, should a requirement to implement a gradual transition away from using covered equipment or services track the remaining term of a cable landing license held by an existing licensee? To the extent an existing licensee seeks to renew or extend a cable landing license upon expiration, we seek comment on whether to require that the licensee must certify that it has removed from the submarine cable system any and all covered equipment or services. In the alternative, should we require such existing licensee to certify that it has a credible plan to remove covered equipment and services within a certain timeframe (*e.g.,* 5 years) and to submit the plan to the Commission? We seek comment on this approach.

80. As an alternative to requiring a transition based on the remaining term of a cable landing license, should we require existing licensees to remove any and all covered equipment or services within a set number of years as of the effective date of any new rule? Is 5 years an appropriate timeframe? Should we adopt a longer or shorter timeframe? What considerations should we review in making a determination about how long to provide for the transition?

81. *Foreign Adversary Annual Report.* Regardless of whether a transition period or a date certain is employed for removing any and all covered equipment or services from an existing submarine cable system, should we in the meantime require such licensees to file a Foreign Adversary Annual Report until such covered equipment or services have been removed? Specifically, should we add a new criterion to newly-adopted rule, § 1.70017(b), to require an existing licensee ''that has purchased, rented, leased, or otherwise obtained equipment or services on the Commission's Covered List and is using in the submarine cable infrastructure'' to file a Foreign Adversary Annual Report consistent with § 1.70017? Would this, in addition to ensuring the Commission has the requisite information, create incentives to remove covered equipment? We seek comment on this approach or if there is another manner in which we can monitor licensees that use covered equipment or services.

### *E. Prioritizing Trusted Technology in Submarine Cable Systems*

82. We seek comment on how the Commission can use its authority pursuant to the Cable Landing License Act and Executive Order 10530, to incentivize and encourage the adoption and the use of trusted technologies produced and provided by the United States and its allies, such that ''American AI technologies, standards, and governance models are adopted worldwide . . .'' How can the Commission leverage the submarine cable licensing regime to ''make [the U.S.] the global partner of choice and the standards setter'' by ''enabl[ing] and encourag[ing] American companies to distribute the American tech stack around the world''? Are there ways we can encourage foreign countries and companies to adopt and use technologies produced and provided by the United States and its allies, as opposed to adopting and using the technologies and produced and provided by foreign adversaries? For example, should the Commission prioritize grants of licenses for submarine cables that land in countries aligned with U.S.-trusted technology standards? Should the Commission prioritize grants of licenses for submarine cables that interconnect to data centers, or other facilities with the necessary infrastructure to support internet traffic exchange, that use trusted technologies, as opposed to technologies produced and provided by foreign adversaries? How should the Commission develop definitions and standards for such a policy?

*F. Artificial Intelligence and Submarine Cable Systems*

83. We seek comment on the use of artificial intelligence in SLTEs in particular, as well as the use of artificial intelligence generally in the submarine cable system as a whole. According to market forecasts, submarine cable operators will likely incorporate artificial intelligence into SLTEs and submarine cables for various reasons. Artificial intelligence, for example, may play a role in improving the function of the submarine cable, such as improving network planning, intelligent traffic routing, and capacity optimization. Artificial intelligence can also safeguard the submarine cable system through predictive maintenance, physical threat detection, and cybersecurity threat detection. While artificial intelligence brings positive attributes to submarine cable operations, we believe that there are significant national security concerns when artificial intelligence technologies involve foreign adversaries. We seek comment on any national security concerns regarding use of artificial intelligence in submarine cable systems. What are the national security impacts and potential threats posed by incorporating artificial intelligence owned by, controlled by, or subject to the direction or jurisdiction of foreign adversaries? Given that submarine cables are critical infrastructure, should we refer assessment of any national security concerns regarding the use of artificial intelligence in submarine cable systems to the Commission's Communications Security, Reliability, and Interoperability Council (CSRIC) for consideration and recommendations?

*G. Additional Measures To Reform and Streamline Rules and Processes*

1. Domestic Cables

84. We seek comment on whether under certain circumstances to streamline approval of domestic cables (*i.e.,* those cables that connect one portion of the United States to another portion of the United States, such as a cable connecting the continental United States to the U.S. Virgin Islands). The Commission currently does not evaluate applications—including applications for a cable landing license or modification, assignment, transfer of control, or renewal or extension of a cable landing license, involving domestic cables (domestic cable applications)—differently than those involving international cables. For cables that connect points solely within the United States and its territories and possessions, NCTA endorsed streamlined review for such cable systems and the Alaska Telecom Association proposed ''streamlined blanket licensing.''

85. A domestic cable application can present national security concerns even if a domestic cable would only connect points within the United States and would not have foreign landing points. For example, a domestic cable application may involve applicants with foreign ownership or propose to use foreign equipment in the cable system. Indeed, several existing domestic cable systems are subject to mitigation agreements with the Committee. We seek comment on whether the certifications we adopt in the *Report and Order* are sufficient to resolve any potential national security or law enforcement concerns and obviate the need for review by the Committee. We seek comment on any national security or law enforcement risks posed by domestic cables that the certifications we adopt in the *Report and Order* may not adequately address.

86. Domestic cable applications are often reviewed by the Committee. We seek comment on reasons why domestic cable applications should undergo review by the Committee and whether the reasons are different than for review of applications involving international cables. If there are national security and law enforcement reasons warranting review by the Committee, are there any mechanisms the Commission and Committee could employ to reduce the time for review of a domestic cable application? Are there any other methods we should consider to streamline review of domestic cable applications in light of the policies adopted in the *Report and Order* and contemplated elsewhere in this *FNPRM*? Are there any other submarine cable rules that the Commission should consider modifying or eliminating in the context of domestic cables?

2. Mitigation Agreements

87. We seek comment on how the Commission can and should modify and streamline any existing cable license conditions that were based on previous mitigation agreements once our rules are in effect. We have made significant regulatory changes to address national security concerns and prior mitigation agreements may not have consistent requirements to ensure the safety and security of submarine cables. Should we, for example, modify and streamline any existing license terms that were based on mitigation agreements, which include Letters of Agreements (LOAs) and National Security Agreements (NSAs), to ensure they are in line with the principles behind our new rules adopted in the *Report and Order*? Should we focus our efforts on modifying license terms based on domestic cable mitigation agreements, such as focusing first on those entered into prior to the effective date of the rules? Should the Commission adopt a procedure that permits licensees of domestic cable systems to attest to the certifications we adopt in the *Report and Order* in order for the Commission to remove license conditions requiring compliance with a mitigation agreement? Can and should the Commission consider modifying or streamlining all license conditions that were based on mitigation agreements generally? What methods could the Commission employ to provide all licensees the intended benefit of consistent national security requirements? We seek comment on how the Commission can and should modify and streamline any existing license terms based on prior mitigation agreements consistent with the principles articulated in the *Report and Order.*

3. Other Agencies and Processes That Address Submarine Cables

88. We recognize that the Commission is not the only agency in the Federal Government that interfaces with submarine cable systems. There are other agencies and regulatory processes that rely on submarine cables for many uses, including government contracts, use of submarine cables for commercial service, and/or reliance on submarine cables for critical missions. Some agencies outside of the Commission include those agency members of the Committee, the Committee on Foreign Investment in the United States (CFIUS), and the Defense Priorities and Allocations System (DPAS), among others. We seek comment on what impacts, if any, the Commission's adopted rules in the *Report and Order* and proposed rules in this *FNPRM* have on these other agencies, government contracts, and processes generally. We seek comment on whether the Commission should reconsider any proposals to better address the interrelationships among the various agencies and processes that affect submarine cables. Additionally, should we reconsider or revise § 1.70007(c) of our newly adopted rules, which requires that licensees shall at all times comply with any requirements of U.S. government authorities regarding the location and concealment of the cable facilities, buildings, and apparatus for the purpose of protecting and safeguarding the cables from injury or

destruction by enemies of the United States? Do the costs of the requirement outweigh the national security and law enforcement benefits?

*H. Alternative Definition of ''Foreign Adversary'' and ''Foreign Adversary Country''*

89. Subsequent to the issuance of the *2024 Cable NPRM,* the Department of Justice issued rules pursuant to Executive Order 14117 (''Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern''). Those rules defined ''country of concern'' as, ''any foreign government that, as determined by the Attorney General with the concurrence of the Secretary of State and the Secretary of Commerce: (a) 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 (b) 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.'' Furthermore, the rules listed ''countries of concern'' as China, Cuba, Iran, North Korea, Russia, and Venezuela, identical to the list of foreign adversary countries in our rule, 47 CFR 1.70001(g). Given the relevance of these rules to our efforts to safeguard submarine cables against threats from foreign adversaries, we seek comment on whether we should incorporate this definition and these determinations into our rules. If so, how? For example, should we include in the definition of ''foreign adversary country'' any country that in the Commerce Department or Justice Department lists? We seek comment on alternative approaches.

*I. Costs and Benefits*

90. We seek comment on the potential benefits and costs of the proposals discussed throughout this *FNPRM.* We believe that the rule changes identified in the *FNPRM* would advance the United States' national security, law enforcement, foreign policy, and trade policy. We expect that these proposals will streamline our rules and processes, and strengthen our oversight of submarine cable systems that reach the United States by increasing the quality and granularity of data and information about these cable systems, including the identity of entities with ownership interests or control of this critical infrastructure.

91. Among the proposals in the *FNPRM,* we propose concrete steps to build upon the *Report and Order* and recent proceedings to prevent national security risks from current and potential foreign adversaries, while encouraging the use of trusted technology and measures to further accelerate the buildout of submarine cables. We propose and seek comment on a regulatory framework that would require entities that own or operate SLTEs to become licensees. We propose granting SLTE owners and operators a blanket license, subject to certain exclusions and routine conditions, to reduce burdens to industry and encourage the investment and deployment of submarine cable systems. As a condition of any grant of a blanket license, in addition to the conditions for all licensees, we also propose to require existing SLTE owners and operators that are owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, or other relevant criteria, to submit a tailored SLTE Foreign Adversary Annual Report to ensure that the Commission maintains consistent oversight over their operations. In addition, we propose new certifications and routine conditions related to foreign adversaries to further protect submarine cables from national security risks. Moreover, we propose an approach to expedite deployment of submarine cables that connect to the United States by presumptively excluding submarine cable applications from referral to the Executive Branch agencies if they meet certain standards. Finally, we propose and broadly seek comment on additional measures to reform and streamline the submarine cable licensing rules and processes, with the goal of accelerating and enhancing the buildout of submarine cable infrastructure, and seek comment on the costs and benefits of the proposed rules and any alternatives.

92. The benefits of the proposed rules are difficult to quantify, as they extend to our national security and public interest responsibilities. We expect that the rules we propose will allow us to build upon the *Report and Order* and recent proceedings to prevent current and potential foreign adversary control and interference in submarine cables. Furthermore, our proposals to develop a framework for SLTEs will allow us to mitigate physical and logical access risks to U.S. submarine cable systems. Moreover, we expect our proposed rules to reform and streamline the application process, saving valuable time and resources for licensees who meet national security conditions. We seek comment on the expected benefits of the proposals in the *FNPRM.*

93. Our estimate of costs should include all of the expected costs that would be incurred as a result of the rules proposed in the *FNPRM,* including the costs of additional data collection concerning SLTEs, reporting costs, and the costs of enforcing our additional requirements. We note that the annual aggregate cost of the proposed rules described above could vary, depending on the rules adopted. We tentatively conclude that the benefits of establishing the proposed rules—which include the safety and reliability of the submarine cable systems and the protection of national security and law enforcement interests—will be in excess of these costs.

94. We seek comment on the costs that applicants will incur from the new requirements detailed above. We expect that our proposal to expedite applications that meet national security conditions will result in significant cost savings for licensees by reducing the time and resources required to prepare these applications. We seek comment on the estimated cost savings that would accrue if these rules are adopted. We also seek comment on any additional costs on licensees, including on small entities.

## IV. Procedural Matters

95. The Commission has also prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning the potential impact of rule and policy change proposals on small entities in the *FNPRM.* The IRFA is set forth in Appendix D. The Commission invites the general public, in particular small businesses, to comment on the IRFA. Comments must be filed by the deadlines for comments on the *FNPRM* indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

96. *Paperwork Reduction Act.* The *FNPRM* may contain proposed new or modified information collections. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on any information collections contained in this document, as required by the Paperwork Reduction Act of 1995, 44 U.S.C. 3501–3521. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

97. *Ex Parte Presentations-Permit-But-Disclose.* The proceeding this *FNPRM*

initiates shall be treated as a ''permit-but-disclose'' proceeding in accordance with the Commission's *ex parte* rules. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.,* .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

98. *Providing Accountability Through Transparency Act.* Consistent with the Providing Accountability Through Transparency Act, Public Law 1189, a summary of this *FNPRM* will be available on *https://www.fcc.gov/proposed-rulemakings.*

99. *OPEN Government Data Act.* The OPEN Government Data Act requires agencies to make ''public data assets'' available under an open license and as ''open Government data assets,'' *i.e.,* in machine-readable, open format, unencumbered by use restrictions other than intellectual property rights, and based on an open standard that is maintained by a standards organization. This requirement is to be implemented ''in accordance with guidance by the Director'' of the OMB. The term ''public data asset'' means ''a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under [the Freedom of Information Act (FOIA)].'' A ''data asset'' is ''a collection of data elements or data sets that may be grouped together,'' and ''data'' is ''recorded information, regardless of form or the media on which the data is recorded.''

100. *Filing Requirements—Comments and Replies.* Pursuant to §§ 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments and reply comments in response to the *FNPRM* on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings,* 63 FR 24121 (1998).

101. *Availability of Documents.* Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS. When the FCC Headquarters reopens to the public, these documents will also be available for public inspection during regular business hours in the FCC Reference Center, Federal Communications Commission, 45 L Street NE, Washington, DC 20554.

102. *Further Information.* For further information, contact Desiree Hanssen of the Office of International Affairs, at 202–418–0887 or *Desiree.Hanssen@fcc.gov.*

## V. Initial Regulatory Flexibility Analysis

103. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the policies and rules proposed in the *FNPRM* assessing the possible significant economic impact on a substantial number of small entities. The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments specified on the first page of the *FNPRM.* The Commission will send a copy of the *FNPRM,* including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). In addition, the *FNPRM* and IRFA (or summaries thereof) will be published in the **Federal Register**.

### *A. Need for, and Objectives of, the Proposed Rules*

104. In this *FNPRM,* we propose to build upon the efforts adopted in the *Report and Order* to prevent national security risks from current and potential foreign adversaries, while encouraging the use of trusted technology and measures to further accelerate the buildout of submarine cables. We propose to and seek comment on a regulatory framework that would require entities that own or operate submarine line terminal equipment (SLTE), including any that may be small business entities, to become licensees. We propose granting SLTE owners and operators a blanket license, subject to certain exclusions and routine conditions, to reduce burdens to industry and encourage the investment in and deployment of submarine cable systems. As a condition of any grant of a blanket license, in addition to the conditions for all licensees, we also propose to require SLTE owners and operators that are owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, or other relevant criteria, to submit a tailored annual report (SLTE Foreign Adversary Annual Report) to ensure that the Commission maintains consistent oversight over their operations.

105. We propose new certifications and routine conditions related to foreign adversaries to further protect submarine cables from national security risks as explained in detail in the *FNPRM.* For example, we seek comment on whether to require an applicant for a cable landing license to certify, as a condition of the potential grant of an application, that it will not use any equipment in the operation of the submarine cable system that are produced by entities that are ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'' as defined in the *Report and Order.* Another example, we propose to adopt a routine condition prohibiting the use of certain third-party service providers and propose to adopt related certifications, to ensure the security, integrity, and resiliency of submarine cable systems. We also seek comment on adopting a routine condition that would prohibit cable landing licensees from entering into new or an extension of existing arrangements for IRUs or leases for capacity on submarine cable systems landing in the United States, with any entity identified on the Covered List. We propose routine conditions that would require licensees to submit notifications of important changes to the submarine cable system, and seek comment on adopting routine

conditions that would require cable landing licensees to submit certifications in the event of changes that result in a licensee becoming owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, or changes to the Department of Commerce's list of foreign adversary countries, or changes to the Covered List.

106. We propose an approach to expedite deployment of submarine cables that connect to the United States by presumptively excluding submarine cable applications from referral to the Executive Branch agencies if they meet certain standards. To further protect U.S. submarine cable networks from national security and law enforcement threats, we seek comment on whether to require existing licensees to remove from their submarine cable system any and all covered equipment or services, within a specified timeframe prior to the expiration of the license. We also seek comment on how the Commission can use its authority pursuant to the Cable Landing License Act and Executive Order 10530, to incentivize and encourage the adoption and the use of trusted technologies produced and provided by the United States and its foreign allies. We seek comment on whether under certain circumstances to streamline approval of domestic cables. Finally, we seek comment on the costs and benefits of the proposed rules and any alternatives, including the impact of the proposed rules on small entities and alternative approaches.

*B. Legal Basis*

107. The proposed action is authorized pursuant to sections 1, 4(i), 4(j), 201–255, 303(r), 403, and 413 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i), 154(j), 201–255, 303(r), 403, and 413, and the Cable Landing License Act, 47 U.S.C. 34–39, and Executive Order No. 10530, section 5(a), (May 12, 1954) reprinted as amended in 3 U.S.C. 301.

*C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply*

108. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted. The RFA generally defines the term ''small entity'' as having the same meaning as the terms ''small business,'' ''small organization,'' and ''small governmental jurisdiction.'' In addition, the term ''small business'' has the same meaning as the term ''small business concern'' under the Small Business Act.'' A ''small business concern'' is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.

109. *All Other Telecommunications.* This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Providers of internet services (*e.g.,* dial-up ISPs) or Voice over Internet Protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $40 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Based on this data, the Commission estimates that the majority of ''All Other Telecommunications'' firms can be considered small.

110. *Computer Infrastructure Providers, Data Processing, Web Hosting, and Related Services.* This industry comprises establishments primarily engaged in providing computing infrastructure, data processing services, Web hosting services (except software publishing), and related services, including streaming support services (except streaming distribution services). Cloud storage services, computer data storage services, computing platform infrastructure provision Infrastructure as a service (IaaS), optical scanning services, Platform as a service (PaaS), and video and audio technical streaming support services are included in this industry. Data processing establishments provide complete processing and specialized reports from data supplied by clients or provide automated data processing and data entry services. The SBA small business size standard for this industry classifies firms with annual receipts of $40 million or less as small. U.S. Census Bureau data for 2017 indicate that 9,058 firms in this industry were operational for the entire year. Of this total, 8,345 firms had revenue of less than $25 million. Thus, under the SBA size standard the majority of firms in this industry are small.

111. *Competitive Local Exchange Carriers (CLECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 3,378 providers that reported they were competitive local service providers. Of these providers, the Commission estimates that 3,230 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

112. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 127 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 109 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

113. *Internet Publishing and Broadcasting and Web Search Portals.* This industry comprises establishments primarily engaged in (1) publishing and/or broadcasting content on the internet exclusively or (2) operating websites

that use a search engine to generate and maintain extensive databases of internet addresses and content in an easily searchable format (and known as Web search portals). The publishing and broadcasting establishments in this industry do not provide traditional (non-internet) versions of the content that they publish or broadcast. They provide textual, audio, and/or video content of general or specific interest on the internet exclusively. Establishments known as web search portals often provide additional internet services, such as email, connections to other websites, auctions, news, and other limited content, and serve as a home base for internet users. The SBA small business size standard for this industry classifies firms having 1,000 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were firms that 5,117 operated for the entire year. Of this total, 5,002 firms operated with fewer than 250 employees. Thus, under this size standard the majority of firms in this industry can be considered small.

114. *Internet Service Providers (Non-Broadband).* Internet access service providers using client-supplied telecommunications connections (*e.g.,* dial-up ISPs) as well as VoIP service providers using client-supplied telecommunications connections fall in the industry classification of All Other Telecommunications. The SBA small business size standard for this industry classifies firms with annual receipts of $40 million or less as small. For this industry, U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Consequently, under the SBA size standard a majority of firms in this industry can be considered small.

115. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, in general, a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses. Next, ''small organizations'' are not-for-profit enterprises that are independently owned and operated and not dominant their field. While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees. Finally, ''small governmental jurisdictions'' are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand. Based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.

116. *Wired Broadband Internet Access Service Providers (Wired ISPs).* Providers of wired broadband internet access service include various types of providers except dial-up internet access providers. Wireline service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules. Wired broadband internet services fall in the Wired Telecommunications Carriers industry. The SBA small business size standard for this industry classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees.

117. Additionally, according to Commission data on internet access services as of June 30, 2024, nationwide there were approximately 2,204 providers of connections over 200 kbps in at least one direction using various wireline technologies. The Commission does not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, in light of the general data on fixed technology service providers in the Commission's *2024 Communications Marketplace Report,* we believe that the majority of wireline internet access service providers can be considered small entities.

118. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.

119. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged in the provision of fixed local services. Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

### *D. Description of Economic Impact and Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities*

120. The RFA directs agencies to describe the economic impact of proposed rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirements and the type of professional skills necessary for preparation of the report or record.

121. The *FNPRM* proposes rules that would impose new, additional reporting, recordkeeping, or other compliance obligations on small entities. The proposed rule changes identified in the *FNPRM* would advance United States' national security and economic security through protecting submarine cable infrastructure and promoting U.S. trusted technologies. We expect that these proposals will streamline our rules and processes, including for any small entities, and strengthen oversight of submarine cable systems that reach the United States. The *FNPRM* propose to presumptively

exclude submarine cable applications from referral to the Executive Branch agencies if they meet certain standards, which could potentially assist small entities. The *FNPRM* seeks comment on additional approaches, such as a requirement for existing licensees to remove from their submarine cable system equipment and services identified on the Covered List within a specified timeframe prior to the expiration of the license and streamlined approval of submarine cables that connect one portion of the United States to another portion, *i.e.,* domestic cables. We seek comment on ways the Commission can incentivize adoption and use of trusted technologies produced and provided by the United States and its foreign allies. The *FNPRM* proposes rules requiring applicants to certify that they will not use equipment or services on the submarine cable produced or provided by entities that are ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,'' as defined in rules adopted in the *Report and Order*. The *FNPRM* seeks comment on prohibiting licensees from using third-party service providers owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, identified in the Covered List, or that can access the submarine cable system from a foreign adversary country. We propose requiring applicants to provide cable installation, maintenance and repair plans with their application, recognizing that this rule proposal may ultimately affect small entities. Finally, we propose and seek comment on additional measures to reform and streamline the submarine cable licensing rules and processes and seek comment on the costs and benefits of the proposed rules and any alternatives.

122. The *FNPRM* proposes requiring SLTE owners and operators to become licenses but, to reduce burdens, proposes to grant these entities blanket licenses. The blanket licensing proposal would prevent any SLTE owner from having to apply for a license or for a modification to the license they already possess, making the licensing requirement cost-free for licensees. The *FNPRM* seeks comment on requiring SLTE owners and operators to comply with the routine conditions required of existing licensees, which may include filing annual circuit capacity reports. We seek comment on requiring SLTE owners and operators who meet the criteria for filing a Foreign Adversary Annual Report to file such a report. At this time, it is difficult to determine the number of SLTE owners and operators that this would impact. Additionally, we seek comment on whether to apply prior approval and/or post-consummation transaction requirements to SLTE owners and operators. Such a requirement, if adopted, would impose the cost of reporting pro forma transfers of control or assignments of licenses on SLTE owners, and of seeking Commission approval for substantive transfers of control or assignments prior to the transaction.

123. We also seek comment on a requirement to provide submarine cable installation, maintenance, and repair plans to the Commission upon request, which we do not anticipate to be costly as the licensee will likely already produce such plans in the ordinary course of business.

124. We seek comment on new routine conditions for all licensees, including requiring licensees to notify the Commission for changes to the coordinates or addresses for each beach manhole, cable landing station, or network operations center (NOC); notification of a licensee's license expiration and intent of non-renewal or non-extension of the license; notification of a system retirement; certification for changes to foreign adversary ownership of a licensee; and certification for changes to the foreign adversary country list. We propose to require a certification of changes to the Covered List. The cost of compliance for a licensee would vary depending on how often the licensee undergoes any of the experiences that would trigger a notification or certification to the Commission. We anticipate that the information the Commission seeks would be information licensees would already possess in the ordinary course of business.

125. The *FNPRM* seeks comment on whether to require licensees to gradually transition away from use of equipment and services identified on the Covered List in their submarine cable system. We anticipate such a requirement may be burdensome to licensees, including any small business or small entity licensees, and seek comment on minimizing those burdens.

126. Our estimate of costs should include all of the expected costs that would be incurred as a result of the rules proposed in the *FNPRM,* including the costs of additional data collection concerning SLTEs, reporting costs, and the costs of enforcing our additional requirements. We note that the annual aggregate cost of the proposed rules described above will vary, depending on the rules adopted. We estimate that our proposal to require SLTE owners and operators to be licensees in new submarine cable system applications will increase costs for applicants by approximately $18,200 per SLTE owner and operator. We seek comment on the number of SLTE owners and operators that will be added as licensees to each new application. Moreover, we expect that our proposal to expedite applications that meet national security conditions will result in significant cost savings for licensees by reducing the time and resources required to prepare these applications. We seek comment on the estimated cost savings that would accrue if these rules are adopted. We also seek comment on any additional costs on licensees, including on small entities.

127. We are especially interested in estimates that address alternative means to provide the same benefits, in terms of protecting submarine cable infrastructure from national security risks, at lower costs. The Commission expects the information we receive in comments including, where requested, cost and benefit analyses, will help to identify and evaluate relevant compliance matters for small entities, including compliance costs and other burdens that may result if the proposals and associated requirements discussed in the *FNPRM* are adopted.

### *E. Discussion of Significant Alternatives Considered That Minimize the Significant Economic Impact on Small Entities*

128. The RFA directs agencies to provide a description of any significant alternatives to the proposed rules that would accomplish the stated objectives of applicable statutes, and minimize any significant economic impact on small entities. The discussion is required to include alternatives such as: ''(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities.''

129. As described in the *FNPRM,* we consider and seek comment on the potential impact and burdens our proposed rules would generally have on submarine cable applicants and licensees, including owners of SLTE, some of whom may be small entities. As part of our proposals, we discuss alternative options that could potentially reduce the impacts and burdens with respect to small entities

and more generally for entities subject to the Commission's submarine cable rules.

130. We considered the burdens on SLTE owners in our proposal to extend licensing requirements to SLTE owners, by proposing blanket licensing that would prevent SLTE owners from having to apply for a license or for a modification to an existing license. We do not know how many SLTE owners are small businesses, but our proposal to minimize the burden on SLTE owners of proposed licensing would also lighten the burden on small business SLTE owners.

131. We seek comment on the burdens of applicants submitting cable installation and maintenance and repair plans with their application, and on licensees if a routine condition were imposed requiring their cable installation and repair plans. The major alternative to these proposals is opting not to impose them if the burdens are too onerous and outweigh the benefits.

132. We propose additional requirements on licensees' cybersecurity and physical security risk management plans. We seek comment which standards and best practices to use, proposing alternatives such as National Institute of Standards and Technology Cybersecurity Framework, Cybersecurity & Infrastructure Security Agency Cybersecurity Cross sector Performance Goals and Objectives, or the Center for Internet Security's Critical Security Controls (CIS Controls).

133. We seek comment on whether to impose routine conditions tailored to SLTE owners and operators who may become licensees, and in doing so seek comment on which routine conditions are warranted; the contemplated alternatives include refraining from imposing any or all of them.

134. We seek comment on a broad range of timelines for transitioning licensees away from use of equipment and services on the Covered List, and seek comment on alternatives such as having licensees submit their own plan for removal of covered equipment and services within a specified timeframe.

135. We also contemplate a number of proposals to expedite or streamline submarine cable applications, including expediting review of domestic U.S. cables and excluding from referral to the Executive Branch applicants which meet certain requirements, which could benefit any submarine cable licensees who are small businesses.

*F. Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rules*

136. None.

## VI. Ordering Clauses

137. *It is ordered* that, pursuant to sections 1, 4(i), 4(j), 201–255, 303(r), 403, 413 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i), 154(j), 201–255, 303(r), 403, 413, and the Cable Landing License Act of 1921, 47 U.S.C. 34–39, and Executive Order No. 10530, section 5(a) (May 12, 1954) reprinted as amended in 3 U.S.C. 301, this Further Notice of Proposed Rulemaking *is hereby adopted.*

138. *It is further ordered* that the Office of the Managing Director, Performance Program Management, *shall send* a copy of this Further Notice of Proposed Rulemaking in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. 801(a)(1)(A).

139. *It is further ordered* that the Commission's Office of the Secretary *shall send* a copy of this Further Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analyses, to the Chief Counsel for Advocacy of the Small Business Administration.

Federal Communications Commission.

**Aleta Bowers,**

*Federal Register Liaison Officer, Office of the Secretary.*

[FR Doc. 2025–19657 Filed 10–24–25; 8:45 am]

**BILLING CODE 6712–01–P**

# Notices

Federal Register
Vol. 90, No. 205
Monday, October 27, 2025

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 COMMERCE

### Patent and Trademark Office

**[Docket No.: PTO–P–2025–0182]**

### Streamlined Claim Set Pilot Program

**AGENCY:** United States Patent and Trademark Office, Department of Commerce.

**ACTION:** Notice.

**SUMMARY:** The United States Patent and Trademark Office (USPTO) is implementing the Streamlined Claim Set Pilot Program to evaluate how having a limited number of claims under examination impacts pendency and examination quality. Under the pilot program, certain pending utility patent applications that have no more than one independent claim and no more than ten total claims may be eligible for expedited examination, if the requirements specified in this notice are met. An applicant may comply with the claim requirements of the pilot program by filing a preliminary amendment before or with a petition to make special under the pilot program. Applications accepted into the pilot program will be advanced out of turn (*i.e.,* accorded special status) for examination until a first Office action is issued. This notice sets forth the requirements of the pilot program and describes how the pilot program will be administered. The USPTO anticipates that focusing examination resources on already-filed, unexamined applications that have a streamlined claim set will enhance efforts to reduce the USPTO's inventory and pendency, and that the data gathered from this pilot program will support designing future efforts to expedite patent examination.

**DATES:** *Pilot Duration:* The Streamlined Claim Set Pilot Program will accept petitions to make special beginning October 27, 2025, until either October 27, 2026 or the date each Technology Center that examines utility applications has been docketed at least approximately 200 applications accepted into the pilot program, whichever occurs first. The USPTO recognizes that participation in the pilot program across Technology Centers may vary. Disparities in participation across Technology Centers, such as when the pilot program applications accepted in a Technology Center significantly exceeds 200, may result in early termination of the pilot program. The USPTO may, at its sole discretion, terminate the pilot program for any reason, including factors such as workload and resources needed to administer the program, feedback from the public, and the effectiveness of the program. If the pilot program is terminated, the USPTO will notify the public. The USPTO, on its website, will specify the number of petitions filed and the number of applications accepted into the pilot program for each Technology Center. A petition filed under the pilot program before the termination of the program will be considered on its merits.

**FOR FURTHER INFORMATION CONTACT:** Nicholas Hill, Legal Advisor, Office of Patent Legal Administration, Office of the Deputy Commissioner for Patents, at *Nicholas.Hill@uspto.gov;* or Kristie A. Mahone, Senior Legal Advisor, Office of Patent Legal Administration, Office of the Deputy Commissioner for Patents, at *Kristie.Mahone@uspto.gov.* For questions on electronic filing, please contact the Electronic Business Center at 866–217–9197 or *ebc@uspto.gov*. For questions relating to a particular petition, please contact the Office of Petitions at 571–272–3282.

**SUPPLEMENTARY INFORMATION:** New patent applications ordinarily are taken up for examination in the order of their U.S. filing date or national stage entry date. *See* sections 708 and 1893.03(b) of the Manual of Patent Examining Procedure (MPEP) (9th Edition, Rev. 01.2024, November 2024). The USPTO has procedures to advance out of turn (accord special status) the examination of a utility application, provided that the applicant files (1) a petition to make special, or (2) a request for prioritized examination. *See* 37 CFR 1.102 and *Discontinuation of the Accelerated Examination Program for Utility Applications,* 90 FR 24324 (June 10, 2025) (final rule).

To qualify for the Streamlined Claim Set Pilot Program, an applicant must file a timely petition to make special under the pilot program in an original (non-reissue),[1] noncontinuing, utility application filed under 35 U.S.C. 111(a) before October 27, 2025. National stage applications filed under 35 U.S.C. 371 are not eligible for participation in the pilot program. The petition to make special under the pilot program must be filed with the petition fee under 37 CFR 1.17(h) before the issuance of a first Office action, including a written restriction requirement. An applicant should not file a petition to make special under the pilot program in an application that is already docketed to an examiner. The USPTO will generally dismiss a petition under the pilot program if the application has already been docketed to a particular examiner in a Technology Center at the time the petition is taken up for decision.

To be eligible for the pilot program, an application must have no more than one independent claim, no more than ten total claims, no multiple dependent claims, and all claims other than the independent claim must comply with the dependency format specified in this notice. An applicant may comply with the claim requirements of the pilot program by filing a preliminary amendment before or with the petition to make special. The entry of such a preliminary amendment will not, however, be contingent upon the grant of the petition to make special. An applicant must also certify that no inventor or joint inventor has been named as the inventor or a joint inventor on more than three other nonprovisional applications in which a petition to make special under this program has been filed. Applications accepted into the program will be advanced out of turn (*i.e.,* accorded special status) for a first Office action. After the first Office action, the application will no longer be treated as special during examination.

#### Definition

*Noncontinuing application:* A noncontinuing application is an application that is not a continuation, divisional, or continuation-in-part application filed under the conditions specified in 35 U.S.C. 120, 121, 365(c),

[1] *See* section 201.02 of the MPEP (''`Original' application is used in the patent statutes and rules to refer to an application which is not a reissue application.'').

or 386(c) and 37 CFR 1.78. *See* section 201.02 of the MPEP.

Any application that claims the benefit of the filing date of a prior-filed application that is a nonprovisional U.S. application and/or international application designating the United States is not eligible for participation in the pilot program. Claiming the benefit under 35 U.S.C. 119(e) of one or more prior provisional applications or claiming a right of priority under 35 U.S.C. 119(a)–(d) or (f) to one or more foreign applications will not affect eligibility for the program.

**Part I. Requirements To Participate**

The petition to make special must be properly signed and accompanied by the fee set forth in 37 CFR 1.17(h), as required by 37 CFR 1.102(d). The patent application and the petition must meet the following requirements.

*(1) Types of Applications and Time for Filing Petition*

The pilot program is available for original, noncontinuing, utility applications filed under 35 U.S.C. 111(a). The application must have an actual filing date that is before October 27, 2025. The petition to make special under the pilot program must be filed before the issuance of a first Office action, including a written restriction requirement. Because preparing a first Office action may begin soon after an application is docketed to an examiner, the USPTO will, as stated above, generally dismiss a petition under the pilot program if the application has already been docketed to a particular examiner in a Technology Center at the time the petition is taken up for decision.

*(2) The USPTO Form Required for Filing Petition*

Form PTO/SB/472, titled ''CERTIFICATION AND PETITION TO MAKE SPECIAL UNDER THE STREAMLINED CLAIM SET PILOT PROGRAM,'' must be used to submit the petition under the pilot program (available at *www.uspto.gov/PatentForms*). Form PTO/SB/472 contains the certification statements and agreement required for participation in the pilot program, and information about the required fee. Use of the form will enable the USPTO to quickly identify and timely process the petition. In addition, use of the form will help applicants understand and comply with the petition requirements of the pilot program. Under 5 CFR 1320.3(h), form PTO/SB/472 does not collect ''information'' within the meaning of the Paperwork Reduction Act of 1995.

*(3) Claim Limit, No Multiple Dependent Claims, Dependency Format, and Agreement*

When the petition to make special is filed, the application must contain no more than one independent claim, no more than ten total claims, and no multiple dependent claims. All claims other than the single independent claim must comply with the dependency format specified below.

For applications accepted into the pilot program, the examiner may refuse entry of any amendment that, if entered, would result in a set of pending claims with more than one independent claim, more than ten total claims, or a multiple dependent claim. The examiner may also refuse entry of any amendment that would result in a claim other than the independent claim being noncompliant with the dependency format specified in this notice. An applicant may meet the claim requirements of the pilot program by filing a preliminary amendment in compliance with 37 CFR 1.121 before or with the petition to make special. *See* section 714 of the MPEP, subsection II, for more information on the manner of making amendments under 37 CFR 1.121. The preliminary amendment may accompany the petition to make special. Preliminary amendments filed after the petition to make special is filed will not be considered when deciding the petition. A preliminary amendment reducing the number of claims will not entitle an applicant to a refund of previously paid excess claims fees. *See* section 607 of the MPEP, subsection III.

To comply with the dependency format for this pilot program, a claim must be in proper dependent form under 35 U.S.C. 112(d). That is, the claim must refer to a previous claim, include every limitation of the previous claim referred to, and then specify a further limitation of the subject matter of the previous claim. *See* section 608.01(n) of the MPEP, subsection III. In addition, to comply with the dependency format for this pilot program, the reference to the previous claim must appear in the preamble, and the claim must be directed to the same statutory class of invention as the independent claim.

For example, consider a claim set having independent claim 1, which recites ''A widget comprising A and B,'' and claim 2.

- If claim 2 recites ''The widget of claim 1 further comprising C,'' the claim would comply with the dependency format for the pilot program.
- If claim 2 recites ''A fastener for use in securing the widget of claim 1,'' the claim would not comply with the dependency format for the pilot program because it does not include all of the limitations of the previous claim.
- If claim 2 recites ''A device comprising the widget of claim 1 fastened to a gadget,'' the claim would not comply with the dependency format for the pilot program because the reference to the previous claim does not appear in the preamble.
- If claim 2 recites ''A method of producing the widget of claim 1,'' the claim would not comply with the dependency format for the pilot program because claim 2 is not directed to the same statutory class of invention as the independent claim.

If the application is granted special status under the program, the applicant must agree to comply with the claim requirements of the pilot program during the remainder of pendency.

*(4) Publication Requirement for Applications*

If there is a nonpublication request in the application, the applicant must file a rescission of the nonpublication request no later than the time the petition to make special is filed. The applicant may use form PTO/SB/36 to rescind the nonpublication request.

*(5) Electronic Filing of Petition and Application Required*

The petition to make special may be made only by filing form PTO/SB/472, which must be filed electronically using the USPTO's Patent Center (at *www.uspto.gov/PatentCenter*). Applicants must file the petition using the document description (''Petition for Streamlined Claim Set Pilot'') indicated on form PTO/SB/472. In addition, the application must have been filed using the USPTO patent electronic filing system (currently Patent Center).

*(6) Use of DOCX Format for the Specification, Claim(s), and Abstract*

DOCX format delivers a number of benefits, including increased efficiencies and higher data quality, that enhance the USPTO's ability to expedite examination. Thus, for an application to be eligible for the pilot program, the specification, claim(s), and abstract must be in compliance with the USPTO requirements for submission in DOCX format at the time the application was filed. *See* 37 CFR 1.16(u).

*(7) Filing Limitations*

An applicant may file a petition to participate in the pilot program if no inventor or joint inventor has been named as the inventor or a joint inventor on more than three other nonprovisional patent applications in

which a petition to make special under this pilot program has been filed. Therefore, if the inventor or any one of the joint inventors of the instant application has been named as the inventor or a joint inventor on more than three other nonprovisional applications in which a petition under this pilot program has been filed, then a petition for the instant application may not be appropriately filed. Form PTO/SB/472 includes a certification statement that no inventor or joint inventor has been named on more than three other nonprovisional applications in which a petition to make special under the pilot program has been filed.

*Part II. Internal Processing of the Petition Under the Pilot Program*

If applicant files a petition to make special under the pilot program, the USPTO will decide the petition once pre-examination processing of the application is completed. If the petition is granted, the application will be accorded special status under the pilot program. The application will be placed on an examiner's special docket until issuance of a first Office action. After the first Office action, the application will no longer be treated as special during examination. For example, if an amendment is filed after the first Office action, it will be placed on the examiner's regular amended docket.

Meeting the requirements in Part I of this notice will not ensure acceptance into the pilot program. The USPTO will generally dismiss a petition under the pilot program if the application has already been docketed to an examiner in a Technology Center at the time the petition is being reviewed for decision. The USPTO will not refund the 37 CFR 1.17(h) petition fee if an application is not accepted into the pilot program. This includes occurrences where the petition is dismissed because the application has been docketed to an examiner when the petition is taken up for decision despite being filed before the application was docketed to the examiner. *See* section 607.02 of the MPEP.

The purpose of the pilot program is to assess the effect of having a limited number of claims under examination on pendency and examination quality. As such, the USPTO intends to continue accepting applications into the pilot program until each Technology Center that examines utility applications has been docketed at least approximately 200 pilot applications. This is to make certain that the data collected during the pilot program is a balanced representation of examination across all technology areas. The USPTO will indicate on its website the total number of petitions filed and the number of applications accepted into the pilot program for each Technology Center.

If the petition to make special under the pilot program does not comply with the requirements set forth in this notice, the USPTO will dismiss the petition. In view of the limited duration of the pilot program and the limited number of applications being accepted into the pilot program, an applicant will not have an opportunity to correct deficiencies in the petition after a petition is dismissed. An applicant may file only a single petition under the pilot program for an application.

**Part III. Requirements for Restriction**

The USPTO anticipates fewer restriction requirements than in non-pilot program applications due to the claim set requirements of the pilot program. If the examiner believes that a requirement for restriction is appropriate, including an election of species requirement, the examiner should try to contact the applicant in accordance with the procedure for telephone restriction practice set forth in section 812.01 of the MPEP. If the applicant does not make an election (for example, does not reply to a request for a telephonic interview within five business days of the examiner's request), the examiner will mail a written restriction requirement, and the application will no longer be treated as special. In such cases, the written restriction requirement would be considered the ''first Office action'' in terms of this pilot program.

**Part IV. Office Actions and Replies Under the Pilot Program**

Applications that are accorded special status under the pilot program will be placed on an examiner's special docket until a first Office action is issued. After the first Office action, the application will be entered into the examiner's regular docket.

The time periods set for reply in Office actions for an application granted special status under the pilot program will be the same as those set forth in section 710.02(b) of the MPEP. A reply to an Office action must be fully responsive to the rejections, objections, and requirements made by the examiner. Any amendment filed in reply to an Office action may be treated as not fully responsive if it attempts to (1) add claims that would result in more than one independent claim and/or more than ten total claims pending in the application; (2) add any multiple dependent claim(s); or (3) present a claim, other than the independent claim, that does not comply with the dependency format set forth in Part I, section 3, of this notice. If a reply to a nonfinal Office action is not fully responsive for failing to comply with the pilot program's claim requirements but is a *bona fide* attempt to advance the application to final action, the examiner may, at the examiner's discretion, provide a shortened statutory period of two months for the applicant to provide a fully responsive reply. Extensions of this time period under 37 CFR 1.136(a) to the notice of nonresponsive amendment will be permitted, but in no way can any extension carry the date for reply to this notice beyond the maximum period of SIX MONTHS set by statute (35 U.S.C. 133). However, any further nonresponsive amendment typically will not be treated as *bona fide,* and therefore, the time period set in the prior notice will continue to run.

**Part V. After-Final and Appeal Procedures**

Any amendment, affidavit, or other evidence after a final Office action and prior to an appeal must comply with 37 CFR 1.116. During the appeal process, the application will be treated in accordance with the normal appeal procedure. *See* MPEP Chapter 1200.

**Part VI. Proceedings Outside of the Normal Examination Process**

If an application becomes involved in proceedings outside of the normal examination process (for example, a secrecy order, derivation proceeding, or petition under 37 CFR 1.181 through 1.183), the application will not be under special status during those proceedings. For example, while under a secrecy order, the application will be treated in accordance with the normal secrecy order procedures and will not be in special status under the pilot program. Once the proceeding outside of the normal examination process is completed, the application will continue in special status, as described above in this notice.

**Part VII. Withdrawal From the Pilot Program**

There is no provision for withdrawal from the pilot program. An applicant may abandon an application that has been granted special status under the pilot program in favor of a continuing application. However, a continuing application will not be granted special status based on the petition filed in the parent application. Only noncontinuing applications are eligible for this pilot program.

**Part VIII. Evaluation of the Pilot Program**

The pilot program is designed to allow the USPTO to evaluate how having a limited number of claims under examination affects pendency and examination quality. Accordingly, the USPTO intends to collect data on the progression of applications accepted into the pilot program throughout the examination process. During or after the pilot program, the USPTO will provide avenues for participants to provide feedback on their experience with the pilot program. As applicable, the USPTO will follow the United States Government Accountability Office's (GAO's) leading practices for effective pilot design, including (1) establishing clear objectives; (2) collecting relevant data; (3) evaluating outcomes; (4) considering scalability; and (5) ensuring stakeholder communication. *See* GAO, *Data Act: Section 5 Pilot Design Issues Need to Be Addressed to Meet Goal of Reducing Recipient Reporting Burden,* GAO–16–438 (April 19, 2016).

**John A. Squires,**

*Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office.*

[FR Doc. 2025–19669 Filed 10–24–25; 8:45 am]

**BILLING CODE 3510–16–P**

## ENVIRONMENTAL PROTECTION AGENCY

**[EPA–HQ–OPP–2025–0756; FRL–12903–03–OCSPP]**

### FIFRA Scientific Advisory Panel (SAP); Notice of Postponement of Public Meeting

**AGENCY:** Environmental Protection Agency (EPA).

**ACTION:** Notice.

**SUMMARY:** The Agency has postponed the 3-day virtual public meeting of the Federal Insecticide, Fungicide, and Rodenticide Act Scientific Advisory Panel (FIFRA SAP) for peer review on ''Determining the Absence of Novel Proteins in the Saliva of Genetically Engineered Mosquitoes for Mosquito Control'' scheduled for November 3 to 5, 2025. The meeting was announced in the **Federal Register** on July 24, 2025. The meeting will be rescheduled.

**FOR FURTHER INFORMATION CONTACT:** Alie Muneer, Designated Federal Official, Mission Support Division, Office of Program Support, Office of Chemical Safety and Pollution Prevention, Environmental Protection Agency; telephone number: (202) 564–6369 or the main office number: (202) 564–8450; email address: *muneer.alie@epa.gov*.

**SUPPLEMENTARY INFORMATION:** The meeting was announced in the **Federal Register** on July 24, 2025 (90 FR 34864 (FRL–12903–01–OCSPP). This meeting is being rescheduled due to the lapse in government appropriations and its impact on potential and existing panel members. A new notice announcing the new date will be published in the **Federal Register** at least 15 days prior to the meeting being held.

*Authority:* 5 U.S.C. 10; 7 U.S.C. 136 *et seq.;* 21 U.S.C. 301 *et seq.*

Dated: October 22, 2025.

**Nancy B. Beck,**

*Principal Deputy Assistant Administrator, Office of Chemical Safety and Pollution Prevention.*

[FR Doc. 2025–19663 Filed 10–24–25; 8:45 am]

**BILLING CODE 6560–50–P**

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

### Determination Pursuant to Section 102 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, as Amended

**AGENCY:** Office of the Secretary, Department of Homeland Security.

**ACTION:** Notice of determination.

**SUMMARY:** The Secretary of Homeland Security has determined, pursuant to law, that it is necessary to waive certain laws, regulations, and other legal requirements in order to ensure the expeditious construction of barriers and roads in the vicinity of the international land border in the state of Texas.

**DATES:** This determination takes effect on October 27, 2025.

**SUPPLEMENTARY INFORMATION:** Important mission requirements of the Department of Homeland Security (''DHS'') include border security and the detection and prevention of illegal entry into the United States. Border security is critical to the nation's national security. Recognizing the critical importance of border security, Congress has mandated DHS to achieve and maintain operational control of the international land border. Secure Fence Act of 2006, Public Law 109–367, section 2, 120 Stat. 2638 (Oct. 26, 2006) (8 U.S.C. 1701 note). Congress defined ''operational control'' as the prevention of all unlawful entries into the United States, including entries by terrorists, other unlawful aliens, instruments of terrorism, narcotics, and other contraband. *Id.* Consistent with that mandate, the President's Executive Order on Securing Our Borders directs that I take all appropriate action to deploy and construct physical barriers to ensure complete operational control of the southern border of the United States. Executive Order 14165, section 3 (Jan. 20, 2025).

Congress has provided to the Secretary of Homeland Security a number of authorities necessary to carry out DHS's border security mission. One of those authorities is found at section 102 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, as amended (''IIRIRA''). Public Law 104–208, Div. C, 110 Stat. 3009–546, 3009–554 (Sept. 30, 1996) (8 U.S.C. 1103 note), as amended by the REAL ID Act of 2005, Public Law 109–13, Div. B, 119 Stat. 231, 302, 306 (May 11, 2005) (8 U.S.C. 1103 note), as amended by the Secure Fence Act of 2006, Public Law 109–367, section 3, 120 Stat. 2638 (Oct. 26, 2006) (8 U.S.C. 1103 note), as amended by the Department of Homeland Security Appropriations Act, 2008, Public Law 110–161, Div. E, Title V, section 564, 121 Stat. 2090 (Dec. 26, 2007). In section 102(a) of IIRIRA, Congress provided that the Secretary of Homeland Security shall take such actions as may be necessary to install additional physical barriers and roads (including the removal of obstacles to detection of illegal entrants) in the vicinity of the United States border to deter illegal crossings in areas of high illegal entry into the United States. In section 102(b) of IIRIRA, Congress mandated that in carrying out the authority of section 102(a), I provide for the installation of additional fencing, barriers, roads, lighting, cameras, and sensors to achieve and maintain operational control of the border. Finally, in section 102(c) of IIRIRA, Congress granted to the Secretary of Homeland Security the authority to waive all legal requirements that I, in my sole discretion, determine necessary to ensure the expeditious construction of barriers and roads authorized by section 102 of IIRIRA.

**Determination and Waiver**

*Section 1*

The United States Border Patrol Del Rio Sector is an area of high illegal entry. Between fiscal year 2021 and July 2025, Border Patrol apprehended over 1,408,600 illegal aliens attempting to enter the United States between border crossings in the Del Rio Sector. In that same time period Border Patrol seized over 275 pounds of marijuana, over 131 pounds of cocaine, over 18 pounds of

heroin, over 353 pounds of methamphetamine, and over five pounds of fentanyl.

Since the President took office, DHS has delivered the most secure border in history. More can and must be done, however. As the statistics cited above demonstrate, the Del Rio Sector is an area of high illegal entry where illegal aliens regularly attempt to enter the United States and smuggle illicit drugs, and given my mandate to achieve and maintain operational control of the border, I must use my authority under section 102 of IIRIRA to install additional barriers and roads in the Del Rio Sector. Therefore, DHS will take immediate action to construct additional barriers and roads in a segment of the border in the Del Rio Sector. The segment where such construction will occur is referred to herein as the ''project area,'' which is more specifically described in Section 2 below.

*Section 2*

I determine that the following area in the vicinity of the United States border, located in the State of Texas within the U. S. Border Patrol Del Rio Sector, is an area of high illegal entry (the ''project area''): Within the Del Rio Sector, starting at approximately GPS point 29.09, −100.67 and extending south and east to approximately GPS point 28.47, −100.36.

There is presently an acute and immediate need to construct additional physical barriers and roads in the vicinity of the border of the United States in order to prevent unlawful entries into the United States in the project area pursuant to section 102(a) and 102(b) of IIRIRA. In order to ensure the expeditious construction of additional physical barriers and roads in the project area, I have determined that it is necessary that I exercise the authority that is vested in me by section 102(c) of IIRIRA.

Accordingly, pursuant to section 102(c) of IIRIRA, I hereby waive in their entirety, with respect to the construction of physical barriers and roads (including, but not limited to, accessing the project areas, creating and using staging areas, the conduct of earthwork, excavation, fill, and site preparation, and installation and upkeep of physical barriers, roads, supporting elements, drainage, erosion controls, safety features, lighting, cameras, and sensors) in the project area, all of the following statutes, including all federal, state, or other laws, regulations, and legal requirements of, deriving from, or related to the subject of, the following statutes, as amended: The National Environmental Policy Act (Pub. L. 91–190, 83 Stat. 852 (Jan. 1, 1970) (42 U.S.C. 4321 *et seq.*)); the Endangered Species Act (Pub. L. 93–205, 87 Stat. 884 (Dec. 28, 1973) (16 U.S.C. 1531 *et seq.*)); the Federal Water Pollution Control Act (commonly referred to as the Clean Water Act (33 U.S.C. 1251 *et seq.*)); the National Historic Preservation Act (Pub. L. 89–665, 80 Stat. 915 (Oct. 15, 1966), as amended, repealed, or replaced by Pub. L. 113–287 (Dec. 19, 2014) (formerly codified at 16 U.S.C. 470 *et seq.,* now codified at 54 U.S.C. 100101 note and 54 U.S.C. 300101 *et seq.*)); the Migratory Bird Treaty Act (16 U.S.C. 703 *et seq.*); the Migratory Bird Conservation Act (16 U.S.C. 715 *et seq.*); the Clean Air Act (42 U.S.C. 7401 *et seq.*); the Archeological Resources Protection Act (Pub. L. 96–95 (16 U.S.C. 470aa *et seq.*)); the Paleontological Resources Preservation Act (16 U.S.C. 470aaa *et seq.*); the Federal Cave Resources Protection Act of 1988 (16 U.S.C. 4301 *et seq.*); the National Trails System Act (16 U.S.C. 1241 *et seq.*); the Safe Drinking Water Act (42 U.S.C. 300f *et seq.*); the Noise Control Act (42 U.S.C. 4901 *et seq.*); the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act (42 U.S.C. 6901 *et seq.*); the Comprehensive Environmental Response, Compensation, and Liability Act (42 U.S.C. 9601 *et seq.*); the Archaeological and Historic Preservation Act (Pub. L. 86–523, as amended, repealed, or replaced by Pub. L. 113–287 (Dec. 19, 2014) (formerly codified at 16 U.S.C. 469 *et seq.,* now codified at 54 U.S.C. 312502 *et seq.*)); the Antiquities Act (formerly codified at 16 U.S.C. 431 *et seq.* and 16 U.S.C. 431a *et seq.,* now codified 54 U.S.C. 320301 *et seq.*); the Historic Sites, Buildings, and Antiquities Act (formerly codified at 16 U.S.C. 461 *et seq.,* now codified at 54 U.S.C. 320301–320303 & 320101–320106); the Eagle Protection Act (16 U.S.C. 668 *et seq.*); the Native American Graves Protection and Repatriation Act (25 U.S.C. 3001 *et seq.*); the Administrative Procedure Act (5 U.S.C. 551 *et seq.*); Section 438 of the Energy Independence and Security Act (42 U.S.C. 17094); the National Fish and Wildlife Act of 1956 (Pub. L. 84–1024 (16 U.S.C. 742a, *et seq.*)); the Fish and Wildlife Coordination Act (Pub. L. 73–121 (16 U.S.C. 661 *et seq.*)); the Farmland Protection Policy Act (7 U.S.C. 4201 *et seq.*); the Federal Land Policy and Management Act (Pub L. 94–579 (43 U.S.C. 1701 *et seq.*)); the Wild Horse and Burro Act (16 U.S.C. 1331 *et seq.*); 43 U.S.C. 387; the Wild and Scenic Rivers Act (Pub. L. 90–542 (16 U.S.C. 1281 *et seq.*); the Rivers and Harbors Act of 1899 (33 U.S.C. 403 *et seq.*); the Federal Insecticide, Fungicide, and Rodenticide Act, (16 U.S.C. 136–136y); and the Marine Mammal Protection Act (16 U.S.C. 1361–1421h).

This waiver does not revoke or supersede any other waiver determination made pursuant to section 102(c) of IIRIRA. Such waivers shall remain in full force and effect in accordance with their terms. I reserve the authority to execute further waivers from time to time as I may determine to be necessary under section 102 of IIRIRA.

**Kristi Noem,**

*Secretary of Homeland Security.*

[FR Doc. 2025–19656 Filed 10–24–25; 8:45 am]

**BILLING CODE 9111–14–P**

## JUDICIAL CONFERENCE OF THE UNITED STATES

### Advisory Committee on Evidence Rules; Meeting of the Judicial Conference

**AGENCY:** Judicial Conference of the United States.

**ACTION:** Advisory Committee on Evidence Rules; revised notice of open meeting.

**SUMMARY:** The Advisory Committee on Evidence Rules will hold a meeting virtually on November 5, 2025, rather than in New Orleans, LA, as previously announced. The meeting is open to the public only for remote observation with no participation. Please see the **SUPPLEMENTARY INFORMATION** section in this notice for instructions on observing the meeting.

**DATES:** November 5, 2025.

**ADDRESSES:** An agenda and supporting materials will be posted at least 7 days in advance of the meeting at: *https://www.uscourts.gov/forms-rules/records-rules-committees/agenda-books*.

**FOR FURTHER INFORMATION CONTACT:** Carolyn A. Dubay, Chief Counsel, Rules Committee Staff, Administrative Office of the U.S. Courts, Thurgood Marshall Federal Judiciary Building, One Columbus Circle NE, Suite 7–300, Washington, DC 20544, Phone (202) 502–1820, *RulesCommittee_Secretary@ao.uscourts.gov*.

**SUPPLEMENTARY INFORMATION:** Remote registration is available until the meeting date, provided it is completed before the projected end time. The announcement for this meeting was previously published in the **Federal**

**Register** on September 2, 2025 at 90 FR 42446.

(Authority: 28 U.S.C. 2073.)

Dated: October 22, 2025.

**Shelly L. Cox,**

*Management Analyst, Rules Committee Staff.*

[FR Doc. 2025–19660 Filed 10–24–25; 8:45 am]

**BILLING CODE 2210–55–P**

## JUDICIAL CONFERENCE OF THE UNITED STATES

### Advisory Committee on Criminal Rules; Meeting of the Judicial Conference

**AGENCY:** Judicial Conference of the United States.

**ACTION:** Advisory Committee on Criminal Rules; revised notice of open meeting.

**SUMMARY:** The Advisory Committee on Criminal Rules will hold a meeting virtually on November 6, 2025, rather than in New Orleans, LA, as previously announced. The meeting is open to the public only for remote observation with no participation. Please see the **SUPPLEMENTARY INFORMATION** section in this notice for instructions on observing the meeting.

**DATES:** November 6, 2025.

**ADDRESSES:** An agenda and supporting materials will be posted at least 7 days in advance of the meeting at: *https://www.uscourts.gov/forms-rules/records-rules-committees/agenda-books*.

**FOR FURTHER INFORMATION CONTACT:** Carolyn A. Dubay, Chief Counsel, Rules Committee Staff, Administrative Office of the U.S. Courts, Thurgood Marshall Federal Judiciary Building, One Columbus Circle NE, Suite 7–300, Washington, DC 20544, Phone (202) 502–1820, *RulesCommittee_Secretary@ao.uscourts.gov*.

**SUPPLEMENTARY INFORMATION:** Remote registration is available until the meeting date, provided it is completed before the projected end time. The announcement for this meeting was previously published in the **Federal Register** on September 2, 2025 at 90 FR 42446.

(Authority: 28 U.S.C. 2073.)

Dated: October 22, 2025.

**Shelly L. Cox,**

*Management Analyst, Rules Committee Staff.*

[FR Doc. 2025–19661 Filed 10–24–25; 8:45 am]

**BILLING CODE 2210–55–P**

## NATIONAL CREDIT UNION ADMINISTRATION

**[NCUA–2025–0543]**

### The NCUA Staff Draft 2026–2027 Budget

**AGENCY:** National Credit Union Administration (NCUA).

**ACTION:** Notice.

**SUMMARY:** The NCUA's staff draft ''detailed business-type budget'' for 2026 and 2027 was made available for public review in the **Federal Register** as required by federal statute on September 29, 2025 as docket number NCUA–2025–0543. The NCUA will hold an in-person budget hearing to discuss its staff draft budget. This notice is being issued to let the public know the hearing has been rescheduled to November 5, 2025 at 1 p.m. Eastern.

**DATES:** The hearing date included in the notice published on October 21, 2025 (90 FR 48439) is changed to November 5, 2025, at 1 p.m. Eastern.

**FOR FURTHER INFORMATION CONTACT:** Melissa L. Lowden, Acting Chief Financial Officer, National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314–3428, or telephone: (703) 518–1182.

**SUPPLEMENTARY INFORMATION:** As noted in documents published on September 29, 2025 (90 FR 4664) and October 21, 2025 (90 FR 48439), the NCUA will hold a public hearing on its staff draft budget for 2026–2027. Interested parties are referred to those notices for further background and deadlines for providing input. This notice is being issued to reschedule the in-person public hearing from November 6, 2025 at 1 p.m. Eastern to November 5, 2025 at 1 p.m. Eastern. All other details and deadlines associated with the staff draft budget are unchanged.

By the National Credit Union Administration Board on October 22, 2025.

**Melane Conyers-Ausbrooks,**

*Secretary of the Board.*

[FR Doc. 2025–19659 Filed 10–24–25; 8:45 am]

**BILLING CODE 7535–01–P**

## POSTAL REGULATORY COMMISSION

**[Docket Nos. MC2026–46 and K2026–46; MC2026–47 and K2026–47]**

### New Postal Products

**AGENCY:** Postal Regulatory Commission.

**ACTION:** Notice.

**SUMMARY:** The Commission is noticing a recent Postal Service filing for the Commission's consideration concerning a negotiated service agreement. This notice informs the public of the filing, invites public comment, and takes other administrative steps.

**DATES:** *Comments are due:* October 30, 2025.

**ADDRESSES:** Submit comments electronically via the Commission's Filing Online system at *https://www.prc.gov.* Those who cannot submit comments electronically should contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section by telephone for advice on filing alternatives.

**FOR FURTHER INFORMATION CONTACT:** David A. Trissell, General Counsel, at 202–789–6820.

**SUPPLEMENTARY INFORMATION:**

**Table of Contents**

I. Introduction
II. Public Proceeding(s)
III. Summary Proceeding(s)

**I. Introduction**

Pursuant to 39 CFR 3041.405, the Commission gives notice that the Postal Service filed request(s) for the Commission to consider matters related to Competitive negotiated service agreement(s). The request(s) may propose the addition of a negotiated service agreement from the Competitive product list or the modification of an existing product currently appearing on the Competitive product list.

The public portions of the Postal Service's request(s) can be accessed via the Commission's website (*http://www.prc.gov*). Non-public portions of the Postal Service's request(s), if any, can be accessed through compliance with the requirements of 39 CFR 3011.301.[1]

Section II identifies the docket number(s) associated with each Postal Service request, if any, that will be reviewed in a public proceeding as defined by 39 CFR 3010.101(p), the title of each such request, the request's acceptance date, and the authority cited by the Postal Service for each request. For each such request, the Commission appoints an officer of the Commission to represent the interests of the general public in the proceeding, pursuant to 39 U.S.C. 505 and 39 CFR 3000.114 (Public Representative). The Public Representative does not represent any individual person, entity or particular point of view, and, when Commission attorneys are appointed, no attorney-

[1] *See* Docket No. RM2018–3, Order Adopting Final Rules Relating to Non-Public Information, June 27, 2018, Attachment A at 19–22 (Order No. 4679).

client relationship is established. Section II also establishes comment deadline(s) pertaining to each such request.

The Commission invites comments on whether the Postal Service's request(s) identified in Section II, if any, are consistent with the policies of title 39. Applicable statutory and regulatory requirements include 39 U.S.C. 3632, 39 U.S.C. 3633, 39 U.S.C. 3642, 39 CFR part 3035, and 39 CFR part 3041. Comment deadline(s) for each such request, if any, appear in Section II.

Section III identifies the docket number(s) associated with each Postal Service request, if any, to add a standardized distinct product to the Competitive product list or to amend a standardized distinct product, the title of each such request, the request's acceptance date, and the authority cited by the Postal Service for each request. Standardized distinct products are negotiated service agreements that are variations of one or more Competitive products, and for which financial models, minimum rates, and classification criteria have undergone advance Commission review. *See* 39 CFR 3041.110(n); 39 CFR 3041.205(a). Such requests are reviewed in summary proceedings pursuant to 39 CFR 3041.325(c)(2) and 39 CFR 3041.505(f)(1). Pursuant to 39 CFR 3041.405(c)–(d), the Commission does not appoint a Public Representative or request public comment in proceedings to review such requests. The comment due date discussed above does not apply to Section III proceedings (Docket Nos. MC2026–47 and K2026–47).

**II. Public Proceeding(s)**

1. *Docket No(s).:* MC2026–46 and K2026–46; *Filing Title:* USPS Request to Add Priority Mail Contract 940 to the Competitive Product List and Notice of Filing Materials Under Seal; *Filing Acceptance Date:* October 22, 2025; *Filing Authority:* 39 U.S.C. 3642, 39 CFR 3035.105, and 39 CFR 3041.310; *Public Representative:* Christopher Mohr; *Comments Due:* October 30, 2025.

**III. Summary Proceeding(s)**

1. *Docket No(s).:* MC2026–47 and K2026–47; *Filing Title:* USPS Request to Add New Fulfillment Standardized Distinct Product, PM–GA Contract 889, and Notice of Filing Materials Under Seal; *Filing Acceptance Date:* October 22, 2025; *Filing Authority:* 39 U.S.C. 3642 and 3633, 39 CFR 3035.105, and 39 CFR 3041.325.

This Notice will be published in the **Federal Register**.

**Erica A. Barker,**

*Secretary.*

[FR Doc. 2025–19666 Filed 10–24–25; 8:45 am]

**BILLING CODE 7710–FW–P**

## STATE JUSTICE INSTITUTE

### Grant Guideline; Notice

**AGENCY:** State Justice Institute.

**ACTION:** Grant Guideline for Fiscal Year (FY) 2026.

**SUMMARY:** This guideline sets forth the administrative, programmatic, and financial requirements attendant to FY 2026 State Justice Institute grants.

**DATES:** October 7, 2025.

**ADDRESSES:** State Justice Institute, 12700 Fair Lakes Circle, Suite 340, Fairfax, VA 22033.

**FOR FURTHER INFORMATION CONTACT:** Jonathan Mattiello, Executive Director, State Justice Institute, 703–660–4979, *jonathan.mattiello@sji.gov.*

**SUPPLEMENTARY INFORMATION:** Pursuant to the State Justice Institute Act of 1984 (42 U.S.C. 10701 *et seq.*), the State Justice Institute is authorized to award grants, cooperative agreements, and contracts to state and local courts, nonprofit organizations, and others for the purpose of improving the quality of justice in the state courts of the United States.

The following Grant Guideline is adopted by the State Justice Institute for FY 2026.

**Table of Contents**

I. Eligibility
II. Grant Application Deadlines
III. The Mission of the State Justice Institute
IV. Grant Types
V. Application and Submission Information
VI. How To Apply
VII. Post-Award Reporting Requirements
VIII. Compliance Requirements
IX. Financial Requirements
X. Grant Adjustments

**I. Eligibility**

Pursuant to the State Justice Institute Act of 1984 (42 U.S.C. 10701 *et seq.*), the State Justice Institute (SJI) is authorized to award grants, cooperative agreements, and contracts to state and local courts, national nonprofit organizations, and others for the purpose of improving the quality of justice in the state courts of the United States.

SJI is authorized by Congress to award grants, cooperative agreements, and contracts to the following entities and types of organizations:

- State and local courts and their agencies (42 U.S.C. 10705(b)(1)(A)).
- National nonprofit organizations controlled by, operating in conjunction with, and serving the judicial branches of state governments (42 U.S.C. 10705(b)(1)(B)).
- National nonprofit organizations for the education and training of judges and support personnel of the judicial branch of state governments (42 U.S.C. 10705(b)(1)(C)). An applicant is considered a national education and training applicant under section 10705(b)(1)(C) if:
  - the principal purpose or activity of the applicant is to provide education and training to state and local judges and court personnel; and
  - the applicant demonstrates a record of substantial experience in the field of judicial education and training.
- Other eligible grant recipients (42 U.S.C. 10705(b)(2)(A) through (D)).
  - Provided that the objectives of the project can be served better, SJI is also authorized to make awards to:
    - Nonprofit organizations with expertise in judicial administration
    - Institutions of higher education
    - Individuals, partnerships, firms, corporations (for-profit organizations must waive their fees)
    - Private agencies with expertise in judicial administration
  - SJI may also make awards to state or local agencies and institutions other than courts for services that cannot be adequately provided through nongovernmental arrangements (42 U.S.C. 10705(b)(3)).

SJI is prohibited from awarding grants to federal, tribal, and international courts.

**II. Grant Application Deadlines**

The SJI Board of Directors makes awards on a federal fiscal year quarterly basis. Applications may be submitted at any time but will be considered for award based only on the timetable below.

TABLE 1—APPLICATION DEADLINES BY FEDERAL FISCAL YEAR QUARTER

| Federal fiscal year quarter | Application due date |
|---|---|
| 1 | November 1. |
| 2 | February 1. |
| 3 | May 1. |
| 4 | August 1. |

To be considered timely, an application must be submitted by the application deadline noted above. Applicants must use the SJI Grants Management System (GMS) to submit all applications and post-award

documents. The SJI GMS is accessible at *https://gms.sji.gov.* SJI urges applicants to submit applications at least 72 hours prior to the application due date to allow time for the applicant to receive an application acceptance message and to correct in a timely fashion any problems that may arise, such as missing or incomplete forms.

Questions related to the SJI Grant Program or the SJI GMS should be directed to *contact@sji.gov.*

**III. The Mission of the State Justice Institute**

The State Justice Institute Authorization Act of 1984 (42 U.S.C. 10701 *et seq.*) established SJI to improve the administration of justice in the state courts of the United States. Incorporated in the state of Virginia as a private, nonprofit corporation, SJI is charged, by statute, with the responsibility to:

- direct a national program of financial assistance designed to ensure that each citizen of the United States is provided ready access to a fair and effective system of justice;
- foster coordination and cooperation with the federal judiciary;
- promote recognition of the importance of the separation of powers doctrine to an independent judiciary; and
- encourage education for judges and support personnel of state court systems through national and state organizations.

To accomplish these broad objectives, SJI is authorized to provide funding to state courts, national organizations that support and are supported by state courts, national judicial education organizations, and other organizations that can assist in improving the quality of justice in the state courts.

Through the award of grants, contracts, and cooperative agreements, SJI is authorized to perform the following activities:

- support technical assistance, demonstrations, special projects, research, and training to improve the administration of justice in the state courts;
- provide for the preparation, publication, and dissemination of information regarding State judicial systems;
- participate in joint projects with Federal agencies and other private grantors;
- evaluate or provide for the evaluation of programs and projects to determine their impact upon the quality of criminal, civil, and juvenile justice and the extent to which they have contributed to improving the quality of justice in the state courts;
- encourage and assist in furthering judicial education; and
- encourage, assist, and serve in a consulting capacity state and local courts in the development, maintenance, and coordination of criminal, civil, and juvenile justice programs and services.

SJI is supervised by a board of directors appointed by the U.S. President, with the advice and consent of the U.S. Senate. The SJI Board of Directors is statutorily composed of six judges; a State court administrator; and four members of the public, no more than two of the same political party. Additional information about SJI, including a list of members of the SJI Board of Directors, is available at *https://www.sji.gov.*

*a. Priority Investment Areas*

The SJI Board of Directors has established Priority Investment Areas for grant funding. SJI will allocate significant financial resources through grant-making for these Priority Investment Areas. The Priority Investment Areas are applicable to all grant types. SJI strongly encourages potential grant applicants to consider projects addressing one or more of these Priority Investment Areas and to integrate the following factors into each proposed project:

- evidence-based, data-driven decision-making;
- cross-sector collaboration;
- systemic approaches (as opposed to standalone programs);
- institutionalization of new court processes and procedures;
- ease of replication; and
- sustainability.

For FY 2026, the Priority Investment Areas are listed below in no specific order.

1. Opioids and Other Dangerous Drugs and Behavioral Health Responses

- *Opioids and Behavioral Health Court Responses*—Research indicates that justice-involved persons have significantly greater proportions of mental, substance use, and co-occurring disorders than are found in the public. SJI supports cross-sector collaboration and information sharing that emphasizes policies and practices designed to improve court responses to justice-involved persons with behavioral health and other co-occurring needs.
- *Trauma-Informed Approaches*—Judges, court staff, system stakeholders, and court-involved persons (*e.g.,* defendants, respondents, and victims) alike may be impacted by prior trauma. This is particularly, but not exclusively, true for those with mental illness and/or substance use disorders. SJI supports trauma-informed training, policies, and practices in all aspects of the judicial process.

2. Promoting Access to Justice and Procedural Fairness

- *Procedural Fairness*—A fundamental role of courts is to ensure fair processes and just outcomes for litigants. SJI promotes the integration of research-based procedural fairness principles, policies, and practices into state court operations to increase public trust and confidence in the court system, reduce recidivism, and increase compliance with court orders.
- *Self-Represented Litigation*—SJI promotes court-based solutions to address increases in self-represented litigants; helps make courts more user-friendly by simplifying court forms; provides one-on-one assistance; develops guides, handbooks, and instructions on how to proceed; develops court-based self-help centers; and uses internet technologies to increase access. These projects are improving outcomes for litigants and saving valuable court resources.

3. Protecting Victims, Underserved, and Vulnerable Populations

- *Human Trafficking*—SJI addresses the impact of federal and state human-trafficking laws on the state courts and the challenges faced by state courts in dealing with cases involving trafficking victims and their families, including victims who are U.S. citizens. These efforts are intended to empower state courts to identify victims, link them with vital services, and hold traffickers accountable.
- *Rural Justice*—Rural areas and their justice systems routinely have fewer resources and more barriers—such as unavailability of services, lack of transportation, and smaller workforces—than their urban counterparts. Programs and practices that are effective in urban areas are often inappropriate and/or lack supported research for implementation in rural areas. SJI supports rural courts by identifying promising and best practices and promoting resources, education, and training opportunities that are uniquely designed for rural courts and court users.
- *Guardianship, Conservatorship, and Elder Issues*—SJI assists courts in improving court oversight of guardians and conservators for the elderly and incapacitated adults through visitor programs, electronic reporting, and training.

4. Advancing Justice Reform

• *Criminal Justice Reform*—SJI assists state courts in promoting offender accountability and oversight; fosters transparency, governance, and structural reforms that promote access to justice; and implements innovative diversion and reentry programs that serve to improve outcomes for justice-involved persons and reduce the impact of the costs of the justice system.

• *Juvenile Justice Reform*—SJI supports innovative projects that advance best practices in handling dependency and delinquency cases, promote effective court oversight of juveniles in the justice system, address the impact of trauma on juvenile behavior, assist the courts in identification of appropriate provision of services for juveniles, and address juvenile reentry.

• *Family and Civil Justice Reform*—SJI promotes court-based solutions for the myriad types of civil cases, such as domestic relations, housing, employment, and debt collection, which are overwhelming court dockets.

5. Transforming Courts

• *Courthouse and Public Safety*—In the current climate of increasing threats and acts of violence against courthouses across the nation, state and local courts are seeking new and innovative ways to enhance the safety of courthouses. SJI has long recognized the need to assist state and local courts in improving the safety of the public, court staff, and judges in court facilities.

• *Technology*—Courts must integrate technological advances into daily judicial processes and proceedings. SJI supports projects that institutionalize innovative technology that has successfully advanced the use of electronic filing and payment systems, online dispute resolution, remote work, and virtual court proceedings. SJI promotes projects that streamline case filing and management processes, thereby reducing time and costs to litigants and the courts; provide online access to courts to litigants so that disputes can be resolved more efficiently; and make structural changes to court services that enable them to evolve into an online environment. Additionally, SJI supports the examination of potential integration of Artificial Intelligence (AI) into court processes, including identification of positive outcomes and potential limitations of AI.

• *Cybersecurity*—Courts must also be prepared for cyberattacks on court systems, such as denial of service and ransomware attacks on court case management systems, websites, and other critical information technology infrastructure. SJI supports projects that assist courts in preparing for and responding to these attacks and shares lessons learned to courts across the United States.

• *Emergency Response and Recovery*—Courts must be prepared for natural disasters and public health emergencies and institutionalize the most effective and efficient practices and processes that evolve during response and recovery. SJI supports projects that look to the future of judicial service delivery by identifying and replicating innovations and alternate means of conducting court business due to public health emergencies, such as pandemics and natural disasters like hurricanes, floods, earthquakes, and wildfires.

• *Strategic Planning*—Courts must rely on a deliberate process to determine organizational values, mission, vision, goals, and objectives. SJI promotes structured planning processes and organizational assessments to assist courts in setting priorities, allocating resources, and identifying areas for ongoing improvements in efficiency and effectiveness. Strategic planning includes elements of court governance, data collection, management, analysis, sharing, and sustainable court governance models that drive decision-making. Strategic plans and outcomes must be communicated to judges, court staff, justice partners, and the public.

• *Workforce Development*—State courts require a workforce that is adaptable to public demands for services. SJI supports projects that focus on the tools needed to enable judges, court managers, and staff to be innovative, forward-thinking court leaders.

## IV. Grant Types

SJI supports five types of grants: Project, Technical Assistance (TA), Curriculum Adaptation and Training (CAT), Strategic Initiatives Grants (SIG) Program, and the Education Support Program (ESP). A brief description of each type of grant is below.

*a. Project Grant*

Project grants are intended to support innovative education and training, research and evaluation, demonstration, and TA projects that can improve the administration of justice in state courts locally or nationwide. State court and national nonprofit applicants may request up to $300,000 for 36 months. Local court applicants may request up to $200,000 for 24 months. Examples of expenses not covered by project grants include the salaries or benefits of full- or part-time court employees. Funding may not be used for the ordinary, routine operations of court systems.

All applicants for project grants must contribute a cash match greater than or equal to the SJI award amount. This means that grant awards by SJI must be matched at least dollar for dollar by grant applicants. For example, an applicant seeking a $300,000 Project Grant must provide a cash match of at least $300,000. Applicants may contribute the required cash match directly or in cooperation with third parties. Funding from other federal departments or agencies may not be used for a cash match.

*b. TA Grant*

TA grants are intended to provide state or local courts—or regional court associations—with sufficient support to obtain expert assistance to diagnose a problem, develop a response to that problem, and implement any needed changes. TA grants may not exceed $75,000 or 12 months in duration. In calculating project duration, applicants are cautioned to fully consider the time required to issue a request for proposals, negotiate a contract with the selected provider, and execute the project. Funds may not be used for salaries or benefits of full- or part-time court employees.

Applicants for TA grants are required to contribute a total match (cash and in-kind) of no less than 50 percent of the SJI award amount, of which 20 percent must be cash. For example, an applicant seeking a $75,000 TA Grant must provide a $37,500 match, of which up to $30,000 can be in-kind and not less than $7,500 must be cash. Funding from other federal departments and agencies may not be used for a cash match.

*c. CAT Grant*

CAT grants are intended to: (1) enable courts or national court associations to modify and adapt model curricula, course modules, or conference programs to meet states' or local jurisdictions' educational needs; train instructors to present portions or all of the curricula; and pilot-test them to determine their appropriateness, quality, and effectiveness; or (2) conduct judicial branch education and training programs, led by either expert or in-house personnel, designed to prepare judges and court personnel for innovations, reforms, and/or new technologies recently adopted by grantee courts. CAT grants may not exceed $40,000 or 12 months in duration. Examples of expenses not covered by CAT grants include the

salaries or benefits of full- or part-time court employees.

Applicants for CAT grants are required to contribute a total match (cash and in-kind) of not less than 50 percent of the SJI award amount, of which 20 percent must be cash. For example, an applicant seeking a $40,000 CAT grant must provide a $20,000 match, of which up to $16,000 can be in-kind and not less than $4,000 must be cash. Funding from other federal departments and agencies may not be used for a cash match.

*d. SIG Program*

The SIG Program provides SJI with the flexibility to address national court issues as they occur and develop solutions to those problems. This is an innovative approach where SJI uses its expertise and the expertise and knowledge of its grantees to address key issues facing state courts across the United States.

The funding is used for grants or contractual services and is handled at the discretion of the SJI Board of Directors and staff. SJI requires the submission of a concept paper prior to the full application process. *Only applicants that submit an approved concept paper will be invited to submit a full application for funding. Potential applicants are strongly encouraged to contact SJI prior to submitting a concept paper for guidance on this initial step.*

*e. ESP for Judges and Court Managers*

The ESP is intended to enhance the skills, knowledge, and abilities of state court judges and court managers by enabling them to attend out-of-state or enroll in online educational and training programs sponsored by national and state providers they could not otherwise attend or take online because of limited state, local, and personal budgets. The program covers only the cost of tuition up to a maximum of $1,000 per course.

The ESP is administered by the National Judicial College (NJC) and the National Center for State Courts (NCSC)/Institute for Court Management (ICM), in partnership with SJI. For NJC courses, register online at *https://www.judges.org/courses.* For ICM courses, register online at *https://www.ncsc.org/courses.* During the respective registration processes, each website will ask whether a scholarship is needed to participate. Follow the online instructions to request tuition assistance.

## V. Application and Submission Information

This section describes in detail what an application must include. An applicant should anticipate that if he or she fails to submit an application that contains all the specified project components, it may negatively affect the review of the application. Applicants must use the SJI GMS to submit all applications and post-award documents. The SJI GMS is accessible at *https://gms.sji.gov.*

*a. Application Components*

Applicants for SJI grants must submit the following forms and/or documents via the SJI GMS:

1. Application Form

The application form requests basic information regarding the proposed project, the applicant, and the total amount of funding requested from SJI. It also requires the signature of an individual authorized to certify on behalf of the applicant that the information contained in the application is true and complete; submission of the application has been authorized by the applicant; and, if funding for the proposed project is approved, the applicant will comply with the requirements and conditions of the award, including the assurances set forth in section V.A.4, *Assurances,* of this guideline.

2. Certificate of State Approval

An application from a state or local court must include a copy of the *Certificate of State Approval* signed by the state's chief justice or state court administrator. The signature denotes that the proposed project has been approved by the state's highest court or the agency or council it has designated. Further, the signature denotes, if applicable, a cash-match reduction has been requested, and that if SJI approves funding for the project, the court or the specified designee will receive, administer, and be accountable for the awarded funds.

3. Budget Form

Applicants must provide a detailed budget and a budget narrative providing an explanation of the basis for the amounts in each budget category. If funds from other sources are required to conduct the project, either as a match or to support other aspects of the project, the source, current status of the request, and anticipated decision date must be provided.

4. Assurances

The *Assurances* form lists the statutory, regulatory, and policy requirements with which recipients of SJI funds must comply.

5. Disclosure of Lobbying Activities

Applicants other than units of state or local government are required to disclose whether they, or another entity that is part of the same organization as the applicant, have advocated a position before Congress on any issue, and to identify the specific subjects of their lobbying efforts.

6. Project Abstract

The abstract must highlight the purposes, goals, methods, and anticipated benefits of the proposed project. It must not exceed one single-spaced page and must be uploaded on the ''Attachments'' tab in the SJI GMS.

7. Program Narrative

The program narrative for an application may not exceed 25 double-spaced pages on 8½- by 11-inch paper with 1-inch margins, using a standard 12-point font. The pages must be numbered. This page limit does not include the forms, the abstract, the budget narrative, or any additional attachments. The program narrative must address the following, noting any specific areas to address by grant type:

*i. Statement of Need.* Applicants must explain the critical need they are facing and how SJI funds will enable them to meet this critical need. The applicants must also explain why state or local resources are not sufficient to fully support the costs of the project.

Applicants must provide a verified source for the data (*i.e.,* federal, state, and local databases) that supports the problem statement. The discussion must include specific references to the relevant literature and to experience in the field. SJI continues to make all grant reports and most grant products available online through the NCSC Library and Digital Archive. Applicants are required to conduct a search of the NCSC Library and Digital Archive on the topic areas they are addressing. This search must include SJI-funded grants and previous projects not supported by SJI. Searches for SJI grant reports and other state court resources begin with the NCSC Library section. Applicants must discuss the results of their research, how they plan to incorporate the previous work into their proposed project, and if the project will differ from prior work.

*ii. Project Grants.* If the project is to be conducted in any specific location(s), applicants must discuss the particular

needs of the project site(s) the project would address and why existing programs, procedures, services, or other resources do not meet those needs.

If the project is not site-specific, the applicants must discuss the problems that the proposed project would address and why existing programs, procedures, services, or other resources cannot adequately resolve those problems. In addition, applicants must describe how, if applicable, the project will be sustained in the future through existing resources.

*iii. TA Grants.* Applicants must explain why state or local resources are unable to fully support the modification and presentation of the model curriculum. The applicants must also describe the potential for replicating or integrating the adapted curriculum in the future using state or local funds once it has been successfully adapted and tested. In addition, applicants must describe how, if applicable, the project will be sustained in the future through existing resources.

*iv. CAT Grants (curriculum adaptation).* Applicants must explain why state or local resources are unable to fully support the modification and presentation of the model curriculum. The applicants must also describe the potential for replicating or integrating the adapted curriculum in the future using state or local funds once it has been successfully adapted and tested.

*v. CAT Grants (training).* Applicants must describe the court reform or initiative prompting the need for training. Applicants must also discuss how the proposed training will help them implement planned changes at the court and why state or local resources are not sufficient to fully support the costs of the required training.

*vi. SIGs.* Applicants must detail the origin of the project (*i.e.,* requested by SJI or a request to SJI) and provide a detailed description of the issue of national impact the proposed project will address, including any evaluations, reports, resolutions, or other data to support the need statement.

*b. Project Description and Objectives*

The applicants must include a clear, concise statement of what the proposed project is intended to accomplish and how those objectives will be met. Applicants must delineate the tasks to be performed in achieving the project objectives and the methods to be used for accomplishing each task.

Applicants must describe how the proposed project addresses one or more Priority Investment Areas. If the project does not address one or more Priority Investment Areas, the applicants must provide an explanation as to the reason.

1. Application Details by Project Type

*i. Project Grants.* The applicants must include detailed descriptions of tasks, methods, and evaluations. For example:

- *Research and evaluation projects.* The applicants must include the data sources, data collection strategies, variables to be examined, and analytic procedures to be used for conducting the research or evaluation and ensuring the validity and general applicability of the results. For projects involving human subjects, the discussion of methods must address the procedures for obtaining respondents' informed consent, ensuring the respondents' privacy and freedom from risk or harm, and protecting others who are not the subjects of research but would be affected by the research. If the potential exists for risk or harm to human subjects, a discussion must be included that explains the value of the proposed research and the methods to be used to minimize or eliminate such risk. Refer to section VIII.R.3, *Human Subject Protection,* of this guideline for additional information.
- *Education and training projects.* The applicants must include the adult education techniques to be used in designing and presenting the program, including the teaching and learning objectives of the educational design, the teaching methods to be used, and the opportunities for structured interaction among the participants. The opportunities applicants must include are: how faculty would be recruited, selected, and trained; the proposed number and length of the conferences, courses, seminars, or workshops to be conducted and the estimated number of persons who would attend them; the materials to be provided and how they would be developed; and the cost to participants.
- *Demonstration projects.* The applicants must include the demonstration sites and the reasons they were selected or, if the sites have not been chosen, how they would be identified; how the applicants would obtain the cooperation of demonstration sites; and how the program or procedures would be implemented and monitored.
- *TA projects.* The applicants must explain the types of assistance that would be provided, the particular issues and problems for which assistance would be provided, the type of assistance determined, how suitable providers would be selected and briefed, and how reports would be reviewed.

*ii. TA Grants.* Applicants must identify which organization or individual will be hired to provide the assistance and how the consultant was selected. The applicants must describe the tasks the consultant will perform and how the tasks will be accomplished.

If a consultant has not yet been identified, the applicants must describe the procedures and criteria that will be used to select the consultant (applicants are expected to follow their jurisdictions' normal procedures for procuring consultant services).

If the consultant has been identified, the applicants must provide a letter from that individual or organization documenting interest in and availability for the project, as well as the consultant's ability to complete the assignment within the proposed timeframe and for the proposed cost. The consultant must agree to submit a detailed written report to the court and SJI upon completion of the TA. Applicants must then describe the steps that have been or will be taken to facilitate implementation of the consultant's recommendations upon completion of the technical assistance.

The applicants must then address the following questions:

- What specific tasks will the consultant and court staff undertake?
- What is the schedule for completion of each required task and the entire project?
- How will the applicant oversee the project and provide guidance to the consultant, and who at the court or regional court association would be responsible for coordinating all project tasks and submitting Quarterly Progress and Financial Status Reports?

*iii. CAT Grants (curriculum adaptation).* The applicants must provide the title of the curriculum that will be adapted and identify the entity that originally developed the curriculum. Applicants must allow at least 90 days between the potential award date and the date of the proposed program to allow sufficient time for planning. This period of time should be reflected in the project timeline. The applicants must also address the following questions:

- Why is this education program needed at the present time?
- What are the project's goals?
- What are the learning objectives of the adapted curriculum?
- What program components would be implemented, and what types of modifications, if any, are anticipated in length, format, learning objectives, teaching methods, or content?
- Who would be responsible for adapting the model curriculum?

• Who would the participants be, how many would there be, how would they be recruited, and from where would they come (*e.g.,* from a single local jurisdiction, from across the state, from a multistate region, from across the nation, etc.)?

The applicants must also provide the proposed timeline, including the project start and end dates, the date(s) the judicial branch education program will be presented, and the process that will be used to modify and present the program. Applicants must also identify who will serve as faculty, and how they will be selected, in addition to the measures taken to facilitate subsequent presentations of the program.

*iv. CAT Grants (training).* The applicants must identify the tasks the trainer will be expected to perform, which organization or individual will be hired, and, if in-house personnel are not the trainer, how the trainer will be selected.

If a trainer has not yet been identified, the applicants must describe the procedures and criteria that will be used to select the trainer.

If the trainer has been identified, the applicants must provide a letter from that individual or organization documenting interest in and availability for the project, as well as the trainer's ability to complete the assignment within the proposed timeframe and for the proposed cost.

In addition, the applicants must address the following questions:

• What specific tasks would the trainer and court staff or regional court association members undertake?

• What presentation methods will be used?

• What is the schedule for completion of each required task and the entire project?

• How will the applicant oversee the project and provide guidance to the trainer, and who at the court or affiliated with the regional court association would be responsible for coordinating all project tasks and submitting Quarterly Progress and Financial Status Reports?

• The applicant must explain what steps have been or will be taken to coordinate the implementation of the training. For example, if the support or cooperation of specific court, regional court association officials, committees, other agencies, funding bodies, organizations, or a court other than the applicant will be needed to adopt the reform and initiate the proposed training, how will the applicant secure their involvement in the development and implementation of the training?

*v. SIGs.* The applicants should expand upon the project description and objectives described in the approved concept paper. Any and all feedback and questions submitted by the SJI Board of Directors and staff during the review of the concept paper should also be incorporated into the project design.

2. Dissemination Plan

The application must: (1) explain how and to whom the products would be disseminated; describe how they would benefit the state courts, including how they could be used by judges and court personnel; (2) identify development, production, and dissemination costs covered by the project budget; and (3) present the basis on which products and services developed or provided under the grant would be offered to the court community and the public at large (*i.e.,* whether products would be distributed at no cost to recipients, or if costs are involved, the reason for charging recipients and the estimated price of the product). Ordinarily, applicants must schedule all product preparation and distribution activities within the project period.

The type of product to be prepared depends on the nature of the project. For example, in most instances, the products of a research, evaluation, or demonstration project must include: (1) an article summarizing the project findings that is publishable in a journal serving the courts community nationally, (2) an executive summary that would be disseminated to the project's primary audience, or (3) both an article and executive summary. Applicants proposing to conduct empirical research or evaluation projects with national import must describe how they would make their data available for secondary analysis after the grant period.

The curricula and other products developed through education and training projects must be designed for use by others and again by the original participants in the course of their duties. Applicants proposing to develop web-based products must provide, for sending, a notice and description of the document (*i.e.,* a written report with a reference to the website) to the appropriate audiences to alert them to the availability of the website or electronic product.

Applicants must submit a final draft of all written grant products to SJI for review and approval at least 30 days before the products are submitted for publication or reproduction. Applicants must provide multimedia products for SJI review at the treatment, script, rough-cut, and final stages of development, or their equivalents. No grant funds may be obligated for publication or reproduction of a final grant product without the written approval of SJI. Project products should be submitted to SJI electronically in HTML or PDF format.

Applicants must also include in all project products a prominent acknowledgment that SJI provided support and a disclaimer paragraph such as, ''This [document, film, videotape, etc.] was developed under [grant/cooperative agreement] number SJI-[insert number] from the State Justice Institute. The points of view expressed are those of the [author(s), filmmaker(s), etc.] and do not necessarily represent the official position or policies of the State Justice Institute.'' The ''SJI'' logo must appear on the front cover of a written product or in the opening frames of a website or other multimedia products, unless SJI approves another placement. The SJI logo can be downloaded from SJI's website (*https://www.sji.gov*) at the bottom of the ''Grants'' page.

3. Staff Capability and Organizational Capacity

An applicant that is not a state or local court and has not received a grant from SJI within the past 3 years must indicate whether it is either: (1) a national nonprofit organization controlled by, operating in conjunction with, and serving the judicial branches of state governments; or (2) a national nonprofit organization for the education and training of state court judges and support personnel. If the applicant is a nonjudicial unit of Federal, State, or local government, it must explain whether the proposed services could be adequately provided by nongovernmental entities.

Applicants that have not received a grant from SJI within the past 3 years must include a statement describing their capacity to administer grant funds, including the financial systems used to monitor project expenditures (and income, if any), a summary of their past experience in administering grants, and any resources or capabilities they have that would particularly assist in the successful completion of the project.

Unless requested otherwise, an applicant that has received a grant from SJI within the past 3 years must describe only the changes in its organizational capacity, tax status, or financial capability that may affect its capacity to administer a grant. If the applicant is a nonprofit organization (other than a university), it must also provide documentation of its 501(c)(3) tax-exempt status as determined by the

Internal Revenue Service and a copy of a current certified audit report. For the purpose of this requirement, ''current'' means no earlier than 2 years prior to the present calendar year.

The applicant must include a summary of key staff members' and consultants' training and experience that qualify them to conduct and manage the proposed project. Resumes of identified staff should be attached to the application. If one or more key staff members and consultants are not known at the time of the application, a description of the criteria that would be used to select persons for these positions should be included. The applicant must also identify the person who would be responsible for managing and reporting on the financial aspects of the proposed project.

4. Evaluation

Projects must include an evaluation plan to determine whether the project has met its objectives. The evaluation must be designed to provide an objective and independent assessment of the effectiveness or usefulness of the training or services provided; the impact of the procedures, technology, or services tested; or the validity and applicability of the research conducted. The evaluation plan must be appropriate to the type of project proposed, considering the nature, scope, and magnitude of the project.

5. Sustainability

Describe how the project will be sustained after SJI assistance ends. The sustainability plan must describe how current collaborations and evaluations will be used to leverage ongoing resources. SJI encourages applicants to ensure sustainability by coordinating with local, state, and other federal resources.

*c. Budget and Matching State Contribution*

Applicants must complete a budget in the SJI GMS and upload a budget narrative. The budget narrative must provide the basis for all project-related costs and the sources of any match, as required. The budget narrative must thoroughly and clearly describe every category of expense listed. SJI expects proposed budgets to be complete, cost effective, and allowable (*i.e.,* reasonable, allocable, and necessary for project activities).

*1. Prohibited Uses of SJI Funds.* To ensure that funds made available are used to supplement and improve the operation of state courts, rather than to support basic court services, funds shall not be used:

- To supplant state or local funds supporting a program or activity (*e.g.,* paying the salary of court employees who would be performing their normal duties as part of the project or paying rent for space that is part of the court's normal operations).
- To construct court facilities or structures.
- Solely to purchase equipment.

Examples of *basic court services* include:

- Hiring of personnel;
- Purchase and/or maintenance of equipment;
- Purchase of software and/or licenses;
- Purchase of internet access or service;
- Supplies to support the day-to-day operations of courts.

The final determination of what constitutes basic court services is made by SJI and is not negotiable.

Meals and refreshments are not allowable costs.

Trinkets (*e.g.,* items such as hats, mugs, portfolios, t-shirts, coins, gift bags, gift cards, etc.) may not be purchased with SJI grant funding.

*2. Justification of Personnel Compensation.* The applicants must set forth the amount of time the individuals who would staff the proposed project would devote, the annual salary of each of those persons, and the number of workdays per year used to calculate the amount of time or daily rates of those individuals. The applicants must explain any deviations from current rates or established written organizational policies. No grant funds or cash match may be used to pay the salary and related costs for a current or new employee of a court or other unit of government because such funds would constitute a supplantation of state or local funds in violation of 42 U.S.C. 10706(d)(1); this includes new employees hired specifically for the project. The salary and any related costs for a current or new employee of a court or other unit of government may only be accepted as an in-kind match.

*3. Fringe Benefit Computation.* For nongovernmental entities, applicants must provide a description of the fringe benefits provided to employees. If percentages are used, the authority for such use should be presented, as well as a description of the elements included in the determination of the percentage rate.

*4. Consultant/Contractual Services and Honoraria.* The applicants must describe the tasks each consultant would perform, the estimated total amount to be paid to each consultant, the basis for compensation rates (*e.g.,* the number of days multiplied by the daily consultant rates), and the method for selection. Prior written SJI approval is required for any consultant rate in excess of $800 per day; SJI funds may not be used to pay a consultant more than $1,100 per day. Honorarium payments must be justified in the same manner as consultant payments.

*5. Travel.* Transportation costs and per diem rates must comply with the policies of the applicant organization. If the applicant does not have an established travel policy, then travel rates must be consistent with those established by the Federal Government. The budget narrative must include an explanation of the rate used, including the components of the per diem rate and the basis for the estimated transportation expenses. The purpose of the travel must also be included in the narrative.

*6. Equipment.* Grant funds may be used to purchase only the equipment necessary to demonstrate a new technological application in a court or that is otherwise essential to accomplishing the objectives of the project. In other words, grant funds cannot be used strictly for the purpose of purchasing equipment. Equipment purchases to support basic court operations will not be approved. Applicants must describe the equipment to be purchased or leased and explain why the acquisition of that equipment is essential to accomplish the project's goals and objectives. The narrative must clearly identify which equipment is to be leased and which is to be purchased. The method of procurement must also be described.

*7. Supplies.* Applicants must provide a general description of the supplies necessary to accomplish the goals and objectives of the grant. In addition, the applicants must provide the basis for the amount requested for this expenditure category.

*8. Construction.* Construction expenses are prohibited.

*9. Postage.* Anticipated postage costs for project-related mailings, including distribution of the final product(s), should be described in the budget narrative. The cost of special mailings, such as for a survey or for announcing a workshop, should be distinguished from routine mailing costs. The bases for all postage estimates should be included in the budget narrative.

*10. Printing/Photocopying.* Anticipated costs for printing or photocopying project documents, reports, and publications must be included in the budget narrative, along with the bases used to calculate these estimates.

*11. Indirect Costs.* Indirect costs are only applicable to organizations that are not state courts or government agencies. Recoverable indirect costs are limited to no more than 75 percent of a grantee's direct personnel costs (*i.e.,* salaries plus fringe benefits). Applicants must describe the indirect-cost rates applicable to the grant in detail. If costs often included within an indirect-cost rate are charged directly (*e.g.,* a percentage of the time of senior managers to supervise project activities), the applicants should specify that these costs are not included within their approved indirect-cost rate. If an applicant has an indirect-cost rate or allocation plan approved by any federal granting agency, a copy of the approved rate agreement must be attached to the application.

*12. Matching Requirements.* SJI grants require a match, which is the portion of project costs not borne by SJI and includes both cash and in-kind matches as outlined in this paragraph. A cash match is the direct outlay of funds by the grantee or a third party to support the project. Other federal department and agency funding may not be used for a cash match. An in-kind match consists of contributions of time and/or services of current staff members, new employees, space, supplies, etc., that are made to the project by the grantee or others (*e.g.,* advisory board members) working directly on the project. An in-kind match can also consist of that portion of the grantee's federally approved indirect-cost rate that exceeds the limit of permitted charges (75 percent of salaries and benefits).

The grantee is responsible for ensuring that the total amount of the match proposed is contributed. If a proposed contribution is not fully met, SJI may reduce the award amount accordingly, to maintain the ratio originally provided for in the award agreement. The match should be expended at the same rate as SJI funding.

*i. Project Grants.* Applicants for Project grants must contribute a cash match greater than or equal to the SJI award amount. This means that grant awards by SJI must be matched at least dollar for dollar by grant applicants. For example, an applicant seeking a $300,000 Project grant must provide a cash match of at least $300,000. Applicants may contribute the required cash match directly or in cooperation with third parties.

*ii. TA Grants.* Applicants for TA grants are required to contribute a total match (cash and in-kind) of no less than 50 percent of the SJI award amount, of which 20 percent must be cash. For example, an applicant seeking a $75,000 TA grant must provide a $37,500 match, of which up to $30,000 can be in-kind and not less than $7,500 must be cash.

*iii. CAT Grants.* Applicants for CAT grants are required to contribute a total match (cash and in-kind) of not less than 50 percent of the SJI award amount, of which 20 percent must be cash. For example, an applicant seeking a $40,000 CAT grant must provide a $20,000 match, of which up to $16,000 can be in-kind and not less than $4,000 must be cash. Funding from other federal departments and agencies may not be used for a cash match.

*iv. SIGs.* State and local courts and non-court units of government must provide a dollar-for-dollar cash match for SIG projects. Matching funds may not be required for SIG projects that are awarded to non-court or nongovernmental entities.

*13. Letters of Support.* Written assurances of support or cooperation should accompany the application letter if the support or cooperation of agencies, funding bodies, organizations, or courts other than the applicant would be needed in order for the consultant to perform the required tasks. Applicants may also submit memorandums of agreement or understanding, as appropriate.

*14. Project Timeline.* A project timeline detailing each project objective, activity, expected completion date, and responsible person or organization should be included. The plan should include the starting and completion date for each task; the time commitments to the project of key staff and their responsibilities regarding each project task; and the procedures that would ensure that all tasks are performed on time, within budget, and at the highest level of quality. In preparing the project timeline, applicants must make certain that all project activities, including publication or reproduction of project products and their initial dissemination, would occur within the proposed project period. The project timeline must also provide for the submission of Quarterly Progress and Financial Status Reports within 30 days after the close of each calendar quarter, as well as submission of all final closeout documents. The project timeline may be included in the program narrative or provided as a separate attachment.

*15. Other Attachments.* Resumes of key project staff may also be included. Additional background material should be attached only if it is essential to impart a clear understanding of the proposed project. Numerous and lengthy appendices are strongly discouraged.

*d. Application Review Information*

*1. Selection Criteria.* In addition to the criteria detailed below, SJI will consider whether the applicant is a state or local court, a national court support or education organization, a non-court unit of government, or other type of entity eligible to receive grants under SJI's enabling legislation; the availability of financial assistance from other sources for the project; the diversity of subject matter; geographic diversity; the level and nature of the match that would be provided; reasonableness of the proposed budget; the extent to which the proposed project would also benefit the federal courts or help state or local courts enforce federal constitutional and legislative requirements; and the level of appropriations available to SJI in the current year and the amount expected to be available in succeeding fiscal years, when determining which projects to support.

*2. Project Grant Applications.* Project grant applications will be rated based on the criteria set forth below:

- Soundness of the methodology.
- Demonstration of need for the project.
- Appropriateness of the proposed evaluation design.
- If applicable, the key findings and recommendations of the most recent evaluation and the proposed responses to those findings and recommendations.
- Applicant's management plan and organizational capabilities.
- Qualifications of the project's staff.
- Products and benefits resulting from the project, including the extent to which the project will have long-term benefits for state courts across the nation.
- Degree to which the findings, procedures, training, technology, or other results of the project can be transferred to other jurisdictions.
- Reasonableness of the proposed budget.
- Demonstration of cooperation and support of other agencies that may be affected by the project.

*3. TA Grant Applications.* TA grant applications will be rated based on the following criteria:

- Whether the assistance would address a critical need of the applicant.
- Soundness of the technical assistance approach to the problem.
- Qualifications of the consultant(s) to be hired or the specific criteria that will be used to select the consultant(s).
- Commitment of the court or association to act on the consultant's recommendations.
- Reasonableness of the proposed budget.

*4. CAT Grant Applications.* CAT grant applications will be rated based on the following criteria:

- Goals and objectives of the proposed project.
- How the training would address a critical need of the court or association.
- Need for outside funding to support the program.
- Soundness of the approach in achieving the project's educational or training objectives.
- Integration of distance learning and technology in project design and delivery.
- Qualifications of the trainer(s) to be hired or the specific criteria that will be used to select the trainer(s) (training project only).
- Likelihood of effective implementation and integration of the modified curriculum into the state or local jurisdiction's ongoing educational programming (curriculum adaptation project only).
- Commitment of the court or association to the training program (training project only).
- Expressions of interest by judges and/or court personnel, as demonstrated by letters of support.

*5. SIG Applications.* SIG applications will be rated based on the following criteria:

- Goals and objectives of the proposed project.
- Demonstration of need for the project.
- Degree to which the project addresses a current national court issue.
- Level of innovation in addressing the identified need.
- Potential impact on the court community.
- Qualifications of the consultant(s) engaged to manage the project.

*6. Review Process.* SJI reviews the application to make sure that the information presented is reasonable, understandable, measurable, and achievable, as well as consistent with this guideline. Applications must meet basic minimum requirements. Although specific requirements may vary by grant type, the following are common requirements applicable to all SJI grant applications:

- Must be submitted by an eligible type of applicant.
- Must request funding within funding constraints of each grant type (if applicable).
- Must be within statutorily allowable expenditures.
- Must include all required forms and documents.
- The SJI Board of Directors reviews all applications and makes final funding decisions. The decision to fund a project is solely that of the SJI Board of Directors.

*7. Notification of SJI Board of Directors Decision.* The Chairman of the Board signs grant awards on behalf of SJI. SJI will notify applicants regarding the SJI Board of Directors' decisions to award, defer, or deny their respective applications. If requested, SJI conveys the key issues and questions that arose during the review process. A decision by the SJI Board of Directors to deny an application may not be appealed, but it does not prohibit resubmission of a proposal in a subsequent funding cycle.

*8. Response to Notification of Award.* Grantees have 30 days from the date they were notified about their award to respond to any revisions requested by the SJI Board of Directors. If the requested revisions (or a reasonable schedule for submitting such revisions) have not been submitted to SJI within 30 days after notification, the award may be rescinded, and the application presented to the SJI Board of Directors for reconsideration. Special conditions, in the form of incentives or sanctions, may also be used in other situations.

## VI. How To Apply

Applicants must use the SJI GMS to submit all applications and post-award documents. SJI urges applicants to submit applications at least 72 hours prior to the application due date in order to allow time for the applicant to receive an application acceptance message and to correct, in a timely fashion, any problems that may arise, such as missing or incomplete forms. Files must be in .doc, .docx, .xls, .xlsx, .pdf, .jpg, or .png format. Individual file size cannot exceed 5 MB.

*a. Submission Steps*

Applicants (except for ESP) must register with the SJI GMS to submit applications for funding consideration. Below are the basic steps for submission:

1. Access the SJI GMS and complete the information required to create an account.
2. If you already have an account, log in and create a new application.
3. Complete all required forms and upload all required documents:
   - Application Form.
   - Certificate of State Approval.
   - Budget and Budget Narrative.
   - Assurances.
   - Disclosure of Lobbying Activities.
   - Project Abstract.
   - Program Narrative.
   - Attachments.
     - Letters of Support.
     - Project Timeline.
     - Resumes.
     - Indirect-Cost Approval.
     - Other Attachments.
4. Certify and submit the application to SJI for review.

## VII. Post-Award Reporting Requirements

All required reports and documents must be submitted via the SJI GMS.

*a. Quarterly Reporting Requirements*

Recipients of SJI funds must submit Quarterly Progress and Financial Status Reports within 30 days after the close of each calendar quarter (*i.e.,* no later than January 30, April 30, July 30, and October 30).

*1. Program Progress Reports.* Program Progress Reports must include a narrative description of project activities during the calendar quarter; the relationship between those activities, the task schedule, and objectives set forth in the approved application or an approved adjustment thereto; any significant problem areas that have developed and how they will be resolved; and the activities scheduled during the next reporting period. Failure to comply with the requirements of this provision could result in the termination of a grantee's award.

*2. Financial Reporting.* A Financial Status Report is required from all grantees for each active quarter on a calendar-quarter basis. This report is due within 30 days after the close of the calendar quarter. It is designed to provide financial information relating to SJI funds, state and local matching shares, project income, and any other sources of funds for the project, as well as information on obligations and outlays.

*b. Request for Reimbursement of Funds*

Awardees will receive funds on a reimbursable basis via electronic funds transfer (EFT) basis. All requests for reimbursement must include a Unique Entity Identifier (UEI) as generated by the System for Reward Management (SAM) with an active registration. Upon receipt, review, and approval of a request for reimbursement by SJI, payment will be issued directly to the grantee or its designated fiscal agent. Requests for reimbursements, along with the instructions for their preparation are available in the SJI GMS.

*1. Accounting System.* Awardees are responsible for establishing and maintaining an adequate system of accounting and internal controls. Awardees are also responsible for ensuring an adequate system exists for each of their subgrantees and

contractors. An acceptable and adequate accounting system:

- Properly accounts for receipt of funds under each grant awarded and the expenditure of funds for each grant by category of expenditure (including matching contributions and project income).
- Assures that expended funds are applied to the appropriate budget category included within the approved grant.
- Presents and classifies historical costs of the grant as required for budgetary and evaluation purposes.
- Provides cost and property controls to assure optimal use of grant funds.
- Is integrated with a system of internal controls adequate to safeguard the funds and assets covered, check the accuracy and reliability of the accounting data, promote operational efficiency, and assure conformance with any general or special conditions of the grant.
- Meets the prescribed requirements for periodic financial reporting of operations.
- Provides financial data for planning, control, measurement, and evaluation of direct and indirect costs.

*c. Final Progress Report*

The Final Progress Report must describe the project activities during the final calendar quarter of the project and the close-out period, including to whom project products have been disseminated; provide a summary of activities during the entire project; specify whether all the objectives set forth in the approved application or an approved adjustment have been met and, if any of the objectives have not been met, explain why not; and discuss what, if anything, could have been done differently that might have enhanced the impact of the project or improved its operation. In addition, grantees are required to submit electronic copies of the final products related to the project (*e.g.,* reports, curriculum, etc.). These reporting requirements apply at the conclusion of every grant.

**VIII. Compliance Requirements**

*a. Advocacy*

No funds made available by SJI may be used to support or conduct training programs for the purpose of advocating particular nonjudicial public policies or encouraging nonjudicial political activities (42 U.S.C. 10706(b)).

*b. Approval of Key Staff*

If the qualifications of an employee or consultant assigned to a key project staff position are not adequately described in the application or if there is a change of a person assigned to such a position, the recipient must submit a description of the qualifications of the newly assigned person to SJI. Prior written approval of the qualifications of the new person assigned to a key staff position must be received from SJI before the salary or consulting fee of that person and associated costs may be paid or reimbursed from grant funds.

*c. Audit*

Recipients of SJI grants must provide for an annual fiscal audit, which includes an opinion on whether the financial statements of the grantee fairly present its financial position and its financial operations in accordance with generally accepted accounting principles. If requested, a copy of the audit report must be made available electronically to SJI.

*d. Budget Revisions*

Prior SJI approval is required for budget revisions among direct-cost categories that: (1) transfer grant funds to an unbudgeted cost category; or (2) individually or cumulatively exceed 5 percent of the approved original budget or the most recently approved revised budget. Refer to section X, *Grant Adjustments,* of this guideline for additional details about the process for modifying the project budget.

*e. Conflict of Interest*

Personnel and other officials connected with SJI-funded programs must adhere to the following requirements:

- Officials or employees of a recipient court or organization must not participate personally through decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise, in any proceeding, application, request for a ruling or other determination, contract, grant, cooperative agreement, claim, controversy, or other particular matter in which SJI funds are used, where, to their knowledge, they or their immediate family; partners; organization other than a public agency in which they are serving as officer, director, trustee, partner, or employee; or any person or organization with whom they are negotiating or have any arrangement concerning prospective employment have a financial interest.
- In the use of SJI project funds, an official or employee of a recipient court or organization must avoid any action that might result in or create the appearance of:
  - using an official position for private gain; or
  - adversely affecting the confidence of the public in the integrity of the SJI program.
- Requests for proposals (RFPs) or invitations for bids issued by a recipient of SJI funds or a subgrantee or subcontractor will provide notice to prospective bidders that the contractors who develop or draft specifications, requirements, statements of work, and/or RFPs for a proposed procurement will be excluded from bidding on or submitting a proposal to compete for the award of such procurement.

*f. Inventions and Patents*

If any patentable items, patent rights, processes, or inventions are produced during the course of SJI-sponsored work, such fact must be promptly and fully reported to SJI. Unless there is a prior agreement between the grantee and SJI on the disposition of such items, SJI will determine whether protection of the invention or discovery may be sought should the grantee choose to pursue such protection.

*g. Lobbying*

Funds awarded to recipients by SJI must not be used—directly or indirectly—to influence Executive Orders or similar promulgations by federal, state, or local agencies; or to influence the passage or defeat of any legislation by federal, state, or local legislative bodies (42 U.S.C. 10706(a)).

It is the policy of the SJI Board of Directors to award funds only to support applications submitted by organizations that would carry out the objectives of their applications in an unbiased manner. Consistent with this policy and the provisions of 42 U.S.C. 10706, SJI will not knowingly award a grant to an applicant that has, directly or through an entity that is part of the same organization as the applicant, advocated a position before Congress on the specific subject matter of the application.

*h. Matching Requirements*

All grant recipients are required to provide a match. A match is the portion of project costs not borne by SJI. A match includes both cash and in-kind contributions. A cash match is the direct outlay of funds by the grantee or a third party to support the project. An in-kind match for state and local courts or other units of government consists of contributions of time and/or services of current staff members, new employees, space, supplies, etc., made to the project by the grantee or others (*e.g.,* advisory board members) working directly on the project. Generally, these same items are considered cash matches for

nongovernmental entities. For nongovernmental entities, a federally approved indirect-cost rate may be used as an in-kind match for that portion of the rate that exceeds the limit of permitted charges for indirect costs (75 percent of salaries and benefits).

Under normal circumstances, an allowable match may be incurred only during the project period. The amount and nature of the required match depends on the type of grant. Refer to section V.C.12, *Matching Requirements,* of this guideline for details by grant type.

The grantee is responsible for ensuring that the total amount of the match proposed is contributed. If a proposed contribution is not fully met, SJI may reduce the award amount accordingly to maintain the ratio originally provided for in the award agreement. The match should be expended at the same rate as SJI funding.

The SJI Board of Directors looks favorably upon any unrequired match contributed by applicants when making grant decisions. The match requirement may be waived in exceptionally rare circumstances upon the request of the chief justice of the highest court in the state or the highest-ranking official in the requesting organization, and approval by the SJI Board of Directors (42 U.S.C. 10705(d)). The SJI Board of Directors encourages all applicants to provide the maximum amount of cash and in-kind match possible, even if a waiver is approved. The amount and nature of the match are criteria in the grant selection process.

Other federal department and agency funding may not be used for a cash match.

*i. Nondiscrimination*

No person may, on the basis of race, sex, national origin, disability, color, or creed, be excluded from participation in, denied the benefits of, or otherwise subjected to discrimination under any program or activity supported by SJI funds. Recipients of SJI funds must take any measures necessary to effectuate this provision immediately.

*j. Political Activities*

No recipient may contribute or make available SJI funds, program personnel, or equipment to any political party or association or the campaign of any candidate for public or party office. Recipients are also prohibited from using funds in advocating or opposing any ballot measure, initiative, or referendum. Officers and employees of recipients must not intentionally identify SJI or recipients with any partisan or nonpartisan political activity associated with a political party or association or the campaign of any candidate for public or party office (42 U.S.C. 10706(a)).

*k. Products*

*1. Acknowledgment, Logo, and Disclaimer.* Recipients of SJI funds must acknowledge prominently on all products that were developed with grant funds that support was received from SJI. The SJI logo must appear on the front cover of a written product, or in the opening frames of a multimedia product, unless another placement is approved in writing by SJI. This includes final products printed or otherwise reproduced during the grant period as well as reprintings or reproductions of those materials following the end of the grant period. The SJI logo can be downloaded from SJI's website (*https://www.sji.gov*) at the bottom of the ''Grants'' page.

Recipients also must display the following disclaimer on all grant products: ''This [document, film, videotape, etc.] was developed under [grant/cooperative agreement] number SJI-[insert number] from the State Justice Institute. The points of view expressed are those of the [author(s), filmmaker(s), etc.] and do not necessarily represent the official position or policies of the State Justice Institute.''

*i. Project Grants.* In addition to other required grant products and reports, recipients must provide a one-page executive summary of the project. The summary should include a background on the project, the tasks undertaken, and the outcome. In addition, the summary should provide the performance metrics that were used during the project, and how performance will be measured in the future.

*ii. TA Grants.* Grantees must submit a final report that explains how they intend to act on the consultant's recommendations as well as a copy of the consultant's written report. Both should be submitted in electronic format.

*iii. CAT Grants.* Grantees must submit an electronic version of the agenda or schedule, an outline of presentations and/or relevant instructor's notes; copies of overhead transparencies, Microsoft PowerPoint presentations, or other visual aids; exercises, case studies, and other background materials; hypotheticals, quizzes, and other materials involving the participants; manuals, handbooks, conference packets, and evaluation forms; and suggestions for replicating the program, including possible faculty or the preferred qualifications or experience of those selected as faculty, developed under the grant after the grant period, along with a final report that includes any evaluation results and explains how the grantee intends to present the educational program in the future, as well as the consultant's or trainer's report. All items should be submitted in electronic format.

*2. Charges for Grant-Related Products/Recovery of Costs.* SJI's mission is to support improvements in the quality of justice and foster innovative, efficient solutions to common issues faced by all courts. SJI has recognized and established procedures for supporting research and development of grant products (*e.g.,* a report, curriculum, video, software, database, or website) through competitive grant awards based on the merit reviews of proposed projects. To ensure that all grants benefit the entire court community, projects SJI considers worthy of support (in whole or in part) are required to be disseminated widely and to be available for public consumption. This includes open-source software and interfaces. Costs for development, production, and dissemination are allowable as direct costs to SJI.

Applicants must disclose their intent to sell grant-related products in the application. Grantees must obtain SJI's prior written approval of their plans to recover project costs through the sale of grant products. Written requests to recover costs ordinarily should be received during the grant period and should specify the nature and extent of the costs to be recouped, the reason that such costs were not budgeted (if the rationale was not disclosed in the approved application), the number of copies to be sold, the intended audience for the products to be sold, and the proposed sale price. If the product is to be sold for more than $25, the written request should also include a detailed itemization of costs that will be recovered and a certification that the costs were not supported by either SJI grant funds or grantee matching contributions.

In the event that the sale of grant products results in revenues that exceed the costs to develop, produce, and disseminate the product, the revenue must continue to be used for the authorized purposes of the SJI-funded project or other purposes consistent with the State Justice Institute Act that have been approved by SJI.

*l. Copyrights*

Except as otherwise provided in the terms and conditions of an SJI award, a

recipient is free to copyright any books, publications, or other copyrightable materials developed in the course of an SJI-supported project. SJI must reserve a royalty-free, nonexclusive, and irrevocable right to reproduce, publish, or otherwise use, and to authorize others to use, the materials for purposes consistent with the State Justice Institute Act.

*m. Due Date*

All products and, for TA and CAT grants, consultant and/or trainer reports are to be completed and distributed not later than the end of the award period, not the 90-day closeout period. The 90-day closeout period is intended only for grantee final reporting and to liquidate obligations.

*n. Distribution*

In addition to the distribution specified in the grant application, grantees must send an electronic version of all products in HTML or PDF format to SJI.

*o. Original Material*

All products prepared as the result of SJI-supported projects must be originally developed material unless otherwise specified in the award documents. Material not originally developed that is included in such products must be properly identified, whether the material is in a verbatim or extensive paraphrase format.

*p. Prohibition Against Litigation Support*

No funds made available by SJI may be used directly or indirectly to support legal assistance for parties in litigation, including cases involving capital punishment.

*q. Reporting Requirements*

All reports must be submitted via the SJI GMS as detailed below:

*1. Quarterly Progress and Financial Status Reports.* Recipients of SJI funds must submit Quarterly Progress and Financial Status Reports within 30 days after the close of each calendar quarter (*i.e.,* no later than January 30, April 30, July 30, and October 30). The Quarterly Progress Reports must include a narrative description of project activities during the calendar quarter; the relationship between those activities, the task schedule, and objectives set forth in the approved application or an approved adjustment thereto; any significant problem areas that have developed and how they will be resolved; and the activities scheduled during the next reporting period. Failure to comply with the requirements of this provision could result in the termination of a grantee's award.

*2. Quarterly Financial Reporting.* The Quarterly Financial Report must be submitted in accordance with section VII.A.2, *Financial Reporting,* of this guideline. A Final Progress Report and Financial Status Report must be submitted within 90 days after the end of the grant period.

*r. Research*

*1. Availability of Research Data for Secondary Analysis.* Upon request, grantees must make available for secondary analysis backup files containing research and evaluation data collected under an SJI grant and the accompanying code manual. Grantees may recover the actual cost of duplicating and mailing, or otherwise transmitting, the dataset and manual from the person or organization requesting the data. Grantees may provide the requested dataset in the format in which it was created and analyzed.

*2. Confidentiality of Information.* Except as provided by federal law other than the State Justice Institute Act, no recipient of financial assistance from SJI may use or reveal any research or statistical information furnished under the Act by any person and identifiable to any specific private person for any purpose other than the purpose for which the information was obtained. Such information and copies thereof will be immune from legal process and must not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action; suit; or other judicial, legislative, or administrative proceedings.

*3. Human Subject Protection.* Human subjects are defined as individuals who are participants in an experimental procedure or who are asked to provide information about themselves, their attitudes, feelings, opinions, and/or experiences through an interview, questionnaire, or other data collection technique. All research involving human subjects must be conducted with the informed consent of those subjects and in a manner that will ensure their privacy and freedom from risk or harm and the protection of persons who are not subjects of the research but would be affected by it—unless such procedures and safeguards would make the research impractical. In such instances, SJI must approve procedures designed by the grantee to provide human subjects with relevant information about the research after their involvement and minimize or eliminate risk or harm to those subjects due to their participation.

*4. Prohibited Uses of SJI Funds.* To ensure SJI funds are used to supplement and improve the operation of state courts, rather than to support basic court services, SJI funds must not be used for the following purposes:

- To supplant state or local funds supporting a program or activity (*e.g.,* paying the salary of court employees who would be performing their normal duties as part of the project or paying rent for space which is part of the court's normal operations).
- To construct court facilities or structures.
- Solely to purchase equipment.

Examples of *basic court services* include:

- Hiring of personnel
- Purchase and/or maintenance of equipment
- Purchase of software and/or licenses
- Purchase of internet access or service
- Supplies to support the day-to-day operations of courts

The final determination of what constitutes basic court services is made by SJI and is not negotiable.

Meals and refreshments are not allowable.

Trinkets (*e.g.,* hats, mugs, portfolios, t-shirts, coins, gift bags, gift cards, etc.) may not be purchased with SJI grant funding.

*5. Suspension or Termination of Funding.* After providing a recipient reasonable notice and opportunity to submit written documentation demonstrating why fund termination or suspension should not occur, SJI may terminate or suspend funding of a project that fails to substantially comply with the Act, the Grant Guideline, or the terms and conditions of the award (42 U.S.C. 10708(a)).

*6. Title to Property.* At the conclusion of the project, title to all expendable and nonexpendable personal property purchased with SJI funds must vest in the recipient court, organization, or individual that purchased the property if certification is made to and approved by SJI that the property will continue to be used for the authorized purposes of the SJI-funded project or other purposes consistent with the State Justice Institute Act. If such certification is not made or SJI disapproves of such certification, title to all such property with an aggregate or individual value of $1,000 or more must vest in SJI, which will direct the disposition of the property.

## IX. Financial Requirements

The purpose of this section is to establish accounting system

requirements and offer guidance on procedures to assist all grantees, subgrantees, contractors, and other organizations in:

- Complying with the statutory requirements for the award, disbursement, and accounting of funds.
- Complying with regulatory requirements of SJI for the financial management and disposition of funds.
- Generating financial data to be used in planning, managing, and controlling projects.
- Facilitating an effective audit of funded programs and projects.

*a. Supervision and Monitoring Responsibilities*

All grantees receiving awards from SJI are responsible for the management and fiscal control of all funds. Responsibilities include accounting for receipts and expenditures, maintaining adequate financial records, and refunding expenditures disallowed by audits. If the project includes subawards, the grantees' responsibilities also include:

*1. Reviewing Financial Operations.* The grantee or its designee must be familiar with, and periodically monitor, its subgrantee's financial operations, records system, and procedures. Particular attention should be directed to the maintenance of current financial data.

*2. Recording Financial Activities.* The subgrantee's grant award or contract obligation as well as cash advances and other financial activities must be recorded in the financial records of the grantee or its designee in summary form. Subgrantee expenditures must be recorded on the books of the state supreme court or evidenced by report forms duly filed by the subgrantee. Matching contributions provided by subgrantees must likewise be recorded, as should any project income resulting from program operations.

*3. Budgeting and Budget Review.* The grantee or its designee must ensure that each subgrantee prepares an adequate budget as the basis for its award commitment. The state supreme court must maintain the details of each project budget on file.

*4. Accounting for Match.* The grantee or its designee will ensure that subgrantees comply with the match requirements specified in this guideline.

*5. Audit Requirement.* The grantee or its designee is required to ensure that subgrantees meet the necessary audit requirements set forth by SJI.

*6. Reporting Irregularities.* The grantee, its designees, and its subgrantees are responsible for promptly reporting to SJI the nature and circumstances surrounding any financial irregularities discovered.

*b. Accounting System*

The grantee is responsible for establishing and maintaining an adequate system of accounting and internal controls and for ensuring that an adequate system exists for each of its subgrantees and contractors. An acceptable and adequate accounting system:

- Properly accounts for receipt of funds under each grant awarded and the expenditure of funds for each grant by category of expenditure, including matching contributions and project income.
- Assures that expended funds are applied to the appropriate budget category included within the approved grant.
- Presents and classifies historical costs of the grant as required for budgetary and evaluation purposes.
- Provides cost and property controls to assure optimal use of grant funds.
- Is integrated with a system of internal controls adequate to safeguard the funds and assets covered, check the accuracy and reliability of the accounting data, promote operational efficiency, and assure conformance with any general or special conditions of the grant.
- Meets the prescribed requirements for periodic financial reporting of operations.
- Provides financial data for planning, control, measurement, and evaluation of direct and indirect costs.

*c. Total Cost Budgeting and Accounting*

Accounting for all funds awarded by SJI must be structured and executed on a total-project-cost basis. That is, total project costs, including SJI funds, state and local matching shares, and any other fund sources included in the approved project budget, serve as the foundation for fiscal administration and accounting. Grant applications and financial reports require budget and cost estimates based on total costs.

*1. Timing of Matching Contributions.* Matching contributions should be applied at the same time as the obligation of SJI funds. Ordinarily, the full matching share must be obligated during the award period; however, with the written permission of SJI, contributions made following approval of the grant by the SJI Board of Directors but before the beginning of the grant may be counted as a match. If a proposed cash or in-kind match is not fully met, SJI may reduce the award amount accordingly to maintain the ratio of grant funds to matching funds stated in the award agreement.

*2. Records for Match.* All grantees must maintain records that clearly show the source, amount, and timing of all matching contributions. In addition, if a project has included, within its approved budget, contributions that exceed the required matching portion, the grantee must maintain records of those contributions in the same manner as it does SJI funds and required matching shares. For all grants made to state and local courts, the state supreme court has primary responsibility for grantee/subgrantee compliance with the requirements of this section.

*3. Maintenance and Retention of Records.* All financial records—including supporting documents; statistical records; and all other information pertinent to grants, subgrants, cooperative agreements, or contracts under grants—must be retained by each organization participating in a project for at least 3 years for purposes of examination and audit. State supreme courts may impose record retention and maintenance requirements in addition to those prescribed in this section.

*4. Coverage.* The retention requirement extends to books of original entry, source documents supporting accounting transactions, the general ledger, subsidiary ledgers, personnel and payroll records, canceled checks, and related documents and records. Source documents include copies of all grant and subgrant awards, applications, and required grantee/subgrantee financial and narrative reports. Personnel and payroll records must include the time and attendance reports for all individuals reimbursed under a grant, subgrant, or contract, whether they are employed full or part time. Time and effort reports are required for consultants.

*5. Retention Period.* The 3-year retention period starts from the date of the submission of the final expenditure report.

*6. Maintenance.* Grantees and subgrantees are expected to see that records of different fiscal years are separately identified and maintained so that requested information can be readily located. Grantees and subgrantees are also obligated to protect records adequately against fire or other damage. When records are stored away from the grantee's or subgrantee's principal office, a written index of the location of stored records should be on hand, and ready access should be assured.

*7. Access.* Grantees and subgrantees must give any authorized representative

of SJI access to and the right to examine all records, books, papers, and documents related to an SJI grant.

*8. Project-Related Income.* Records of the receipt and disposition of project-related income must be maintained by the grantee in the same manner as required for the project funds that gave rise to the income and must be reported to SJI (see section VII.A.2, *Financial Reporting,* of this guideline). The policies governing the disposition of the various types of project-related income are listed below.

*i. Interest.* A state and any agency or instrumentality of a state, including institutions of higher education and hospitals, will not be held accountable for interest earned on advances of project funds. When funds are awarded to subgrantees through a state, the subgrantees are not held accountable for interest earned on advances of project funds. Local units of government and nonprofit organizations that are grantees must refund any interest earned. Grantees must ensure minimum balances in their respective grant cash accounts.

*ii. Royalties.* The grantee or subgrantee may retain all royalties received from copyrights or other works developed under projects or from patents and inventions unless the terms and conditions of the grant provide otherwise.

*iii. Registration and Tuition Fees.* Registration and tuition fees may be considered as a cash match with prior written approval from SJI. Estimates of registration and tuition fees and any expenses to be offset by the fees should be included in the application budget forms and narrative.

*iv. Income from the Sale of Grant Products.* If the sale of products occurs during the project period, the income may be treated as a cash match with the prior written approval of SJI. The costs and income generated by the sales must be reported on the Quarterly Progress and Financial Status Reports and documented in an auditable manner. Whenever possible, the intent to sell a product should be disclosed in the application or reported to SJI in writing once a decision to sell products has been made. The grantee must request approval to recover its product development, reproduction, and dissemination costs (see section VIII.K.2, *Charges for Grant-Related Products/Recovery of Costs,* of this guideline).

*v. Other.* Other project income will be treated in accordance with disposition instructions set forth in the grant's terms and conditions.

*d. Payments and Financial Reporting Requirements*

The procedures and regulations set forth below are applicable to all SJI grant funds and grantees.

*1. Request for Reimbursement of Funds.* Grantees will receive funds on a reimbursable, U.S. Department of the Treasury check-issued or EFT basis. Upon receipt, review, and approval of a Request for Reimbursement (Form R) by SJI, payment will be issued directly to the grantee or its designated fiscal agent. The Form R, along with the instructions for its preparation and the SF 3881 Automated Clearing House (ACH/Miscellaneous Payment Enrollment Form for EFT), are available for download and submission in the SJI GMS.

2. Financial Reporting

*i. General Requirements.* To obtain financial information concerning the use of funds, SJI requires that grantees/subgrantees submit timely reports for review.

*ii. Due Dates and Contents.* A Financial Status Report is required from all grantees for each active quarter on a calendar-quarter basis. This report is due within 30 days after the close of the calendar quarter. It is designed to provide financial information relating to SJI funds, state and local matching shares, project income, and any other sources of funds for the project, as well as information on obligations and outlays. The Financial Status Report (Form F), along with instructions, is accessible in the SJI GMS. If a grantee requests substantial payment for a project prior to the completion of a given quarter, SJI may request a brief summary of the amount requested, by object class, to support the Request for Reimbursement.

*iii. Consequences of Noncompliance with Submission Requirement.* Failure of the grantee to submit required Progress and Financial Status Reports may result in suspension or termination of grant reimbursement.

*e. Allowability of Costs*

1. Costs Requiring Prior Approval

*i. Pre-Agreement Costs.* The written prior approval of SJI is required for costs that are considered necessary but that occur prior to the start date of the project period.

*ii. Equipment.* Grant funds may be used to purchase or lease only that equipment essential to accomplishing the goals and objectives of the project. The written prior approval of SJI is required when: (1) the amount of automated data processing equipment to be purchased or leased exceeds $10,000; or (2) the amount of software to be purchased exceeds $3,000.

*iii. Consultants.* The written prior approval of SJI is required when the rate of compensation to be paid to a consultant exceeds $800 a day. SJI funds may not be used to pay a consultant more than $1,100 per day.

*iv. Budget Revisions.* Prior SJI approval is required for budget revisions among direct-cost categories that: (1) transfer grant funds to an unbudgeted cost category; or (2) individually or cumulatively exceed 5 percent of the approved original budget or the most recently approved revised budget.

*2. Travel Costs.* Transportation and per diem rates must comply with the policies of the grantee. If the grantee does not have an established written travel policy, then travel rates must be consistent with those established by the U.S. General Services Administration. Grant funds may not be used to cover the transportation or per diem costs for a member of a national organization to attend an annual or other regular meeting, or conference of that organization.

*3. Indirect Costs.* Indirect costs are only applicable to organizations that are not state courts or government agencies. These are costs of an organization that are not readily assignable to a particular project but are necessary to the operation of the organization and the performance of the project. The costs of operating and maintaining facilities, depreciation, and administrative salaries are examples of the types of costs that are usually treated as indirect costs. Although SJI's policy requires all costs to be budgeted directly, it will accept indirect costs if a grantee has an indirect-cost rate approved by a federal agency; however, recoverable indirect costs are limited to no more than 75 percent of a grantee's direct personnel costs (salaries plus fringe benefits).

*i. Approved Plan Available.*

- A copy of an indirect-cost-rate agreement or allocation plan approved for a grantee during the preceding 2 years by any federal granting agency on the basis of allocation methods substantially in accord with those set forth in the applicable cost circulars must be submitted to SJI.

- Where flat rates are accepted in lieu of actual, indirect costs, grantees may not also charge expenses normally included in overhead pools (*e.g.,* accounting services, legal services, building occupancy and maintenance, etc.) as direct costs.

*f. Audit Requirements*

*1. Implementation.* Grantees must provide for an annual fiscal audit. This requirement also applies to a state or local court receiving a subgrant from the state supreme court. Audits conducted using generally accepted auditing standards in the United States will satisfy the requirement for an annual fiscal audit. The audit must be conducted by an independent Certified Public Accountant or a state or local agency authorized to audit government agencies. The audit report must be made available to SJI electronically, if requested.

*2. Resolution and Clearance of Audit Reports.* Timely action on recommendations by responsible management officials is an integral part of the effectiveness of an audit. Each grantee must have policies and procedures for acting on audit recommendations by designating officials responsible for:

- Following up.
- Maintaining a record of the actions taken on recommendations and time schedules.
- Responding to and acting on audit recommendations.
- Submitting periodic reports to SJI on recommendations and actions taken.

*3. Consequences of Non-Resolution of Audit Issues.* Ordinarily, SJI will not make a subsequent grant award to an applicant that has an unresolved audit report involving SJI awards. Failure of the grantee to resolve audit questions may also result in the suspension or termination of payments for active SJI grants to that organization.

*g. Closeout of Grants*

*1. Grantee Closeout Requirements.* Within 90 days of the end date of the grant or any approved extension thereof, the following documents must be submitted to SJI by grantees:

*i. Financial Status Report.* The final report of expenditures must have no unliquidated obligations and must indicate the exact balance of unobligated funds. Any unobligated or unexpended funds will be de-obligated from the award by SJI. Final payment requests for obligations incurred during the award period must be submitted to SJI prior to the end of the 90-day closeout period.

*ii. Final Progress Report.* This report should describe the project activities during the final calendar quarter of the project and the closeout period, including to whom project products have been disseminated; provide a summary of activities during the entire project; specify whether all the objectives set forth in the approved application or an approved adjustment have been met and, if any of the objectives have not been met, explain why not; and discuss what, if anything, could have been done differently that might have enhanced the impact of the project or improved its operation. These reporting requirements apply at the conclusion of every grant.

*2. Extension of Closeout Period.* Upon the written request of the grantee, SJI may extend the closeout period to assure completion of the grantee's closeout requirements. Requests for an extension must be submitted at least 14 days before the end of the closeout period and must explain why the extension is necessary and what steps will be taken to assure that all the grantee's responsibilities will be met by the end of the extension period. Extensions must be submitted via the SJI GMS as Grant Adjustments.

**X. Grant Adjustments**

All requests for programmatic or budgetary adjustments requiring SJI approval must be submitted by the project director in a timely manner (ordinarily 30 days prior to the implementation of the adjustment being requested). All requests for changes from the approved application will be carefully reviewed for both consistency with this guideline and the enhancement of grant goals and objectives. Failure to submit adjustments in a timely manner may result in the termination of a grantee's award.

*a. Grant Adjustments Requiring Prior Written Approval*

The following Grant Adjustments require the prior written approval of SJI:

- Budget revisions among direct-cost categories that: (1) transfer grant funds to an unbudgeted cost category; or (2) individually or cumulatively exceed 5 percent of the approved original budget or the most recently approved revised budget.
- A change in the scope of work to be performed or the objectives of the project.
- A change in the project site.
- A change in the project period, such as an extension of the grant period or extension of the Final Financial Report or Final Progress Report deadline.
- Satisfaction of special conditions, if required.
- A change in or temporary absence of the project director.
- The assignment of an employee or consultant to a key staff position whose qualifications were not described in the application, or a change in a person assigned to a key project staff position.
- A change in or temporary absence of the person responsible for managing and reporting on the grant's finances.
- A change in the name of the grantee organization.
- A transfer or contracting out of grant-supported activities.
- A transfer of the grant to another recipient.
- Pre-agreement costs.
- The purchase of Americans with Disabilities Act (ADA) equipment and software.
- Consultant rates.
- A change in the nature or number of the products to be prepared or the way a product would be distributed.

*b. Requests for Grant Adjustments*

All grantees must promptly notify SJI, in writing, of events or proposed changes that may require adjustments to the approved project design. In requesting an adjustment, the grantee must set forth the reasons and basis for the proposed adjustment and any other information the program manager determines would help SJI's review. All requests for Grant Adjustments must be submitted via the SJI GMS.

*c. Notification of Approval or Disapproval*

If the request is approved, the grantee will be sent a Grant Adjustment signed by the SJI Executive Director. If the request is denied, the grantee will be sent a written explanation of the reasons for the denial.

*d. Changes in the Scope of the Grant*

Major changes in scope, duration, training methodology, or other significant areas must be approved in advance by SJI. A grantee may make minor changes to methodology, approach, or other aspects of the grant to expedite achievement of the grant's objectives with subsequent notification to SJI.

*e. Date Changes*

A request to change or extend the grant period must be made at least 30 days in advance of the end date of the grant. A revised task plan must accompany a request for an extension of the grant period, along with a revised budget if shifts among budget categories will be needed. A request to change or extend the deadline for the Final Financial Report or Final Progress Report must be made at least 14 days in advance of the report deadline.

*f. Temporary Absence of the Project Director*

Whenever an absence of the project director is expected to exceed a continuous period of 1 month, the plans for the conduct of the project director's duties during such absence must be approved in advance by SJI. This information must be provided in a letter signed by an authorized representative of the grantee or subgrantee at least 30 days before the departure of the project director or as soon as it is known that the project director will be absent. The grant may be terminated if arrangements are not approved in advance by SJI.

*g. Withdrawal of or Change in Project Director*

If the project director relinquishes or expects to relinquish active direction of the project, SJI must be notified immediately. In such cases, if the grantee or subgrantee wishes to terminate the project, SJI will forward procedural instructions upon notification of such intent. If the grantee wishes to continue the project under the direction of another individual, a statement of the candidate's qualifications should be sent to SJI for review and approval. The grant may be terminated if the qualifications of the proposed individual are not approved in advance by SJI.

*h. Transferring or Contracting Out of Grant-Supported Activities*

No principal activity of a grant-supported project may be transferred or contracted out to another organization without specific prior approval by SJI. All such arrangements must be formalized in a contract or other written agreement between the parties involved. Copies of the proposed contract or agreement must be submitted for prior approval to SJI at the earliest possible time. The contract or agreement must state, at a minimum, the activities to be performed, the time schedule, the policies and procedures to be followed, the dollar limitation of the agreement, and the cost principles to be followed in determining what costs, both direct and indirect, will be allowed. The contract or other written agreement must not affect the grantee's overall responsibility for the direction of the project and accountability to SJI.

**State Justice Institute Board of Directors**

Hon. John Minton (Chair), Chief Justice, Supreme Court of Kentucky, Frankfort, KY
Daniel Becker (Vice Chair), State Court Administrator (ret.), Utah Administrative Office of the Courts, Salt Lake City, UT
Hon. Gayle A. Nachtigal (Secretary), Circuit Court Judge (ret.), Washington County Circuit Court, Hillsboro, OR
Hon. David Brewer (Treasurer), Justice (ret.), Supreme Court of Oregon, Salem, OR
Hon. Jonathan Lippman, Chief Judge of the State of New York (ret.); Of Counsel, Latham & Watkins, LLP, New York, NY
Hon. Chase Rogers, Chief Justice (ret.), Supreme Court of Connecticut; Partner, Day Pitney, LLP, Hartford, CT
Hon. Wilfredo Martinez, Senior Judge, Ninth Judicial Circuit of Florida, Orlando, FL
Marsha J. Rabiteau, President & CEO, Center for Human Trafficking Court Solutions, Bloomfield, CT
Jonathan D. Mattiello, Executive Director (ex officio)

**Jonathan D. Mattiello,**

*Executive Director.*

[FR Doc. 2025–19664 Filed 10–24–25; 8:45 am]

**BILLING CODE 6820–SC–P**

## DEPARTMENT OF TRANSPORTATION

### Office of the Secretary

**[Docket No. DOT–OST–2025–1921]**

### Agency Requests for Renewal of a Previously Approved Information Collection: TAR Part 1239-Related

**AGENCY:** Office of the Secretary (OST), U.S. Department of Transportation (DOT).

**ACTION:** Notice and request for comments.

**SUMMARY:** In accordance with the Paperwork Reduction Act of 1995, and Office of Management and Budget (OMB) regulations, the Department of Transportation (DOT) invites public comments on currently approved Transportation Acquisition Regulation (TAR) part 1239 information collection requests (ICRs) and our intention to request OMB approval to renew the ICRs on an interim basis as abstracted below while DOT undertakes further review to streamline its regulations. The public will be afforded another opportunity to review revised streamlined TAR content when published as a part of a proposed rule. DOT is required to publish this notice in the **Federal Register** in accordance with the Paperwork Reduction Act of 1995.

**DATES:** Interested persons are invited to submit comments on or before December 26, 2025.

**ADDRESSES:** DOT invites interested persons to submit comments identified by Docket No. DOT–OST–2025–1921 through one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions on the site. This website provides the ability to type short comments directly into the comment field or attach a file for lengthier comments. If there are difficulties submitting comments, see further information contact below.
- *Fax:* 1–202–493–2251.
- *Mail or Hand Delivery:* Docket Operations, U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building, Room W12–140, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except on Federal holidays.

*Instructions:* All items submitted must cite the OMB control numbers (see abstracts below).

**Note:** Comments received generally will be posted without change to *https://www.regulations.gov,* including any personal and/or business confidential information provided.

**FOR FURTHER INFORMATION CONTACT:** LaWanda Morton-Chunn, Procurement Analyst, Office of the Secretary, 1200 New Jersey Avenue SE, Washington, DC 20590, telephone: (202) 366–2267 or *lawanda.morton-chunn@dot.gov.*

**SUPPLEMENTARY INFORMATION:** DOT invites comments on: (1) whether the proposed collection of information is necessary for the proper performance of the functions of DOT acquisitions, including whether the information will have practical utility; (2) the accuracy of the estimate of the burden of the proposed information collection; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the information collection on respondents, including the use of automated collection techniques or other forms of information technology. OMB has approved this information collection for use through December 31, 2025. DOT proposes that OMB extend its approval for use for three additional years beyond the current expiration date.

**Need for Extension**

As a result of the Revolutionary Federal Acquisition Regulation (FAR) (RFO) Initiative, the Transportation Acquisition Regulation (TAR) is also under review. The TAR must align with on-going interim class deviations to the FAR issued by DOT, as well as a later planned FAR proposed rule to be published in the **Federal Register** by the

FAR Council for public comment in 2026. As a part of its review, DOT will consider revising and removing content where needed, adding agency-level statutory requirements, as required, and revising subpart and section numbering in each TAR part to align with new FAR parts. To implement this initiative and to comply with Executive Order 14275 of April 15, 2025, ''Restoring Common Sense to Federal Procurement,'' and OMB Memorandum M–25–26, ''Overhauling the Federal Acquisition Regulation,'' May 2, 2025, DOT is conducting a concurrent rigorous review of the TAR to streamline and update coverage, where appropriate or to remove content to internal agency procedures. DOT anticipates there may be substantive revisions to the TAR, revisions to current Code of Federal Regulations (CFR) solicitation provisions and contract clauses under Title 48, CFR chapter 12 (the TAR), part 1252. This may include potential reductions in information collection requirements and burden under this approved OMB control number. This review and update will be worked by OSPE in conjunction with the Office of Information Technology after appropriate benchmarking and analysis of statutory and other requirements.

DOT requires an extension of the current information collection requirements currently in the TAR at 48 CFR chapter 12 until this analysis is completed, and a proposed TAR rule is developed and published in the **Federal Register** for public comment, anticipated later in 2026.

The summary below describes the ICRs that DOT will submit for OMB clearance as the PRA requires:

*OMB Control Number:* 2105–0578.

*Title:* Department of Transportation Acquisition Regulation (TAR) Part 1239 Clauses.

*Associated Form(s) TAR part 1252 (TAR 1239-related) clauses:* 1252.239–76; 1252–239–77; 1252–239–80; 1252–239–83; 1252–239–85; and 1252–239–88.

*Type of Review:* Renewal of previously approved information collection.

*Background:* Form (Clause) Title(s): Cloud Computing Services, Data Jurisdiction, Audit Record Retention for Cloud Service Providers, Incident Reporting Timeframes, Personnel Screening—Background Investigations, Security Alerts, Advisories, and Directives.

*Respondents:* General Public.

*Average Number of Respondents:* 534.

*Average Number of Responses:* 534.

*Frequency:* Annually.

*Minutes Required/per Response:* 90.

*Total Burden Imposed (Hours):* 339.

*OMB Control Number:* 2105–0579.

*Title:* Department of Transportation Acquisition Regulation (TAR) Part 1239 Clause.

*Associated Form(s) TAR part 1252 (TAR 1239-related) clause:* 1252.239–75.

*Type of Review:* Renewal of previously approved information collection.

*Background:* DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements

*Respondents:* General Public.

*Average Number of Respondents:* 311.

*Average Number of Responses:* 622.

*Frequency:* Annually.

*Minutes Required/per Response:* 60.

*Total Burden Imposed (Hours):* 622.

*OMB Control Number:* 2105–0580.

*Title:* Department of Transportation Acquisition Regulation (TAR) Part 1239 Clauses.

*Associated Form(s) TAR part 1252 (TAR 1239-related) clauses:* 1252.239–89 and 1252.239–90.

*Type of Review:* Renewal of previously approved information collection.

*Background:* Technology Modernization and Technology Upgrades/Refreshment.

*Respondents:* General Public.

*Average Number of Respondents:* 366.

*Average Number of Responses:* 366.

*Frequency:* Annually.

*Minutes Required/per Response:* 90.

*Total Burden Imposed (Hours):* 550.

*OMB Control Number:* 2105–0581.

*Title:* Department of Transportation Acquisition Regulation (TAR) Part 1239 Clauses.

*Associated Form(s) TAR part 1252 (TAR 1239-related) clause:* 1252.239–70.

*Type of Review:* Renewal of previously approved information collection.

*Background:* Security Requirements for Unclassified Information Technology Resources.

*Respondents:* General Public.

*Average Number of Respondents:* 844.

*Average Number of Responses:* 844.

*Frequency:* Annually.

*Minutes Required/per Response:* 30.

*Total Burden Imposed (Hours):* 422.

*OMB Control Number:* 2105–0582.

*Title:* Department of Transportation Acquisition Regulation (TAR) Part 1239 Clauses.

*Associated Form(s) TAR part 1252 (TAR 1239-related) clauses:* 1252.239–72 and 1252.239–74.

*Type of Review:* Renewal of previously approved information collection.

*Background:* Compliance with Safeguarding DOT Sensitive Data Controls and Safeguarding DOT Sensitive Data and Cyber Incident Reporting.

*Respondents:* General Public.

*Average Number of Respondents:* 145.

*Average Number of Responses:* 145.

*Frequency:* Annually.

*Minutes Required/per Response:* 30.

*Total Burden Imposed (Hours):* 73.

*Authority:* The Paperwork Reduction Act of 1995; 44 U.S.C. Chapter 35, as amended; and 49 CFR 1.48.

**Karyn Gorman,**

*Chief Privacy Officer, Office of the Secretary.*

[FR Doc. 2025–19662 Filed 10–24–25; 8:45 am]

**BILLING CODE 4910–9X–P**

## UNIFIED CARRIER REGISTRATION PLAN

### Sunshine Act Meetings

**TIME AND DATE:** October 30, 2025, 10:00 a.m. to 1:00 p.m., EDT.

**PLACE:** The meeting will be accessible via conference call and via Zoom Meeting and Screenshare. Any interested person may call (i) 1–929–205–6099 (US Toll) or 1–669–900–6833 (US Toll), Meeting ID: 994 7596 5095, to listen and participate in this meeting. The website to participate via Zoom Meeting and Screenshare is *https://kellen.zoom.us/meeting/register/r01rkz6zS4OEO48aZH9dpg.*

**STATUS:** This meeting will be open to the public.

**MATTERS TO BE CONSIDERED:** The Unified Carrier Registration Plan Board of Directors (the ''Board'') will continue its work in developing and implementing the Unified Carrier Registration Plan and Agreement. The subject matter of this meeting will include:

**Proposed Agenda**

**I. Welcome and Call to Order—UCR Board Chair**

The UCR Board Chair will welcome attendees, call the meeting to order, call roll for the Board, confirm the presence of a quorum, and facilitate self-introductions.

**II. Verification of Publication of Meeting Notice—UCR Executive Director**

The UCR Executive Director will verify publication of the meeting notice on the UCR website and distribution to the UCR contact list via email, followed by subsequent publication of the notice in the **Federal Register**.

**III. Review and Approval of Board Agenda—UCR Board Chair**

*For Discussion and Possible Board Action*

The proposed Agenda will be reviewed. The Board will consider action to adopt.

Ground Rules

➢ Board actions taken only in designated areas on the agenda.

**IV. Approval of Minutes of the August 7, 2025, UCR Board Meeting—UCR Board Chair**

*For Discussion and Possible Board Action*

Draft Minutes from the August 7, 2025, UCR Board meeting will be reviewed. The Board will consider action to approve.

**V. Approval of Minutes of the September 4, 2025, UCR Board Meeting—UCR Board Chair**

*For Discussion and Possible Board Action*

Draft Minutes from the September 4, 2025, UCR Board meeting will be reviewed. The Board will consider action to approve.

**VI. Report of FMCSA—FMCSA Representative**

The Federal Motor Carrier Safety Administration (FMCSA) will provide a report on any relevant agency activity.

**VII. Presentation of Proposed Contract With DSL Transportation Services, Inc.—UCR Board Chair and Executive Director**

The UCR Board Chair and Executive Director will present a proposed 1-year renewal of the contract between the UCR Plan and DSL Transportation Services, Inc. No action is asked from the UCR Board at this meeting.

**VIII. Subcommittee Reports**

*Audit Subcommittee—UCR Audit Subcommittee*

No report.

*Dispute Resolution Subcommittee—UCR Dispute Resolution Subcommittee Chair*

No report.

*Education and Training Subcommittee—UCR Education and Training Subcommittee Chair*

The UCR Education and Training Subcommittee Chair will provide an update on key projects and initiatives, including the ongoing development of the learning management program and training modules, awareness and engagement efforts for various stakeholders, and the optimization of the website and newsletter.

*Enforcement Subcommittee—UCR Enforcement Subcommittee Chair*

The UCR Enforcement Subcommittee Chair will provide an update on current and planned initiatives, including efforts to enhance UCR enforcement efficiency, and recognition of states and inspectors.

*Finance Subcommittee—UCR Finance Subcommittee Chair and UCR Depository Manager*

A. 2027 Registration Fee Update—UCR Finance Subcommittee Chair

The UCR Finance Subcommittee Chair and Executive Director will provide an update on the 2027 registration fee recommendation.

B. Revenues From 2024, 2025, and 2026 Registration Fees—UCR Depository Manager

The UCR Depository Manager will review the revenues received from the 2024, 2025, and 2026, UCR Plan years' registration fees.

C. 2024 External Financial Audit Update—UCR Finance Subcommittee Chair and UCR Depository Manager

The UCR Finance Subcommittee Chair and UCR Depository Manager will provide an update on the UCR Plan's 2024 External Financial Audit.

D. 2026 Administrative Fund Budget—UCR Finance Subcommittee Chair and UCR Depository Manager

For Discussion and Possible Board Action

The UCR Finance Subcommittee Chair and UCR Depository Manager will discuss the proposed 2026 administrative fund budget as approved by the UCR Plan Finance Subcommittee. The UCR Board may take action to approve a 2026 administrative fund budget.

E. Management Report—UCR Finance Subcommittee Chair and UCR Depository Manager

The UCR Finance Subcommittee Chair and UCR Depository Manager will provide an update on UCR finances and related topics.

*Industry Advisory Subcommittee—UCR Industry Advisory Subcommittee Chair*

No report.

**IX. Contractor Reports—UCR Board Chair**

*UCR Executive Director Update*

The UCR Executive Director will provide a report covering his recent activity for the UCR Plan.

*UCR Administrator Update (Kellen)*

The UCR Chief of Staff will provide a management update covering any additional activity for the Depository, Operations, and Communications.

*DSL Transportation Services, Inc.*

DSL Transportation Services, Inc. will report on the latest data from the FARs program, Tier 5 and 6 unregistered motor carriers, and other matters.

*Seikosoft*

Seikosoft will provide an update on its recent/new activity related to the UCR's National Registration System.

**X. Chief Legal Officer Report—UCR Chief Legal Officer**

The UCR Chief Legal Officer will provide a report covering the status of several legal issues involving the UCR Plan.

**XI. Other Business—UCR Board Chair**

The UCR Board Chair will call for any other business, old or new, from the floor.

**XII. Adjournment—UCR Board Chair**

The UCR Board Chair will adjourn the meeting.

The agenda will be available no later than 5:00 p.m. Eastern daylight time, October 22, 2025, at: *https://plan.ucr.gov.*

**CONTACT PERSON FOR MORE INFORMATION:** Elizabeth Leaman, Chair, Unified Carrier Registration Plan Board of Directors, (617) 305–3783, *eleaman@board.ucr.gov.*

**Alex B. Leath,**

*Chief Legal Officer, Unified Carrier Registration Plan.*

[FR Doc. 2025–19667 Filed 10–23–25; 4:15 pm]

**BILLING CODE 4910–YL–P**

# FEDERAL REGISTER

Vol. 90 Monday,
No. 205 October 27, 2025

Part II

## Department of Homeland Security

8 CFR Parts 215 and 235

Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States; Final Rule

## DEPARTMENT OF HOMELAND SECURITY

### 8 CFR Parts 215 and 235

**[Docket No. USCBP–2025–0033; CBP Dec. 25–06]**

**RIN 1651–AB12**

## Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States

**AGENCY:** U.S. Customs and Border Protection, DHS.

**ACTION:** Final rule with request for comments.

**SUMMARY:** This final rule amends Department of Homeland Security (DHS) regulations to provide that DHS may require all aliens to be photographed when entering or exiting the United States, and may require non-exempt aliens to provide other biometrics. The final rule also amends the regulations to remove the references to pilot programs and the port limitation to permit collection of biometrics from aliens departing from airports, land ports, seaports, or any other authorized point of departure. In addition, DHS is requesting comments on the specific collection process as well as costs and benefits for new transportation modalities.

**DATES:**

*Effective Date:* This rule is effective on December 26, 2025.

*Submission of public comments:* Comments must be submitted on or before November 26, 2025.

**ADDRESSES:** You may submit comments regarding the specific collection process as well as costs and benefits for the newly implemented transportation modalities (the Simplified Arrival process at air entry, sea entry processes, and the process for entry for pedestrians at land) to the Federal eRulemaking Portal: *https://www.regulations.gov.* Follow the instructions for sending comments.

*Instructions:* All submissions received must include the agency name and docket number USCBP–2020–0062 or RIN number 1651–AB12. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided. For detailed instructions on submitting comments, see the ''Public Participation'' heading of the **SUPPLEMENTARY INFORMATION** section of this document.

*Docket:* For access to the docket to read background documents or comments received, go to *http://www.regulations.gov.*

**FOR FURTHER INFORMATION CONTACT:** Larry Panetta, Director, Biometrics Program Office, Office of Field Operations, U.S. Customs and Border Protection, by phone at (202) 344–1253 or via email at *larry.a.panetta@cbp.dhs.gov.*

**SUPPLEMENTARY INFORMATION:**

### Table of Contents

I. Public Participation
II. Executive Summary
A. Notice of Proposed Rulemaking
B. Background and Purpose of the Rule
C. Costs, Cost Savings, and Benefits
III. Background
A. National Security and Immigration Benefits of a Biometric Entry-Exit Program
B. Facial Comparison-Based Entry-Exit Process Pursuant to This Final Rule
1. Benefits of a Facial Comparison-Based Process
2. Facial Comparison Technology Gallery Building
3. General Collection Process
4. Facial Comparison-Based Entry Process
5. Facial Comparison-Based Exit Process
6. Alternative Procedures and Public Notice
7. No Match Procedures
8. U.S. Nationals, Dual Nationals and Lawful Permanent Residents
9. Business Requirements for Public-Private Partnerships
IV. Summary of Changes to the Biometric Entry and Exit Regulations
A. General Biometric Exit Requirement for Aliens
B. Collection of Photographs From Aliens Upon Entry and Departure
C. Collection of Biometrics When Departing the United States and Other Minor Conforming and Editorial Changes
V. Discussion of Comments Submitted in Response to the NPRM
A. Overview
B. Discussion of Comments
1. Comments Expressing General Support
2. Comments Expressing General Support With Recommendations
3. Comments Expressing General Inquiries
4. Comments Expressing General Opposition
VI. Statutory and Regulatory Requirements
A. Executive Orders 12866, 13563, and 14192
B. Regulatory Flexibility Act
C. Unfunded Mandates Reform Act of 1995
D. Paperwork Reduction Act
E. Privacy
F. National Environmental Policy Act

### Table of Abbreviations and Acronyms

ADIS—Arrival and Departure Information System
APA—Administrative Procedure Act
APIS—Advance Passenger Information System
CBP—U.S. Customs and Border Protection
DHS—Department of Homeland Security
DHS DPIAC—DHS Data Privacy and Integrity Advisory Committee
DHS TRIP—DHS Traveler Redress Inquiry Program
DHS FIPPS—DHS Fair Information Practice Principles
DOT—Department of Transportation
FBD—Facial Biometric Debarkation
FIS area—Federal Inspection Service area
FOIA—Freedom of Information Act
FY—Fiscal Year
GAO—Government Accountability Office
HART—Homeland Advanced Recognition Technology
IDENT—Automated Biometric Identification System
INA—Immigration and Nationality Act
LPR—lawful permanent resident
NARA—National Archives and Records Administration
NIST—National Institute of Standards and Technology
NPRM—Notice of Proposed Rulemaking
OBIM—Office of Biometric Identity Management
OMB—Office of Management and Budget
PIA—Privacy Impact Assessment
PII—personally identifiable information
PCLOB—Privacy and Civil Liberties Oversight Board
RFA—Regulatory Flexibility Analysis
SORN—System of Records Notice
S&T—Science and Technology
TSA—Transportation Security Administration
TVS—Traveler Verification Service
USCIS—United States Citizenship and Immigration Services
VWP—Visa Waiver Program

## I. Public Participation

Interested persons are invited to participate in this rulemaking by submitting written data, views, or arguments on the specific collection process, as well as costs and benefits regarding the newly implemented transportation modalities for facial biometric collection, namely, the Simplified Arrival process at air entry, the sea entry processes, and the process for entry for pedestrians at land ports. Comments that will provide the most assistance will reference a specific portion of the final rule, explain the reason for any recommended change, and include data, information, or authority that supports such recommended change. All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Comments submitted regarding any topic other than the specific collection process and costs and benefits on these newly implemented transportation modalities are out of scope for this final rule and will not be considered.

## II. Executive Summary

### *A. Notice of Proposed Rulemaking*

On November 18, 2020, the Department of Homeland Security

(DHS) published a Notice of Proposed Rulemaking in the **Federal Register** (85 FR 74162) (hereinafter referenced as ''the NPRM'') proposing to amend the DHS regulations with regard to collection of biometrics from aliens entering and exiting the United States.[1] On February 10, 2021, DHS published a notice in the **Federal Register** (86 FR 8878) stating that it was reopening the comment period for an additional 30 days based on comments received during the initial comment period.

DHS received a total of 320 comments in response to the NPRM. The submissions included comments supporting the rule, requesting clarification, providing suggestions for changes, and voicing concerns. After review of the comments, through this final rule, DHS is finalizing the proposed changes in the NPRM without substantive modification.

*B. Background and Purpose of the Rule*

DHS is mandated by statute to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics,[2] of aliens entering and departing the United States.[3] DHS also has broad authority to control alien travel and to inspect aliens under various provisions of the Immigration and Nationality Act of 1952, Public Law 82–414, 66 Stat. 163, as amended (INA), which may include requiring aliens to provide biometrics and other relevant identifying information upon entry to, or departure from, the United States.[4] DHS, through U.S. Customs and Border Protection (CBP), has been collecting biometric data from certain aliens arriving in the United States since 2004.[5] However, currently there is no comprehensive system in place to collect biometrics from aliens departing the country.

Implementing an integrated biometric entry-exit system that compares biometric data of aliens collected upon arrival with biometric data collected upon departure helps address the national security concerns arising from the threat of terrorism, the fraudulent use of legitimate travel documentation, aliens who remain in the United States beyond their period of authorized stay (overstays) or are present in the United States without being admitted or paroled, as well as incorrect or incomplete biographic data for travelers. As recognized by the National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission), combatting terrorism requires a screening system that examines individuals at multiple points within the travel continuum.[6] An integrated biometric entry-exit system provides an accurate way to verify an individual's identity, and, consequently, can improve security and effectively combat attempts by terrorists who use false travel documents to circumvent border checkpoints. An integrated biometric entry-exit system can also be used to biometrically verify that a person who presents a travel document is the true bearer of that document, which will help prevent visa fraud and the fraudulent use of legitimate travel documentation.

Such a system will also allow DHS to confirm more concretely the identity of aliens seeking entry or admission to the United States and to verify their departure from the United States. By having more accurate border crossing records of aliens, DHS can more effectively identify overstays and aliens who are, or were, present in the United States without being admitted or paroled and prevent their potential unlawful reentry into the United States. It will also make it more difficult for imposters to utilize other travelers' credentials. In addition, performing biometric identity verification can help DHS reconcile any errors or incomplete data in a traveler's biographic data.[7] Ultimately, this provides DHS with more reliable information to verify identities and to strengthen its ability to identify criminals and known or suspected terrorists.

DHS has faced a number of logistical and operational challenges in developing and deploying a biometric exit capability. This is, in part, because U.S. ports generally do not have designated and secure exit areas for conducting outbound inspections, recording travelers' departures, or comparing biometric information against arrival data.

As stated in the NPRM, CBP has been testing various options to collect biometrics at entry and departure.[8] The results of these tests and the recent advancement of new technologies, including facial comparison technology, have provided CBP with a model to implement a comprehensive biometric entry-exit solution. Based on these tests, CBP determined that facial comparison technology is currently the best available method for biometric verification, as it is accurate, unobtrusive, and efficient.[9] This technology uses existing advance passenger information along with photographs, which have already been provided by travelers to the U.S. government for the purpose of facilitating international travel, to create galleries of facial image templates to correspond with who is expected to be

[1] The NPRM referred to ''aliens'' as ''noncitizens.'' This final rule uses the statutory term ''alien'' as appropriate.

[2] Biographic data includes information specific to an individual traveler such as name, date of birth, and travel document number, which are data elements stored in that traveler's passport, visa, or lawful permanent resident card. Biometrics refers to forms of identification based on anatomical, physiological, and behavioral characteristics or other physical attributes unique to a person that can be collected, stored, and used to verify the identity of a person, *e.g.,* fingerprints, photographs, iris, DNA, and voice print. *See* Executive Office of the President, National Science and Technology Council, Subcommittee on Biometrics, ''The National Biometrics Challenge,'' September 2011, available at *https://www.bing.com/ck/a?!&&p=e3dc11c7c1aa323eJmltdHM9MTcyOTIwOTYwMCZpZ3VpZD0zYmYzOTY1ZS01ZjU1LTY0YmItMTUzMC04MjJhNWUxYTY1MDQmaW5zaWQ9NTE5OA&ptn=3&ver=2&hsh=3&fclid=3bf3965e-5f55-64bb-1530-822a5e1a6504&psq=the+national+biometrics+challenge+2011&u=a1aHR0cHM6Ly9vYmFtYXdoaXRlaG91c2UuYXJjaGl2ZXMuZ292L3NpdGVzL2RlZmF1bHQvZmlsZXMvbWljcm9zaXRlcy9vc3RwL2Jpb21ldHJpY3NjaGFsbGVuZ2Uy MDExLnBkZg&ntb=1.* (Last visited May 15, 2025.)

[3] Numerous federal statutes require DHS to create an integrated, automated biometric entry and exit system that records the arrival and departure of aliens, compares the biometric data of aliens to verify their identity, and authenticates travel documents presented by such aliens through the comparison of biometrics. These include: section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104–828, 110 Stat. 3009–546, 3009–558; section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106–215, 114 Stat. 337, 338; section 205 of the Visa Waiver Permanent Program Act of 2000, Public Law 106–396, 114 Stat. 1637, 1641; section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107–56, 115 Stat. 272, 353; section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Public Law 107–173, 116 Stat. 543, 552; section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108–458, 118 Stat. 3638, 3817; section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Implementing Recommendations of the 9/11 Commission Act), Public Law 110–53, 121 Stat. 266, 338; and section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Public Law 114–125, 130 Stat. 122, 199 (6 U.S.C. 211(c)(10)).

[4] *See* INA 214, 215(a), 235(a), 262(a), 263(a), 264(c), 287(b) (8 U.S.C. 1184, 1185(a), 1225(a), 1302(a), 1303(a), 1304(c)), 1357(b)).

[5] *See* the NPRM, 85 FR at 74169 for more information.

[6] The 9/11 Commission Report 384–386 (2004), available at *https://9-11commission.gov/report/* (last visited May 15, 2025). *See also* the NPRM, 85 FR at 74107.

[7] *See* the NPRM, 85 FR at 74107 for more information on how biometric identity verification mitigates risks including overstays, unlawful reentry, and other risks.

[8] *See* the NPRM, 85 FR at 74171–74173 for a discussion of these tests.

[9] *See* the NPRM, 85 FR at 74173–74178 for a discussion of the benefits of a biometric entry-exit system based on facial recognition.

arriving in or departing from the United States on a particular flight, voyage, etc. These photographs may be derived from passport applications, visa applications, immigration applications, or interactions with CBP at a prior border inspection. Once the gallery is created based on the advance information, the facial comparison technology compares a template of a live photograph of the traveler to the gallery of facial image templates. Live photographs are taken where there is clear expectation that travelers will need to provide documentary evidence of their identity. If there is a facial image match, the traveler's identity has been verified. In select cases, fingerprints may also need to be collected, but only as required to better establish links to previously collected traveler biometric records.

CBP has fully implemented its facial comparison system in the commercial air environment at entry through a process known as Simplified Arrival. CBP has implemented exit in the air environment primarily through partnerships with airlines at select locations. CBP has also fully implemented facial comparison biometrics at entry in the sea environment through processes known as Facial Biometric Debarkation (FBD), Mobile Primary Face, and Simplified Arrival Sea, and at entry in the pedestrian land environment through a process known as Pedestrian Entry. CBP plans to eventually establish a biometric entry-exit system at all air, sea, and land ports of entry. *See* CBP, Biometrics, *https://www.cbp.gov/travel/biometrics* (last modified April 24, 2025) (last visited May 12, 2025).

As noted above, in this final rule, CBP is seeking comments regarding the specific collection process as well as costs and benefits for these newly implemented transportation modalities (the Simplified Arrival process at air entry, sea entry processes, and the process for entry for pedestrians at land).

CBP estimates that a biometric entry-exit system can be fully implemented at all commercial airports and sea ports for both entry and exit within the next three to five years. CBP plans to continue to work to determine the best option for implementing a comprehensive biometric entry-exit system nationwide, which may include pilot programs to test various options for travelers at exit in the sea and pedestrian land environment as well as for travelers entering and exiting in vehicles at land ports and on private aircraft.[10] The regulatory changes adopted in this rule are necessary to enable CBP to continue its refinements, and implement facial comparison efficiently once the best solution is identified. As explained in the NPRM, prior to implementation of this rule, CBP could only conduct pilot programs at a limited number of air and sea ports of entry and could only collect biometrics from a limited population.

This final rule advances the legal framework for DHS collection and use of biometrics from aliens through a comprehensive biometric entry-exit system by removing the references to pilot programs and the port limitations and requiring facial comparison biometrics from all aliens on entry and exit. *See* 8 CFR 215.8(a) and 235.1(f). Because CBP is still determining the best way to implement biometric entry-exit in certain environments, as listed above, CBP has not included in this rule an analysis of the costs and benefits for those environments that are not yet operational. When CBP moves forward with a large-scale implementation of biometric entry-exit for vehicles at land ports and private aircraft or biometric exit at pedestrian land or sea ports, CBP will publish a notice in the **Federal Register** with information regarding details of implementation and request comments on the newly implemented transportation modalities.

This final rule provides that all aliens may be required to be photographed upon entry and/or departure. Facial comparison technology upon entry and departure makes the process for verifying aliens' identities more efficient and accurate. It enables CBP to match the travelers' biometric photographs with their biographic information. The ability to biometrically verify the identity to confirm the departure of aliens will improve security, comply with federal statutory requirements, and help DHS detect overstays and aliens who are or were present in the United States without being admitted or paroled and prevent their illegal reentry. Having accurate entry and exit records is a fundamental piece of the U.S. immigration system and detecting overstays supports that system. Remaining in the United States beyond the period of authorized stay is unlawful and carries consequences for future visits to the United States. *See* INA 212(a)(9)(B) (8 U.S.C. 1182(a)(9)(B)). Ensuring the travelers' photographs match with their vetted biographic and biometric information also helps CBP prevent document fraud and the use of fraudulent travel documents, or the use of legitimate travel documents by imposters (thereby also assisting in combatting identity theft), and to identify criminals and known or suspected terrorists.

CBP will comply with all legal requirements (*e.g.,* the Privacy Act of 1974, 5 U.S.C. 552a (Privacy Act), section 208 of the E-Government Act of 2002, Public Law 107–347, 116 Stat. 2899, 2921 (44 U.S.C. 3501 note) (E-Government Act), and section 222 of the Homeland Security Act of 2002, Public Law 107–296, 116 Stat. 2135, as amended (Homeland Security Act) (6 U.S.C. 142)) and departmental and government-wide policies that govern the collection, use, maintenance, and disposition of personally identifiable information (PII), including biometrics. As discussed in section III.B.6 of this final rule, U.S. citizens[11] may voluntarily participate in the biometric verification process. To minimize the data collected on U.S. citizens, CBP will not retain photographs of U.S. citizens collected as part of CBP's biometric verification program in CBP databases once CBP verifies that a traveler is a U.S. citizen. Encounter photos of U.S. citizens will be used exclusively for identity verification purposes and any photos of U.S. citizens will be discarded within 12 hours of verification of the individual's identity and citizenship.

### *C. Costs, Cost Savings, and Benefits*

CBP anticipates that during the time period of analysis (2017–2029) this final rule will result in costs, cost savings, and benefits to CBP, approved partners, and travelers. CBP estimates total costs to CBP, outbound air travelers, inbound pedestrian travelers, and approved partners will range between $1.3 billion (in discounted 2024 U.S. dollars) using a three percent discount rate and $993 million (in discounted 2024 U.S. dollars) using a seven percent discount rate. Annualized costs are estimated to be between $122 million using a three percent discount rate and $119 million using a seven percent discount rate. Meanwhile, total cost savings to inbound air and sea travelers, and CBP, will be between $578 million (in discounted 2024 U.S. dollars) using a three percent discount rate and $406 million (in discounted 2024 U.S. dollars) using a seven percent discount rate. Annualized total cost savings are estimated to range between $54 million using a three percent discount rate, to $49 million using a seven percent discount rate. Total net costs from the

[10] Private aircraft are those engaged in non-commercial flights, sometimes referred to as general aviation. *See* section 122.1(h) of title 19 of the Code of Federal Regulations (CFR) (19 CFR 122.1(h)).

[11] For the purposes of opt out and photo retention policies, U.S. non-citizen nationals are treated the same as U.S. citizens.

implementation of this final rule are expected to range between $722 million (in discounted 2024 U.S. dollars) using a three percent discount rate to $587 million (in discounted 2024 U.S. dollars) using a seven percent discount rate. Annualized net costs are estimated to range between $68 million using a three percent discount rate and $70 million using a seven percent discount rate.[12]

Additionally, some travelers may perceive having their photographs taken for facial comparison as a loss of privacy; however, CBP could not quantify these costs. Other cost savings that CBP was unable to monetize were an estimated time savings to vessel carriers from a swifter debarkation process when using Facial Biometric Debarkation, approximately 1.25 hours per vessel arrival. Improving national and homeland security efforts through the application of facial comparison technology during biometric identification of individuals entering and leaving the United States is the primary benefit of this final rule. CBP was unable to quantify these enhanced security benefits. Table 1 below shows CBP's estimates for future annualized costs, costs savings, benefits, and net costs from this final rule using three and seven percent discount rates over the period of analysis (2017–2029).

TABLE 1—ESTIMATED ANNUALIZED COST, COST SAVINGS, BENEFITS (2017–2029)

[Discounted thousands of 2024 U.S. dollars]

| | 3% Discount rate | 7% Discount rate |
|---|---|---|
| **Costs** | | |
| Annualized monetized costs | $122,259 | $118,870. |
| Annualized quantified, but not monetized costs. | None | None. |
| Qualitative (non-quantified) costs | Perceived privacy loss | Perceived privacy loss. |
| **Cost Savings** | | |
| Annualized monetized cost savings | $54,355 | $48,599. |
| Annualized quantified, but not monetized cost savings. | None | None. |
| Qualitative (non-quantified) cost savings. | None | None. |
| **Benefits** | | |
| Annualized monetized benefits | None | None. |
| Annualized quantified, but not monetized benefits. | None | None. |
| Qualitative (non-quantified) benefits | Enhanced National Security and identification of visa overstays. Once fully implemented possible shorter plane turnaround times. | Enhanced National Security and identification of visa overstays. Once fully implemented possible shorter plane turnaround times. |
| Net Costs Annualized | $67,904 | $70,271. |

## III. Background

As discussed above, CBP is responsible for implementing an integrated, automated entry-exit system that matches the biographic data and biometrics of aliens entering and departing the United States. Furthermore, to carry out its mission responsibilities to control the border and to regulate the arrival and departure of both U.S. citizens and aliens, CBP has the authority to confirm the identity of all travelers and verify that they are the authorized bearers of their travel documents. *See* INA 287(b) (8 U.S.C. 1357(b)).

### *A. National Security, Public Safety, and Immigration Benefits of a Biometric Entry-Exit Program*

The primary benefit of a biometric ~~entry-exit sy~~stem is the enhanced security provided by having biometric confirmation of the identification of alien travelers entering and leaving the United States. CBP has a comprehensive automated biographic information-based system that vets and checks aliens entering and departing the United States. Although this information is extremely valuable to CBP in completing its mission, no biographic information-based system, by itself, can definitively verify the identity of persons presenting travel and identity documents. Modern e-passports can make passport fraud more difficult. However, the best tool to combat passport fraud is to utilize the digital photos contained in e-passports to biometrically verify that a person who presents a travel document is the true bearer of that document. CBP's biometric tests using facial comparison technology support this conclusion.[13] DHS expects that the implementation of this rule will greatly enhance DHS's ability to identify more of these imposters.

In addition to the benefits this technology can provide on entry, an integrated system, including biometric exit, is also essential for maintaining the integrity of the U.S. immigration system. Under current statutes and regulations, entering or staying in the United States without official permission from the U.S. government can cause a person to be legally barred from reentry to the United States for a number of years following that person's departure or

[12] In the economic analysis for this final rule, CBP used a 3% and 7% discount rate showing values in discounted 2024 U.S. dollars, for estimated future quantified and monetized costs, costs savings and benefits.

[13] *See* the NPRM, 85 FR at 74167–74169 for more discussion on how e-passports mitigate fraud.

removal.[14] The absence of an effective biometric exit process has enabled aliens who are present in the United States without being admitted or paroled or who overstayed their authorized period of admission (overstays) to evade immigration laws and avoid the time bars associated with unlawful presence. For Fiscal Year (FY) 2022, DHS estimates that about 853,955 aliens who entered by air or sea and were expected to depart that year overstayed their lawful period of admission, or 3.67 percent of aliens arriving by air and sea.[15] Through its deployment of biometric exit pilots, CBP has been able to process and document hundreds of aliens who were present in the United States without being admitted or paroled.[16] Additionally, biometric exit verification can allow CBP to address errors that sometimes appear in an alien's biographic data.

Finally, a comprehensive and integrated biometric entry-exit system serves as an important tool in the fight against global terrorism. Since the 9/11 attacks, the United States remains vulnerable to the threat of global terrorism. Recognizing terrorism as one of the most serious threats to international peace and security and the need to take immediate action to address the evolving threat environment, the United Nations Security Council adopted a resolution on December 21, 2017, calling on member nations to increase aviation security and to develop and implement systems to collect biometric data to properly identify terrorists.[17] The resolution was co-sponsored by 66 countries, including the United States, and passed the Security Council with unanimous support. CBP's biometric exit program will provide another layer of identity verification and another opportunity to stop these individuals from departing without opportunity for further investigation.

CBP has conducted extensive tests of the biometric comparison technology prior to implementation of this final rule. All of those tests support CBP's statements above regarding the efficacy of the congressionally mandated biometric entry-exit process.[18]

### *B. Facial Comparison-Based Entry-Exit Process Pursuant to This Final Rule*

In this final rule, DHS is amending the regulations to provide that all aliens may be required to be photographed upon entry and departure from the United States. *See* 8 CFR 215.8(a), and 235.1(f). Failure to comply with a requirement to be photographed may result in a determination of inadmissibility or a violation of the terms of the alien's status where CBP requires this information to determine identity or other immigration information.[19]

Facial comparison technology will provide DHS a successful foundation for a biometric exit solution, as well as an improved and more streamlined biometric entry process. The following sections discuss CBP's facial comparison-based entry-exit process pursuant to this final rule. This process has been implemented for entry and exit at commercial airports and for entry at sea ports and pedestrian land ports. In this final rule, CBP seeks comments on these newly implemented transportation modalities. CBP will proceed with full implementation of an entry-exit process at all land modalities and for private aircraft, as well as on exit at sea ports, after refining its biometric exit strategies in those environments. Additionally, when CBP moves forward with a large-scale implementation for entry-exit at land ports or for private aircraft or for exit at sea ports, CBP will publish a notice in the **Federal Register** providing information regarding details of implementation in each new environment and request comments on the newly implemented transportation modalities.

Some of the facial comparison-based entry and exit processes described below may already be implemented in limited form at entry or under biometric exit pilot programs. For such existing processes, CBP adheres to all applicable laws and regulations that govern its collection of biometrics. Pursuant to this final rule, CBP may collect and compare facial images under the processes described here from all aliens arriving in and departing from the United States.

#### 1. Benefits of a Facial Comparison-Based Process

CBP has developed a model for implementing a biometric entry-exit solution using facial comparison technology, currently implemented at commercial air entry and exit, pedestrian entry, and sea entry. As fingerprint scans have proven to be an effective law enforcement tool, CBP will continue to capture fingerprints as one of the initial identification biometrics at entry to the United States.[20] However, CBP has determined that facial comparison technology is currently the best available method for biometric verification at entry and exit as it is efficient, accurate, and unobtrusive. CBP may elect not to collect fingerprints for subsequent identity verification (after collecting them during the initial encounter) where CBP has implemented facial comparison.[21] Fingerprint scans can be used for most aliens should facial comparison fail to properly identify the traveler.

The key benefit of using facial comparison for biometric identity verification (as opposed to fingerprints) is its efficiency. The facial comparison process leverages information that all travelers provide to the U.S. government as a condition for international travel. In general, photographs of travelers are readily available to DHS through sources such as previous encounter photos and visa databases, eliminating the need to collect new information and add another layer to the travel process. In addition, a system that matches a traveler's facial biometrics against a limited number of stored photographs, rather than an entire government database of photographs, significantly reduces the amount of time necessary to verify a traveler's identity. As a result,

[14] *See* INA 212(a)(9)(B) and 217(a)(7) (8 U.S.C. 1182(a)(9)(B) and 8 U.S.C. 1187(a)(7)); see also 8 CFR 217.4(a).

[15] DHS, FY 2023 Entry/Exit Overstay Report (2024), *https://www.dhs.gov/sites/default/files/2024-10/24_1011_CBP-Entry-Exit-Overstay-Report-FY23-Data.pdf* (last visited May 15, 2025).

[16] *See generally* Enterprise Management Information System-Enterprise Data Warehouse (internal CBP reporting system); and CBP, DHS/CBP/PIA–034, Privacy Impact Assessment for the Enterprise Management Information System-Enterprise Data Warehouse (EMIS–EDW) Appendix A (2016 and subsequent updates), available at *https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp_emis_edw-appendixd-january2021.pdf* (last visited May 15, 2025).

[17] S.C. Res. 2396 (Dec. 21, 2017), available at *https://www.un.org/securitycouncil/content/sres23962017#:~:text=Decides%20that%20Member%20States%20shall,and%20suspected%20terrorists%2C%20including%20FTFs* (last visited May 15, 2025).

[18] *See* the NPRM, 85 FR at 74171–74173 for more discussion regarding CBP's prior biometric comparison tests and the results of those tests; *see also* CBP, Biometrics, *https://www.cbp.gov/travel/biometrics* (last modified Apr. 16, 2025) (last visited May 1, 2025).

[19] *See* 8 CFR 215.8(b) and 8 CFR 235.1(f)(1)(iv). In the event of technical failures preventing the capture and matching of photographs of travelers at entry or exit, air carriers and CBP officers will be directed to use manual boarding processes until the systems are functional. In this scenario, a biographic travel record will be created for the traveler but a biometric confirmation will not exist. A missing biometric confirmation record based on technology or operational failures is not considered non-compliance with the regulatory requirements.

[20] Note that the U.S. Department of State also collects biometrics from visa applicants and U.S. Citizenship and Immigration Services (USCIS) collects biometrics at other times that may be accessed by CBP as well.

[21] CBP may collect facial images from all aliens entering or exiting pursuant to this rule, and, when requested, aliens must comply with CBP requirements to submit facial biometrics. CBP also has discretion not to collect facial images in certain cases where CBP determines that is appropriate.

CBP is able to verify the identity of arriving or departing travelers with a high degree of efficiency while facilitating travel for the public.

Biometric verification using facial comparison is highly accurate. The National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) Demographic Effects Report (NIST FRVT Demographic Effects Report) shows that facial comparison technology is able to match travelers at a rate of greater than 98 percent.[22] If the system fails to match a traveler, then a manual review of the traveler's document is performed. Although CBP does not intend to cause delay or adverse consequences for the traveler in these situations, CBP is aware that in rare cases, travelers who fail to match are referred to secondary inspection or to a CBP officer for additional inspection, which may delay or hinder travel.

As an added benefit, a biometric entry-exit system based on facial comparison is relatively unobtrusive. It relies on current traveler behaviors and expectations; most travelers are familiar with cameras and do not need to learn how to have a photograph taken. Finally, the biometric capture device can be installed at an airline departure gate without any necessary changes to existing airport infrastructure.

By collecting photographs from all aliens departing the United States, DHS can more effectively verify their identity and confirm their departure. It also helps DHS identify known or suspected terrorists or criminals traveling using someone else's documents before they depart the country. This collection also helps identify visa overstays and aliens who are present in the United States without having been admitted or paroled, and prevent their illegal reentry into the United States, as well as prevent visa fraud and the use of fraudulent travel documents. After confirmation that the traveler is not the true bearer of a presented travel document, the traveler would then be subject to further inspection, first by the airline and also in some circumstances by CBP officers, which may include fingerprinting and/or an interview. Through this additional inspection, CBP will be better able to identify known criminals and other threats to border security.

The collection of photographs from all aliens avoids the need to have different processes at the point of departure for different alien travelers depending on whether they are exempt or not (such as the exemption based on age provided by the regulations prior to the effective date of this final rule). Collecting photographs from all alien travelers aligns with international passport standards, which require a photograph of the traveler on the document regardless of age or visa classification.

DHS has also determined that the collection of photographs from all aliens at entry is necessary, without regard to age, visa classification, or immigration status. Establishing a requirement that all aliens may be photographed without exemption enables DHS to biometrically verify the identity of all alien travelers traveling to and from the United States, thereby helping prevent visa fraud and the fraudulent use of legitimate travel documentation.

Collecting photographs from all aliens at entry also enables CBP to implement a streamlined entry process using facial comparison for all such aliens. For example, under the Simplified Arrival process, CBP primarily uses photographs rather than fingerprints to verify the traveler's identity and retrieve the traveler's biographic information for inspection.[23] Facial comparison technology can perform the function of biometrically verifying an alien traveler's identity much more efficiently than collecting and comparing an individual's fingerprints each time a person enters and exits the United States.[24] The Simplified Arrival process (which applies only to certain in-scope aliens prior to the effective date of this final rule and will thereafter apply to all aliens) utilizes integrated biometric identity verification with the retrieval of a traveler's biographic data from a single capture of a photograph. In doing so, the Simplified Arrival process eliminates the need for CBP to scan a passport or travel document to pull up the traveler's biographic data for inspection because a facial comparison scan performs this same function more quickly. Using facial comparison at entry can eliminate several administrative processes that will ultimately increase the speed at which CBP can inspect travelers arriving in the United States. By eliminating the administrative tasks involved in scanning a travel document or collecting fingerprints, CBP can devote more resources to interviewing an alien traveler to determine the person's admissibility. The increased efficiency benefits travelers by allowing them more time to make airline connections and spend less time waiting in lines to be processed by CBP. The increased efficiency also benefits the travel industry by allowing faster processing of customers which decreases resources required to process customers as well as increasing customer satisfaction.

Pursuant to this rule, DHS may collect photographs from all aliens seeking to enter or exit the United States regardless of their age for the purposes of identity verification. This enables DHS to associate the immigration records created for children to their adult records later, which will help combat the trafficking of children, and screen for criminal history or associations with terrorist or other organizations seeking to violate applicable law throughout a person's lifetime. The exemptions in the current regulations for biometric collection based on the age of the individual (*i.e.,* under 14 and over 79) were based on technological limitations on collecting fingerprints from children and elderly persons, as well as traditional law enforcement policies and other policies, such as not running criminal history background checks on children. These exemptions are not applicable to CBP's facial comparison-based biometric entry-exit program, as the use of biometrics has expanded beyond criminal history background checks and now plays a vital role in identity verification and management, and combatting the trafficking of children. Furthermore, internal CBP studies of biometric facial match accuracy, historical matching data, examination of biometric matching of ages under 14 and over 79, and CBP standard operating procedures associated with these ages no longer support exempting facial biometric collection from these populations. Exemptions based on age will continue to apply to biometrics other than facial images.

Certain privacy advocates have expressed concern over the accuracy of facial matching technology especially as it relates to demographics such as age, race and sex. CBP has conducted extensive testing of facial matching technology and CBP's internal analysis shows that facial comparison technology as used in international traveler screening operations is able to match travelers at a rate of greater than 98 percent. By expanding the scope of individuals subject to facial image collection, more travelers can be successfully matched. This will improve the experience for all segments of the population, including children and the

[22] *See* NIST, NISTIR 8280, FRVT Part 3: Demographic Effects 8, 26 (2019) (NIST FRVT Demographic Effects Report), available at *https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf* (last visited May 15, 2025).

[23] *See* the NPRM, 85 FR at 74173 for more discussion on the Simplified Arrival process.

[24] Note that CBP will continue to collect fingerprints during initial encounters with aliens entering the United States.

elderly.[25] Additionally, removing biometric exemptions for aliens alleviates the need to have multiple processing procedures for aliens, which would be a resource-intensive process. For entry and exit at land ports and for private aircraft as well as for exit at sea ports, CBP plans to continue to refine biometric exit strategies with the ultimate goal of implementing a comprehensive biometric entry-exit system nationwide. The regulatory changes in this final rule support CBP's efforts to regularly conduct a variety of statistical tests to bolster performance thresholds and minimize any possible bias impact on travelers of a certain race, gender, or nationality.

In this final rule, CBP has not analyzed the costs and benefits for implementing a facial comparison-based biometric entry-exit program for vehicles at land ports and private aircraft, or for exit at sea ports and pedestrians at land ports because CBP is still in the process of determining the best way to implement biometric entry-exit within each of these unique environments.

2. Facial Comparison Technology Gallery Building

CBP has developed a matching service for all biometric entry and exit operations that use facial comparison, regardless of the method of entry or exit (*i.e.,* air, land, and sea) known as Traveler Verification Service (TVS). For all biometric matching deployments, TVS relies on biometric templates generated from pre-existing photographs that CBP already maintains, known as a ''gallery.'' These images may include photographs captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, immigration applications, and photographs from other U.S. government encounters. CBP builds galleries of photographs based on where and when a traveler will enter or exit. If CBP has access to Advance Passenger Information System (APIS) manifest information, CBP will build galleries of photographs based on upcoming flight, vessel, or, in some cases, bus arrivals or departures. If CBP does not have access to APIS manifest information, such as for pedestrians or privately owned vehicles at land ports of entry, CBP may build galleries using photographs of aliens that frequently cross for that specific port of entry, taken at that specific port, that become part of a localized photographic gallery. CBP's TVS facial matching service then generates a biometric template for each gallery photograph that is stored in the TVS virtual private cloud for matching when the traveler arrives or departs.

3. General Collection Process

Due to the complexities in logistics and variety of air, land, and sea port designs across the entry and exit environments, CBP will collect photographs of the arriving or departing traveler via several different methods depending on the local port of entry and mode of travel. Generally, when travelers present themselves for entry or exit, they will encounter a camera connected to CBP's cloud-based TVS facial matching service via a secure, encrypted connection. This camera matches live images with existing photo templates from previously submitted passenger travel documents or other photos that CBP possesses (*e.g.,* CBP encounter photos). The camera may be owned by CBP, the airport or air or vessel carrier, another U.S. government agency such as the Transportation Security Administration (TSA), or a foreign commercial partner. Once the camera captures a quality image and the system successfully finds a match among the historical photo templates of all travelers from the gallery associated with that particular manifest or port, the traveler proceeds to inspection for an admissibility determination by a CBP officer or is permitted to depart the United States. When a no match occurs, CBP or the carrier may use an alternative means to verify the traveler's identity, such as use of an alternate biometric modality like fingerprints, or a manual review of the travel document as has been done historically.

4. Facial Comparison-Based Entry Process

Historically, prior to admission of a person to the United States, CBP used a manual process to inspect travel documents, such as passports or visas, to initiate system checks and verify a traveler's identity, travel history, and any law or border enforcement concerns that may require attention. The new primary entry solutions, including Simplified Arrival, FBD, Mobile Primary Face, and Pedestrian Entry, use biometrics to initiate the transaction and system checks, using facial comparison as the primary biometric verification modality. This shift from a biographic, document-based system to a biometric-initiated transaction requires travelers to provide facial photos for identity verification purposes. This enables CBP to more accurately verify identity and citizenship by matching the traveler's photograph with vetted and validated biographic information that is associated with a validated photo. Studies show that humans can benefit in face comparison tasks when assisted by a machine, and vice versa.[26]

At entry, CBP uses CBP-owned cameras, CBP's primary arrival subsystem of TECS (not an acronym), and the TVS facial matching service to capture facial biometric data from travelers seeking to enter the United States. TVS automatically creates a template from the image and uses the template to query against a gallery of known identities, based on the manifests for entering flights and vessels that day. At this time, CBP is not actively using galleries of known travelers in the land vehicle environment. CBP uses gallery matching in some instances at land borders, such as bus manifest processing. The process works the same as in the air and sea environments, but APIS submission is currently voluntary for commercial bus and rail operators. CBP does not receive a manifest for pedestrians crossing the land border on foot or for persons traveling in private vehicles. CBP is conducting technical demonstrations to determine the feasibility of gallery matching in the personal vehicle environment at entry. CBP uses one-to-one matching in environments where no manifest exists, such as pedestrian entry. In those cases, CBP will use facial comparison technology to compare the live image captured at the time of application for entry with the traveler's travel document (*e.g.,* passport) when possible.

5. Facial Comparison-Based Exit Process

CBP is using biometric technologies in voluntary partnerships with other federal agencies and commercial stakeholders. These partnerships enable CBP to more effectively verify the identities of individuals entering and exiting the United States, identify aliens who are violating the terms of their admission, and expedite immediate action when such violations are identified. In some partnership

[25] *See* Nat'l Inst. Standards & Tech. (NIST), NISTIR 8271, Face Recognition Vendor Test (FRVT) Part 2: Identification 9 (2019), available at *https://doi.org/10.6028/NIST.IR.8271* (last visited May 25, 2025).

[26] *See* P. Jonathon Phillips, et al., Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms, 115 PNAS 6171 (2018), *https://www.pnas.org/content/pnas/115/24/6171.full.pdf* (last visited May 15, 2025). *See also* Hamood M. Alenezi & Markus Bindemann, The Effect of Feedback on Face-Matching Accuracy, 27 Applied Cognitive Psych. 735 (2013), *https://onlinelibrary.wiley.com/doi/abs/10.1002/acp.2968* (last visited May 15, 2025); and Matthew C. Fysh & Markus Bindemann, Effects of time pressure and time passage on face-matching accuracy, 4 Royal Soc'y Open Sci. 170249 (2017), *https://royalsocietypublishing.org/doi/full/10.1098/rsos.170249#RSOS170249C16* (last visited May 15, 2025).

arrangements, an airline or airport authority partner uses its own technology and staff to incorporate TVS biometric facial comparison during the boarding process. These stakeholders have to adhere to strict business requirements and the cameras must meet CBP's technical specifications to capture facial images of travelers, prior to use. Each camera is connected to the TVS via a secure, encrypted connection.

During the boarding process, CBP's facial comparison matching service allows CBP to biometrically verify the identity of travelers departing the United States with the assistance of airline or airport partnerships. Once the traveler's photo is captured via a camera at the departure gate, TVS generates a template from the departure photo and uses that template to search the gallery of historical photo templates in the cloud-based gallery. Some airlines now accept CBP's biometric identity verification in lieu of boarding passes as part of a new paperless, self-boarding process. Carriers, pursuant to the APIS regulations, are responsible for comparing the travel document to validate the information provided and ensure that the person presenting the document ''is the person to whom the travel document was issued.'' 19 CFR 122.49a, 122.49b, 122.75a, and 122.75b. The use of TVS provides a more efficient and accurate way to meet this requirement.

Typically, on air exit, CBP is not permanently stationed at the gate. Therefore, CBP currently relies on the review of biographic data (provided via APIS) to determine whether further inspection on departure is warranted and whether an outbound enforcement team should be sent to the gate. With the use of facial comparison technology, outbound enforcement teams are informed immediately when a no match occurs (via notification on a mobile device) and may, in some cases, determine that additional inspection is warranted. The carrier may also notify CBP if additional CBP inspection is needed.

Outbound processing for travelers on commercial sea vessels (*e.g.,* cruise ships) will resemble the air exit process. It is expected that this process will also be based on an APIS traveler manifest, although CBP is still determining the best way to implement this process. CBP may collect biometrics from travelers leaving the United States at land borders, when staffing permits. CBP may consider and examine partnering opportunities in the future in the land environment to enable more complete collection of biometrics at exit at land borders. When CBP moves forward with a large-scale implementation for entry-exit at land ports or for private aircraft or for exit at sea ports, CBP will publish a notice in the **Federal Register** providing information regarding details of implementation in each new environment and request comments on the newly implemented transportation modalities.

6. Alternative Procedures and Public Notices

All U.S. citizens and nationals are subject to inspection upon arrival into and departure from the United States to confirm their identity and citizenship. *See* INA 287(b) (8 U.S.C. 1357(b)). However, where CBP has implemented a biometric verification program, participation by U.S. citizens in the biometric verification process is voluntary. A U.S. citizen traveler who does not wish to have a photograph taken may request an alternative inspection process. U.S. citizens may notify the airline or vessel boarding agent or a CBP officer if they would like to opt out of the facial comparison-based process at the time of boarding or during the entry process and request that an alternative method of validation be employed. The citizen's identity will then be verified manually by CBP or the gate agent examining the travel document. For example, in the event a U.S. citizen elects not to be photographed at airports where CBP is conducting biometric exit verification, an airline gate agent should perform a manual review of the U.S. citizen's passport. Although CBP and carriers make every effort to ensure no delays or adverse consequences result when a U.S. citizen opts out of the biometric collection, CBP is aware that in some cases, U.S. citizens have alleged that they have been referred to secondary inspection or told they would not be able to board because they declined biometrics. Individuals who feel they were unduly delayed and would like further information regarding their travel record may request information about records contained in the CBP systems through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the access provisions of the Privacy Act of 1974 (5 U.S.C. 552a(d)) online at *https://www.dhs.gov/foia-contactinformation.*

CBP strives to be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of PII, as set forth in this rulemaking, the CBP biometrics website regarding CBP's Biometric Privacy Policy, *https://www.cbp.gov/travel/biometrics/biometric-privacy-policy,* the TVS Privacy Impact Assessment (PIA),[27] and the CBP Privacy Office report entitled ''CBP Privacy Evaluation (CPE) of the TVS in support of the CBP Biometric Entry-Exit Program'' (CPE TVS Report).[28] As detailed in the CPE TVS Report, when airlines or airports are partnering with CBP on biometric air exit, the public is informed that the partner is collecting the biometric data in coordination with CBP.[29] CBP provides notice to travelers at the designated ports of entry through both physical and either electronic message boards or electronic signs, as well as verbal announcements in some cases, to inform the public that CBP will be taking photos for identity verification purposes. CBP also provides notice to the public that a U.S. citizen may opt out of having a photo taken and request an alternative procedure. CBP works with carriers, airports, and other port facilities to incorporate appropriate notices and processes into their current business models. Examples of such notices are available on CBP's Biometrics Resources website, *https://www.cbp.gov/travel/biometrics/resources.* CBP is aware that, in some cases, adequate signage and notice may not have been installed or provided. CBP seeks to ensure that all locations place signs and notice regarding biometric collection where appropriate.[30]

Upon request, CBP officers provide individuals with a handout (*i.e.,* ''tear sheet'') with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on the particular collection method, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information.[31] CBP is aware that some locations may not have had adequate information informing travelers of the availability of a tear sheet for more information. CBP is working to make sure all locations collecting biometrics provide this information and have available tear sheets for travelers. Additionally, in the Federal Inspection

[27] *See* DHS/CBP/PIA–056, Privacy Impact Assessment for the Traveler Verification Service (Nov. 14, 2018, as amended) (TVS PIA), available at *https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf* (last visited May 15, 2025).

[28] *See CBP Privacy Evaluation (CPE) of the Traveler Verification Service (TVS) in support of the CBP Biometric Entry-Exit Program* (Aug. 15, 2022), (CPE TVS Report), available at *https://www.cbp.gov/document/foia-record/cpe-traveler-verification-service-final-report* (last visited May 15, 2025); *see also* TVS PIA at 1.

[29] *See* CPE TVS Report at 6.

[30] *See* CPE TVS Report at 6.

[31] *See* CPE TVS Report at 6.

Service area (FIS area), CBP posts signs informing individuals of possible searches, and the purpose for those searches, upon arrival or departure from the United States.[32] Privacy information on the program, such as applicable System of Records Notices (SORNs) and Privacy Impact Assessments (PIAs), are published on the DHS Privacy website, https://www.*dhs.gov/privacy.* CBP will also continue to make program information, such as FAQs, available for the public on CBP's biometrics website at *https://www.cbp.gov/travel/biometrics.*

7. No Match Procedures

CBP has designed the entry and exit inspection process such that, in the event of a mismatch, false match, or no match, CBP or the carrier may use alternative means to verify the traveler's identity and ensure that the traveler is not unduly delayed. If the system fails to match a traveler, then a manual review of the traveler's document should be performed. On entry, the CBP officer may continue to conduct additional screening or request fingerprints (if appropriate) to verify identity. Each inspection booth at entry is equipped with a fingerprint reader. At departure, after the manual review of the travel document (*i.e.,* scanning a boarding pass and checking a traveler's passport), the airline or cruise line may notify CBP's outbound enforcement teams should additional inspection be required.[33] If the CBP inspection yields no derogatory information, the CBP officer allows the traveler to board/continue travel. If CBP finds actionable derogatory information on the traveler during the additional inspection, the CBP officer may escort the traveler to the FIS area to conduct further questioning and take the appropriate actions under CBP's law enforcement authorities. CBP is aware that in some cases, travelers have been improperly delayed or experienced other adverse consequences due to a mismatch. In the event that an individual does experience a delay or issue as an outcome of these processes, travelers may contact the CBP Information Center and/or DHS Traveler Redress Inquiry Program (TRIP).[34] Signage and tear sheets at select ports of entry where the TVS is employed provide information on how to contact the CBP Information Center and/or DHS TRIP. In addition, travelers may request information from the on-site CBP officer or gate agent.

8. U.S. Nationals, Dual Nationals and Lawful Permanent Residents

Under the INA, a U.S. national is either a citizen of the United States, or a person who, though not a U.S. citizen, owes permanent allegiance to the United States. *See* INA 101(a)(22) (8 U.S.C. 1101(a)(22)). Alien U.S. national status applies only to individuals who were born either in American Samoa or on Swains Island to parents who are not citizens of the United States.[35] Dual nationals are individuals who owe allegiance to both the United States and a foreign country. They are required to obey the laws of both countries, and either country has the right to enforce its laws. For purposes of international travel, U.S. nationals, including dual nationals, must use a U.S. passport (or alternative documentation as required by 22 CFR part 53) to enter and leave the United States. *See* INA 215(b) (8 U.S.C. 1185(b)); 22 CFR 53.1. In cases where dual nationals fail to present the proper travel documents, biometrics may be used to identify that the same individual has traveled using documents issued by different countries.

For purposes of this rule, a U.S. national or dual national who presents as a citizen of another country will be processed as a foreign national and the individual's photo will be retained accordingly, unless the individual is able to present evidence of U.S. citizenship or nationality.[36] Under immigration law, lawful permanent residents (LPRs) are aliens authorized to live permanently within the United States.[37] As such, for purposes of this rule, LPRs will be processed as aliens.

9. Business Requirements for Public-Private Partnerships

The business requirements implemented by CBP with its partners govern the retention and use of the facial images collected using CBP's facial comparison technology. The Business Requirements Documents are available on CBP's biometrics website at *https://www.cbp.gov/travel/biometrics/biometric-privacy-policy* and are also discussed in the TVS PIA.[38] The CBP Business Requirements prohibit CBP's approved partners such as airlines, airport authorities, or cruise lines and participating organizations (*e.g.,* vendors, systems integrators, or other third parties) from retaining the photos they collect under this process for their own business purposes.[39] The partners must immediately purge the images following transmittal to CBP, and the partner must allow CBP to audit compliance with this requirement. To use TVS, private sector partners must agree to these Business Requirements.[40]

## IV. Summary of Changes to the Biometric Entry and Exit Regulations

To advance the legal framework for the full implementation of a biometric exit capability as described above, DHS is amending the regulations in parts 215 and 235 of title 8 of the Code of Federal Regulations (8 CFR parts 215 and 235) that set forth the requirements for providing biometrics upon entry and departure as described below.

### *A. General Biometric Exit Requirement for Aliens*

Prior to the effective date of this final rule, the regulations at 8 CFR 215.8(a)(1) authorize DHS to collect biometric exit information from certain aliens on departure from the United States pursuant to pilot programs at air, land, or sea ports of entry and places a limit of 15 air or sea ports of entry at which

[32] *See* CPE TVS Report at 6–7.

[33] Communication between CBP's outbound enforcement team and airlines/cruise lines is not unique to locations where facial comparison is implemented. During the outbound inspection, CBP may interview the traveler as well as use Biometric Exit-Mobile (BE-Mobile) devices. CBP conducts outbound enforcement operations using BE-Mobile devices in all modes of transportation and also at locations where facial comparison technology (*i.e.,* biometric exit boarding) is unavailable. Neither the operations nor the technology is exclusive to locations where facial comparison-based biometric exit is implemented.

[34] *See* CBP, CBP Information Center, *https://help.cbp.gov/s/?language=en_US* (last visited May 15, 2025); DHS, DHS Traveler Redress Inquiry Program (DHS TRIP), *https://www.dhs.gov/dhs-trip* (last visited May 15, 2025).

[35] *See* U.S. Department of State, Dual Nationality, *https://travel.state.gov/content/travel/en/legal/travel-legal-considerations/Relinquishing-US-Nationality/Dual-Nationality.html* (last visited May 15, 2025).

[36] A person claiming U.S. citizenship or nationality must establish that fact to the examining officer's satisfaction and must present a U.S. passport or alternative documentation as required by 22 CFR part 53. If such person fails to satisfy the examining immigration officer that the traveler is a U.S. citizen, the person shall thereafter be inspected as an alien applicant for admission. 8 CFR 235.1(b).

[37] Under section 101(a) of the INA (8 U.S.C. 1101(a)), the term ''alien'' means any person who is not a citizen or national of the United States. *See also* 8 CFR 215.1(a). Therefore, a lawful permanent resident is an alien under the INA.

[38] TVS PIA at 10, 17–18, 21–22.

[39] CBP, Biometric Air Exit Business Requirements, v3.0 at 10 (2023), *https://www.cbp.gov/sites/default/files/assets/documents/2023-Oct/Biometric%20Air%20Exit%20Business%20Requirements5.pdf* (CBP Biometric Air Exit Business Requirements); and CBP, Biometric Sea Entry-Exit Business Requirements, v2.0 at 10 (2023), *https://www.cbp.gov/sites/default/files/assets/documents/2023-Oct/Sea%20Business%20Requirements%20Document10_0.pdf* (CBP Biometric Sea Entry-Exit Business Requirements).

[40] CBP Biometric Air Exit Business Requirements 8; CBP Biometric Sea Entry-Exit Business Requirements 8.

such biometric exit pilots may be established. The reference to pilot programs and the 15 air or sea port limitation hinder DHS's ability to expand and fully implement a comprehensive biometric exit solution. Therefore, DHS is amending 8 CFR 215.8 by removing the reference to pilot programs and the reference to 15 air or sea port limit, allowing DHS to establish a general biometric exit requirement for aliens.

*B. Collection of Photographs From Aliens Upon Entry and Departure*

To implement a biometric entry-exit system based on facial comparison, DHS is amending the regulations to provide that all aliens may be required to be photographed upon departure from the United States. Specifically, DHS is amending 8 CFR 215.8 to add a new paragraph (a)(1), which provides that an alien may be required to be photographed when departing the United States to determine identity or for other lawful purposes. The collection of photographs from an alien upon departure will assist DHS in determining the alien's identity and whether immigration status in the United States has been properly maintained. The exemptions of certain aliens from the collection of biometrics provided in 8 CFR 215.8(a)(1) and (2), redesignated as 8 CFR 215.8(a)(2) and (3) and revised by this final rule, will no longer pertain to the collection of photographs from aliens upon departure and will only apply to the collection of other biometrics.

In addition, DHS is amending 8 CFR 235.1(f) to add new paragraph (f)(1)(ii), which provides that an alien seeking admission may be required to be photographed to determine the alien's identity, admissibility, and whether immigration status in the United States has been properly maintained. Like the collection of photographs upon departure, the exemptions provided in 8 CFR 235.1(f)(1)(ii), redesignated as 8 CFR 235.1(f)(1)(iii) and revised by this final rule, will no longer pertain to the collection of photographs from aliens seeking admission and will only apply to the collection of other biometrics.

As noted above, DHS is retaining the exemptions in 8 CFR 215.8 and 235.1(f)[41] for the collection of biometrics other than photographs (*e.g.,* fingerprints and other biometrics) from aliens upon entry to and departure from the United States. This is set forth in redesignated 8 CFR 215.8(a)(2) and (3) and 235.1(f)(1)(iii) and (vi) as amended by this final rule. Notwithstanding these exemptions, DHS is authorized to collect biometrics from aliens, regardless of age, citizenship, or visa status, for law enforcement purposes or in other contexts not addressed by these regulations, such as from aliens attempting to enter the United States illegally between U.S. ports of entry.

*C. Collection of Biometrics When Departing the United States and Other Minor Conforming and Editorial Changes*

DHS is amending 8 CFR 215.8(a) to expand where the collection of biometrics may be required. Prior to the effective date of this final rule, 8 CFR 215.8(a)(1) provided that biometrics may be collected from aliens only when departing ''the United States from a designated port of entry.'' As described above, this final rule adds new paragraph 8 CFR 215.8(a)(1) and redesignates 8 CFR 215.8(a)(1) as 8 CFR 215.8(a)(2). Both new paragraph 8 CFR 215.8(a)(1) and redesignated paragraph 8 CFR 215.8(a)(2) now provide that biometrics may be collected from aliens ''when departing the United States'' from any location. This amendment is necessary to allow for the collection of biometrics from individuals upon departure at locations other than from a designated port of entry.[42] Although the majority of travelers depart the United States from a designated port of entry, a few travelers depart the country from locations that are not designated as ports of entry, including airports such as Ronald Reagan Washington National Airport[43] as well as other locations such as pleasure boat docks that are not designated ports of entry. To ensure the implementation of a biometric entry-exit system that tracks all individuals departing the United States, DHS may require aliens to provide biometrics upon departure from designated ports of entry or from any other location.

In addition, DHS is making certain minor conforming and editorial changes in 8 CFR 215.8 and 235.1(f). In 8 CFR 215.8, DHS is redesignating paragraphs (a)(1) and (2) as paragraphs (a)(2) and (3), and revising cross-references and adding paragraph headings as necessary. In § 235.1(f), DHS is redesignating paragraphs (f)(1)(ii), (iii), and (iv) as paragraphs (f)(1)(iii), (v), and (vi), respectively; adding new paragraphs (f)(1)(ii) and (iv); and revising cross-references and adding paragraph headings as necessary. In both §§ 215.8 and 235.1(f), DHS is removing the phrase ''[t]he Secretary of Homeland Security or his or her designee'' and adding in its place ''DHS'', and removing the phrase ''biometric identifiers'' and adding in its place ''biometrics.''

Finally, DHS is amending 8 CFR 215.8(a) and 235.1(f) to remove the specific references to fingerprints and photographs. Prior to the effective date of this final rule, 8 CFR 215.8(a)(1) and 235.1(f)(1)(ii) provided that any alien may be required ''to provide fingerprints, photograph(s) or other specified biometric identifiers'' upon arrival into or departure from the United States. Because this final rule adds new paragraphs relating to the provision of photographs, the word ''photograph(s)'' in these provisions is no longer appropriate. Furthermore, to allow the flexibility for DHS to employ different methods of biometric collection in the future as biometric technology advances, DHS is amending 8 CFR 215.8(a) and 235.1(f) to provide instead that any alien, other than those exempt by regulation, may be required ''to provide other biometrics'' upon arrival into and departure from the United States. *See* 8 CFR 215.8(a)(2) and 235.1(f)(1)(iii). For example, CBP has tested iris technology, and there may be other biometric options that may have potential for implementation in the future.

## V. Discussion of Comments Submitted in Response to the NPRM

*A. Overview*

In response to the NPRM, DHS received 320 comments during the two

[41] The following categories of aliens will remain exempt from the requirements under 8 CFR 215.8 and 235.1 to provide other (non-photograph) biometrics upon arrival to, and departure from, the United States at a U.S. port of entry: Canadian citizens under section 101(a)(15)(B) of the INA who are not otherwise required to present a visa or be issued a form I–94 or Form I–95; aliens younger than 14 or older than 79 on the date of admission; aliens admitted on A–1, A–2, C–3 (except for attendants, servants, or personal employees of accredited officials), G–1, G–2, G–3, G–4, NATO–1, NATO–2, NATO–3, NATO–4, NATO–5, or NATO–6 visas, and certain Taiwan officials who hold E–1 visas and members of their immediate families who hold E–1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to these requirements; classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or an individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply. *See* 8 CFR 215.8(a)(1) and (2); and 8 CFR 235.1(f)(1)(ii) and (iv).

[42] Designated ports of entry are listed in 8 CFR 100.4(a) for aliens arriving by vessel or by land transportation and in 8 CFR 100.4(b) for aliens arriving by aircraft.

[43] This airport is not a port of entry pursuant to 8 CFR 100.4(b) and does not have federal inspection processes or facilities, but it still has a few flights that depart to international locations, mostly those that have CBP preclearance facilities (typically in Canada or the Caribbean).

30 day public comment periods. Commenters consisted of individuals, advocacy groups, legal service providers, professional associations, State and local governments, and social organizations. The comments and responses are grouped by subject area. Some commenters expressed support for the rule and/or offered suggestions for improvement. The majority of commenters expressed general opposition to the rule, mentioning immigration policy concerns, general privacy concerns, and economic concerns.

*B. Discussion of Comments*

1. Comments Expressing General Support

*Comment:* Several commenters generally supported the proposed rule, providing various rationales or supporting data. Commenters noted that biometrics will streamline the travel process, address national security concerns, provide U.S. citizens with the opportunity to request alternative screening procedures and protect children from being exploited by human traffickers.

*Response:* DHS appreciates the support for the rule and agrees that the rule will streamline the travel process and address various national security concerns to include terrorism and nonimmigrants who overstay their authorized period of admission. Furthermore, DHS agrees that the rule preserves the ability for U.S. citizens to request alternative procedures for identity verification. DHS also agrees that this rule will protect youth and children from being exploited by human traffickers; please see the response in Section V.B.4.l., *Under 14 Children: Privacy, Authority and Accuracy Concerns,* below for additional details regarding the benefits of collecting biometrics from children under the age of 14.

2. Comments Expressing General Support With Recommendations

*Comment:* Some commenters expressed support for the rule and offered suggestions for improvement. Commenters supported CBP's efforts to maintain the ability for U.S. citizens to request alternative screening procedures and applauded CBP's efforts to institute privacy protections for all travelers. Commenters noted that an expanded system-wide biometric implementation will not only facilitate travel to include a more hygienic user experience, but also address national security concerns arising from fraudulent documents and those individuals that overstay their authorized period of admission. Several commenters supported DHS's decision to withdraw the 2008 NPRM [44] which proposed to require commercial air and vessel carriers to collect biometric information from certain aliens departing the United States and submit this information to DHS within a certain timeframe.

*Response:* DHS appreciates the support for the rule that provides for continued implementation of the statutorily mandated biometric entry-exit system. DHS also appreciates support for the withdrawal of the 2008 NPRM. DHS agrees that this final rule will streamline the travel process and address various national security concerns to include fraudulent documents and aliens who overstay their authorized period of admission. Furthermore, DHS agrees that the rule preserves the ability for U.S. citizens to request alternative procedures.

*a. Recommendation: Provide additional information for both the traveling public and stakeholders regarding U.S. citizens' voluntary participation in the program.*

*Comment:* Commenters suggested that to instill greater public confidence in the program, CBP should further clarify the option for U.S. citizens to opt out of the program and establish a rule dictating that U.S. citizens' photos may only be kept for up to 12 hours.

*Response:* DHS agrees that U.S. citizens should have proper notification of their option to opt-out of facial comparison. This issue is further discussed in Section V.B.4.e., *U.S. Citizen Opt-Out,* below, including a discussion regarding CBP's authorities, signage/notification, alternative procedures, and training efforts. CBP agrees that the appropriate retention period for U.S. citizen photos should be no more than 12 hours. The National Archives and Records Administration (NARA)-approved records schedule requires destruction of U.S. citizen photos upon confirmation of U.S. citizenship and no later than 12 hours after confirmation of U.S, citizenship CBP worked closely with the NARA to approve the retention period for U.S. citizen photos.[45]

*Comment:* One commenter suggested that both U.S. citizens and aliens should be required to have their photo taken upon arrival/departure.

*Response:* CBP initially considered including U.S. citizens in its biometric entry-exit program because having separate processes for aliens and U.S. citizens at ports of entry creates logistical and operational challenges that affect security, wait times, and the traveler experience. However, CBP determined that the best course of action at this time is to continue to allow U.S. citizens to voluntarily participate in the biometric entry-exit program. CBP does not have plans at this time to require U.S. citizens to be photographed when entering or exiting the United States, as evidenced by DHS's withdrawal of the 2008 NPRM proposing to require biometric collection from U.S. citizens. *See* Withdrawal Notice (85 FR 73644).

Nevertheless, to carry out its responsibilities effectively under the INA, for both arrivals and departures from the United States, CBP must be able to determine conclusively whether a traveler is a U.S. citizen or national or an alien by verifying that the traveler is the true bearer of the presented travel documentation. CBP is authorized to take and consider evidence concerning the privilege of any person to enter, reenter, pass through, or reside in the United States, or concerning any matter material or relevant to the enforcement or administration of the INA. *See* INA 287(b) (8 U.S.C. 1357(b)). A person claiming U.S. citizenship must establish that fact to the examining officer's satisfaction and must present a U.S. passport or alternative documentation. *See* INA 215(b) (8 U.S.C. 1185(b)), 8 CFR 235.1(b), and 22 CFR 53.1.

*b. Recommendation: Increase program transparency to address concerns from privacy advocates and members of Congress.*

*Comment:* Commenters suggested that CBP should provide the public with additional information about the biometric entry-exit program such as data usage, retention, protection, and dissemination, as well as continually update Privacy Impact Assessments and SORNs as biometric technology capabilities and methodologies continue to evolve.

*Response:* CBP endeavors to provide notice to the public continuously regarding the biometric entry-exit program including through regular updates of its PIAs and SORNs as well as the CBP biometric website at *https://www.cbp.gov/travel/biometrics.* See Section V.B.4.d., *Public Notification and Information,* below, for more information on CBP's transparency and communication efforts. See Section V.B.3.c., *Data Security, Retention, and Dissemination Concerns,* below, for

[44] 73 FR 22065 (Apr. 24, 2008).

[45] *See* DHS, CBP, U.S. Citizen Encounter Photos (DAA–0568–2019–0002), available at: *https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0568/daa-0568-2019-0002_sf115.pdf* (last visited May 15, 2025).

more information regarding CBP's data usage, storage, and protection. Additional information is also available in various places on the CBP and DHS websites including *https://www.cbp.gov/travel/biometrics* and *https://www.dhs.gov/privacy,* which provide the relevant PIA and SORN, and which are all updated regularly as capabilities and technologies evolve; and *https://www.dhs.gov/compliance,* which includes information on compliance including periodic reviews of Privacy Threshold Analyses (PTAs), PIAs, and SORNs.

*Comment:* One commenter suggested that CBP work to make sure travelers understand and adjust to the new system in advance of making biometric collection fully mandatory.

*Response:* As mentioned in the NPRM, [46] through the CBP biometrics website at *https://www.cbp.gov/travel/biometrics,* and the TVS PIA,[47] CBP strives to be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of PII. CBP has also gradually rolled out the biometric entry-exit program with various voluntary pilots over the past several years giving the public the opportunity to adjust to this new process. As discussed throughout this final rule, CBP is still in the process of determining the best way to fully implement biometric collection at all entry and exit modalities. CBP has maintained a proactive approach to stakeholder engagement and outreach through participation in speaking engagements, conferences, and stakeholder meetings. This outreach has kept CBP on the forefront of domestic and international engagement by allowing CBP the opportunity to partner with airlines, airport authorities, travel associations and agents, embassies, attachés, and privacy advocacy groups to share programmatic updates on CBP's use of biometric facial comparison technology in the air, land, and sea environments.

CBP also participates regularly in events sponsored by travel industry partners to provide updates which highlight the benefits of biometric facial comparison technology. Some of these partners have included but are not limited to the U.S. Travel Association (USTA), Global Business Travel Association (GBTA), Cruise Line Industry Association (CLIA), American Association of Airport Executives (AAAE), and Airlines for America (A4A), to name just a few. Moreover, to maximize messaging efforts, CBP has often participated in these events in collaboration with its government partners, like TSA or the Science and Technology Directorate (S&T) of DHS.

*Comment:* Commenters also suggested that CBP set a minimum acceptable accuracy rate consistent across demographics, which, along with system improvements, should then be studied and publicized regularly. One commenter encouraged CBP to expedite the implementation of the 2020 U.S. Government Accountability Office (GAO) audit.[48]

*Response:* CBP appreciates the commenters' suggestions regarding tracking accuracy rates and effectiveness of improvements to the matching algorithm. CBP does have a minimum acceptable accuracy rate for the program and does regularly track it to ensure program success. CBP's Biometric Air Exit Key Performance Parameters (KPPs) mandate that the system's True Acceptance Rate (TAR) must equal or exceed 97 percent of all in-scope travelers (as previously defined by 8 CFR 215.8 and 235.1) and that the system's False Acceptance Rate (FAR) must not exceed 0.1 percent of all in-scope travelers. Through congressionally mandated reports, such as the annual DHS Entry/Exit Overstay Report [49] the TSA and CBP: Deployment of Biometric Technologies Report to Congress,[50] and other public reports, such as the annual CBP Trade and Travel Report,[51] CBP discusses the accuracy rates of the Biometric Entry-Exit program as well as system improvements. Additionally, CBP continues to collaborate with DHS S&T, DHS Office of Biometric Identity Management (OBIM), and the National Institute of Standards and Technology (NIST) on technical standards and evaluation to ensure optimal system performance.

CBP concurred with the 2020 GAO audit recommendations and has addressed each recommendation, as indicated in the Recommendations for Executive Action Table on the applicable GAO website.[52]

*c. Recommendation: Provide additional information regarding no match and opt-out procedures.*

*Comment:* Several commenters requested that CBP clarify its process for when a traveler screening yields a no-match result, to include when CBP assistance should be requested. One commenter also requested the number of Biometric Exit-Mobile devices CBP currently has in use today, as they will likely be used for both no-match and opt-out procedures. Additionally, one commenter indicated that CBP should be responsible for the implications of a no-match result.

*Response:* As discussed in the NPRM, in the event of no match at departure, the carrier or CBP officer will perform a manual review of the travel document (*i.e.,* scanning a boarding pass and checking a traveler's passport).[53] If additional inspection is required by a carrier, the carrier line may notify CBP's outbound enforcement teams, but the carrier is not required to do so. Carrier partners should follow internal business rules and policy to manually verify identity and determine boarding status of a traveler. Air carrier and airport partners may contact CBP, in accordance with existing guidelines outlined by the Carrier Liaison Program, when there are issues or concerns with U.S. entry requirements, human trafficking, traveler assessment, fraudulent document detection and imposter identification.[54]

CBP may use mobile devices with the relevant CBP-built mobile applications to support its multilayered enforcement approach. These CBP applications include the Biometric Exit Mobile application. Additional information about the Biometric Exit Mobile application can be found in the Biometric Exit Mobile Program PIA.[55] CBP officers can use the application on any CBP smartphone. CBP does not

[46] *See* the NPRM, 85 FR at 74177 for more information on CBP's protection of PII.

[47] *See* TVS PIA at 19.

[48] *See* GAO, GAO–20–568, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues (2020), available at *https://www.gao.gov/products/gao-20-568* (last visited May 15, 2025).

[49] This report is available for FY22 at *https://www.dhs.gov/sites/default/files/2023-07/23_0707_FY22_FY23_CBP_Integrated_Entry_Exit_Overstay_Report.pdf* and available for previous FYs at *https://www.dhs.gov/publication/entryexit-overstay-report* (last visited May 15, 2025).

[50] This 2019 DHS report is posted in the docket for this rulemaking.

[51] This report is available for FY22 and earlier at *https://www.cbp.gov/document/annual-report/cbp-trade-and-travel-fiscal-year-2022-report* (last visited May 16, 2025).

[52] *See* GAO, GAO–20–568, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues, Recommendations, Recommendations for Executive Action Table, *https://www.gao.gov/products/gao-20-568* (last visited May 15, 2025).

[53] *See* the NPRM, 85 FR at 74177, for further discussion of no match procedures.

[54] CBP, Carrier Information Guide: United States Document Requirements for Travel (2023), available at *https://www.cbp.gov/sites/default/files/assets/documents/2023-Nov/Carrier%20Information%20Guide%20ENGLISH.pdf* (last visited May 15, 2025).

[55] The updated 2018 PIA for DHS/CBP/PIA–026 Biometric Exit Mobile Program, and all prior versions, are available at *https://www.dhs.gov/publication/biometric-exit-mobile-air-test* (last visited May 15, 2025).

dedicate phones to a single mobile application or operation. Rather, officers use these phones to perform various job responsibilities across multiple environments. Ports are provided with enough phones to meet their mobile mission including biometric exit operations. The port will make a determination on how officers will use their phones on a day-by-day basis based on staffing and other law enforcement-related factors.

*Comment:* One commenter expressed concern that CBP will not have the staffing resources to conduct outbound enforcement operations efficiently.

*Response:* CBP has partnered with multiple stakeholders, including airports and airlines, who are assisting with facilitating the collection at departure through the use of CBP's TVS. TVS provides an automated mechanism to verify the identities of travelers. CBP has also partnered with cruise operators in the entry environment and CBP expects these partnerships will also aid in developing a strategy for biometric exit in the sea environment as well. CBP is still determining the best method for using facial biometrics at land exit.

*Comment:* One commenter requested further clarification on the process for families traveling with children, and persons with reduced mobility as experience during the trials has shown that collecting biometric information from these travelers can be difficult and time consuming.

*Response:* Air carriers may use discretion when processing travelers with disabilities and families with children, including conducting manual identity verification using the individual's travel document (document review), as is performed for all flights where biometric processing is not available. Additionally, carriers must abide by existing local, state, and federal laws and regulations regarding processing persons with disabilities.

CBP's biometric entry-exit program does not contradict existing accessibility regulations and processes. In many cases, biometric collection equipment accommodates disabilities; furthermore, it is CBP's policy to afford persons with disabilities an equal opportunity to participate in, or benefit from, CBP-conducted services, programs, and activities and to provide reasonable modifications to its services, programs, and activities to qualified individuals with a disability when necessary to avoid discrimination on the basis of disability.

*d. Recommendation: Clarify the impact that a biometric exit system would have on airport operations and infrastructure requirements for airports and airlines.*

*Comment:* Commenters requested that CBP explain whether the program's implementation would require separate screening lines, separate processes, or notifications for passengers. Additionally, one commenter requested clarification on whether non-U.S. citizens could opt out of the biometric exit process to avoid additional burdens on CBP and/or the carriers during boarding such as separate boarding queues (*i.e.,* one for U.S. citizens and one for aliens).

*Response:* As noted throughout this rule, on the effective date of this final rule, collection of facial biometrics may be required from all aliens entering or exiting the United States, regardless of age, sex, race and nationality. As indicated on privacy signage, also available on CBP's biometrics website, *https://www.cbp.gov/travel/biometrics/resources,* if a traveler is a U.S. citizen and does not wish to have a photograph taken, the traveler may see a gate agent or CBP officer to request alternative procedures for identity verification. The alternative procedures are intended to be similar to the existing processes at entry and exit. See Section V.B.4.e., *U.S. Citizen Opt-Out,* below, for more information regarding CBP's authorities, signage/notification, alternative procedures, and training efforts. CBP will continue its transparency and communication efforts, discussed in detail in Section V.B.4.d., *Public Notification and Information,* below, as it rolls out full implementation of the biometric entry-exit program.

*e. Recommendation: Provide details should airlines/airports choose not to participate in the Biometric Entry-Exit Program.*

*Comment:* Several commenters requested that CBP provide procedures that airlines should follow if they decide not to participate in this voluntary program and that CBP should commit to continue working with those airports that do not participate in the program.

*Response:* Participation in CBP's biometric entry-exit program will remain voluntary for carriers under this final rule. If air carriers or airports do not participate, they will continue conducting manual identity verification. However, CBP may supplement this verification with CBP officers conducting periodic biometric exit operations. CBP uses its Workload Staffing Model to determine the staffing requirements and help make allocation decisions for CBP officers at ports of entry, including airports. CBP will continue to use this data-driven methodology to identify staffing requirements by considering all the activities performed by CBP officers at ports of entry, the volume of those activities, and the levels of effort required to carry them out.

*f. Recommendation: Provide carrier protections through the SAFETY Act.*

*Comment:* Some commenters recommended that DHS provide SAFETY Act [56] legal liability protections for air carriers that participate as partners in CBP's biometric entry-exit program. The commenters stressed the importance of these protections against claims of discrimination in facial comparison technology, as well against any breach of traveler privacy.

*Response:* DHS will not issue a blanket liability protection. Carriers need to work with their technology providers on seeking SAFETY Act certification for biometric technology devices. The SAFETY Act also is designed for anti-terrorism technology certification, not for general privacy or other areas of discrimination concerns. The SAFETY Act offers liability protection to sellers of qualified anti-terrorism technologies to incentivize the development and deployment of anti-terrorism technology solutions. Additional information is available on the DHS S&T SAFETY Act website at *https://www.safetyact.gov/.*

*g. Recommendation: Establish an oversight body on DHS biometric programs.*

*Comment:* One commenter supports the findings and recommendations in the Homeland Security Advisory Council Biometrics Subcommittee 2020 Report,[57] including the establishment of a DHS Biometrics Oversight and Coordination Council.

*Response:* While DHS has not created the specific oversight council as suggested in the 2020 report, numerous oversight processes exist to ensure DHS compliance with civil rights and civil liberties. These processes included congressional hearings, congressionally mandated status update reports and responses to formal congressional inquiries. See Section V.B.4.j., *Government Accountability and Oversight,* below for more information on the various biometric oversight and accountability mechanisms.

[56] Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, Public Law 107–296, 116 Stat. 2135, 2238 (6 U.S.C. 441 *et seq.*).

[57] Homeland Security Advisory Council, Final Report of the Biometrics Subcommittee (2020) (HSAC Biometrics Report), available at *https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf* (last visited May 15, 2025).

*h. Recommendation: Provide more information on the implications of state/local laws and implementation of biometric capabilities in the land and sea environments.*

*Comment:* One commenter requested that CBP provide additional guidance and clarification on the role of the biometric entry-exit program when local laws conflict with CBP's biometric entry-exit strategy. One commenter indicated that further details on process, timing, cost, etc., in the land and sea environments are necessary to ensure traveler confidence and comprehension.

*Response:* CBP is congressionally mandated to implement a Biometric Entry-Exit System and is issuing this regulation to implement such system. The Supremacy Clause of the U.S. Constitution provides that federal laws and treaties are the supreme laws of the land, and it is well established that the power to regulate immigration is exclusively with the federal government. In instances where a state law conflicts with federal immigration laws, the state law must yield. See Section V.4.B.s, *Land and Sea Implementation,* below, for more information on CBP's implementation plan in the land and sea environments.

*i. Recommendation: Further coordinate with NIST to examine existing standards that may unintentionally inhibit CBP's ability to consider other biometric modalities.*

*Comment:* One commenter requested that CBP coordinate with NIST to ascertain gaps that could limit consideration of other biometric modalities—*e.g.,* edge computing platforms, mobile platforms, and cloud-based systems.

*Response:* CBP works closely with DHS S&T, OBIM and NIST on technical standards and system performance regarding facial comparison capabilities as well as remaining informed on the development and evolution of other biometric modalities, especially as it relates to the border security mission.[58]

*j. Recommendation: Implement additional changes to the rule to ensure all aliens arriving to and departing from the United States are thoroughly screened and vetted.*

*Comment:* One commenter requested that CBP remove all age restrictions in 8 CFR 215.8 and 235.1 for all biometric collection regardless of biometric modality and expand biometric collection to include additional biometric modalities (*e.g.,* iris, DNA, voice). Additionally, the commenter requested that DHS finalize both the USCIS and CBP biometrics rules.

*Response:* The NPRM published on September 11, 2020, entitled ''Collection and Use of Biometrics by U.S. Citizenship and Immigration Services,'' 85 FR 56338 (USCIS NPRM), would have implemented the suggested changes if finalized.[59] On May 10, 2021, DHS withdrew the USCIS NPRM. 86 FR 24750. However, since the withdrawal of the NPRM, the President has issued Executive Order No. 14161, *Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats,* 90 FR 8451, (Jan. 30, 2025) (E.O. 14161). E.O. 14161 mandates that DHS protect the American public from ''aliens who intend to commit terrorist attacks, threaten our national security, espouse hateful ideology, or otherwise exploit the immigration laws for malevolent purposes'' and to ''vet and screen to the maximum degree possible all aliens who intend to be admitted, enter, or are already inside the United States.'' Therefore, DHS will consider future efforts to enhance biometric submission to further the goals of this Executive Order.

Through this rulemaking, DHS is removing the age restrictions for photograph collection under 8 CFR 235.1 for aliens seeking admission to the United States, as well as under 8 CFR 215.8 for aliens departing the United States. See Section V.B.4.l, *Under 14 Children: Privacy, Authorities and Accuracy Concerns,* below, for more details.

3. Comments Expressing General Inquiries

a. Rule Impact

*Comment:* Commenters raised questions regarding to whom the rule applies, as well as the purpose and need for the biometric information collected.

*Response:* As stated throughout this rule, on the effective date of this final rule, collection of facial biometrics may be required from all aliens entering or exiting the United States, regardless of age, sex, race and nationality. DHS is mandated by numerous statutes as discussed above[60] to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States. CBP has determined that facial comparison technology is currently the best available method for biometric verification, as it is accurate, unobtrusive, and efficient.

This final rule improves DHS's ability to meaningfully implement a comprehensive biometric entry-exit system and make the process for verifying the identity of aliens more efficient, accurate, and secure by using facial comparison technology. Implementing an integrated biometric entry-exit system that verifies the identity of aliens at arrival and on exit and then uses that information to confirm that the alien has exited as required is essential for addressing the national security concerns arising from the threat of terrorism, combatting the fraudulent use of legitimate travel documentation, and identifying aliens who overstay their authorized period of admission or are present in the United States without being admitted or paroled. An integrated biometric entry-exit system can also fill the gaps left by incorrect or incomplete biographic data for travelers.

b. Technology Usage and Techniques Accuracy and Misidentification

*Comment:* Several commenters raised questions on the training dataset and machine learning models used for facial comparison.

*Response:* The information requested regarding the training dataset and machine learning models CBP uses for facial comparison is proprietary information. CBP works closely with DHS S&T, OBIM and NIST on technical standards and system performance regarding facial comparison capabilities. NIST has conducted in-depth analysis on facial comparison algorithms, which showed that the vendor selected by CBP is capable of delivering algorithms with a high accuracy rate.[61] For more information on NIST's analysis, see Section V.B.4.k, *Accuracy, General Bias, and Misidentification Concerns,* below.

CBP has issued PIAs for many pilots that were testing/developing facial comparison technology. These PIAs include information about how the algorithms are tested to assure accuracy of the facial comparison technology.[62]

[58] *See, e.g.,* DHS/OBIM/PIA–005 Office of Biometric Identity Management (OBIM)-National Institute of Standards of Technology (NIST) Data Transfer 3–5 (2022), available at *https://www.dhs.gov/publication/dhsobimpia-005-office-biometric-identity-management-obim-national-institute-standards* (last visited May 15, 2025).

[60] Two of the relevant statutes are section 110 of the DMIA (8 U.S.C. 1365a) and section 7208 of the IRTPA (8 U.S.C. 1365b). For a more complete list, please refer to Section II.B. of this final rule.

[61] *See* NIST, NISTIR 8280, FRVT Part 3: Demographic Effects 8, 26 (2019) (NIST FRVT Demographic Effects Report), available at *https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf* (last visited May 15, 2025).

[62] *See, e.g.,* DHS/CBP/PIA–025 1:1 Facial Comparison Project, DHS/CBP/PIA–026 Biometric Exit Mobile Air Test, DHS/CBP/PIA–027 Southwest Border Pedestrian Exit Field Test, DHS/CBP/PIA–030 Departure Information Systems Test, and the

Continued

For more information on how CBP ensures high accuracy rates across all demographics see Section V.B.4.k., *Accuracy, General Bias, and Misidentification Concerns,* below.

c. Data Security, Retention, and Dissemination Concerns

*Comment:* Many commenters had questions regarding the safety and protection of sensitive information with use of this technology and linkage to interagency databases. Additionally, one commenter asked whether protection would be provided to the individuals should a breach or cybersecurity incident occur. One commenter asked if CBP could delete the biometric information but retain the record of the entry or exit.

*Response:* Because numerous federal statutes require DHS to create an integrated, automated biometric entry and exit system that records the arrival and departure of aliens, compares the biometric data to verify their identities, and authenticates travel documents, DHS cannot delete personally identifiable data and only retain a record of entry-exit. Furthermore, DHS retains certain records for up to 75 years, which is necessary to support the holding of biometrics of subjects of interest in immigration and border management or law enforcement activities.[63]

When DHS personnel discover a suspected or confirmed privacy incident, there are a series of actions and activities that must occur to appropriately report, investigate, respond, and mitigate the privacy incident. DHS's policy for responding to privacy incidents is established in the DHS Privacy Office, DHS Instruction Guide 047–01–008, Privacy Incident Handling Guidance (2017).[64] Additionally, DHS Privacy Policy Instruction 047–01–006, Privacy Incident Responsibilities and Breach Response Team (2017),[65] provides additional instruction on how DHS and CBP employees should handle and respond to privacy incidents. The Breach Response Team determines the appropriate course of action with respect to any privacy incident investigation, remedy options, resource allocations, risk mitigation, and interagency engagement. DHS and CBP also follow OMB's breach response guidance, including OMB M–17–12 and M–25–04.[66]

For more information on how CBP safeguards sensitive information, see Section V.B.4.g., *Data Security, Retention, and Dissemination Concerns,* below.

4. Comments Expressing General Opposition

a. General Opposition

*Comment:* Some commenters provided general opposition for the proposed rule, with little, non-specific reasoning or justification provided.

*Response:* DHS appreciates the time these commenters took to read the rule, but DHS respectfully disagrees. DHS's intent for this rule is explained in detail in the rule's preamble and throughout the NPRM. DHS is mandated by numerous statutes to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States. Additionally, DHS gave careful consideration to the costs and benefits associated with this regulatory change, as well as considered all of the comments submitted by the public. DHS concludes that after the careful weighing of equities, this rulemaking is necessary as biometrics are simply a more efficient and reliable means of identifying an individual, compared to biographic identifiers.

*Comment:* Some commenters requested that DHS not use the term ''alien'' in the rule.

*Response:* DHS used the term ''noncitizen'' in the NPRM except where quoting directly from statutory or regulatory text that uses the term ''alien.'' However, DHS uses the term ''alien'' in this final rule consistent with the statutory and regulatory text.

*Comment:* Two commenters suggested that DHS should be abolished.

*Response:* Comments suggesting DHS be abolished are outside the scope of this rulemaking. DHS and its homeland security mission are born from the commitment and resolve of Americans across the United States in the wake of the September 11, 2001, attacks. With the enactment of the Homeland Security Act in November 2002, DHS formally came into being as a stand-alone, Cabinet-level department to further coordinate and unify national homeland security efforts, opening its doors on March 1, 2003. As the complex threat environment continues to evolve, DHS will embody the relentless resilience of the American people and continue to ensure a safe, secure, and prosperous homeland.

*Comment:* One commenter expressed concern that the use of technology would cause officers to distance them physically from the subject and/or distance them from personal responsibility for tasks done.

*Response:* CBP's mission is to protect the American people, safeguard our borders, and enhance the nation's economic prosperity. Technology will never replace the skills and capabilities that can only be exhibited by CBP's personnel in identifying and mitigating threats to the nation. In fact, studies[67] have shown that it is the combination of humans, with technology at their disposal, that best serve the CBP mission while simultaneously respecting the rights of all persons. Humans, balanced with technology, are essential to successful execution of these biometric programs.

CBP's investment in technology is designed to empower officers to execute the agency's critical law enforcement mission and alleviate the administrative burden on officers so they are able to focus on enforcement. The use of facial comparison technology saves frontline officers' time in matching travelers to

TVS PIA. These PIAs are available at *https://www.dhs.gov/privacy-documents-us-customs-and-border-protection* (last visited May 16, 2025).

[63] *See* DHS/NPPD/PIA–002, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) 25 (2012) (IDENT PIA), available at *https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system* (last visited May 16, 2025) (note that this website refers to this PIA as ''DHS/OBIM/PIA–001'' due to OBIM renumbering after the DHS National Protection and Programs Directorate (NPPD) became the Cybersecurity and Infrastructure Security Agency within DHS); and DHS/OBIM/PIA–004, Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA (2020) (HART PIA), available at *https://www.dhs.gov/publication/dhsobimpia-004-homeland-advanced-recognition-technology-system-hart-increment-1* (last visited May 16, 2025).

[64] Available at *https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf* (last visited May 16, 2025).

[65] Available at *https://www.dhs.gov/sites/default/files/publications/047-01-006%20Privacy%20Incident%20Responsibilities%20and%20Breach%20Response%20Team%20FINAL%2012-04-17.pdf* (last visited May 16, 2025).

[66] *See* OMB M–17–12, available at *https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf* (last visited July 31, 2025) and OMB 25–04, available at *https://www.whitehouse.gov/wp-content/uploads/2025/01/M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf* (last visited July 31, 2025).

[67] *See* P. Jonathon Phillips, et al., Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms, 115 PNAS 6171 (2018), *https://www.pnas.org/content/pnas/115/24/6171.full.pdf* (last visited May 16, 2025). *See also* Hamood M. Alenezi & Markus Bindemann, The Effect of Feedback on Face-Matching Accuracy, 27 Applied Cognitive Psych. 735 (2013), *https://onlinelibrary.wiley.com/doi/abs/10.1002/acp.2968* (last visited May 16, 2025); and Matthew C. Fysh & Markus Bindemann, Effects of time pressure and time passage on face-matching accuracy, 4 Royal Soc'y Open Sci. 170249 (2017), *https://royalsocietypublishing.org/doi/full/10.1098/rsos.170249#RSOS170249C16* (last visited May 16, 2025).

document photos and capturing fingerprints CBP already has in its holdings, allowing for a focus on threat detection and behavioral indicators that technology cannot identify. CBP's workforce is critical to accomplishing CBP's missions.

b. General Privacy Concerns

*Comment:* Many commenters disagreed with the rule, stating that the proposal is unnecessary, offensive, an invasion of privacy, infringes on freedoms, and would violate the respect, privacy rights, and civil liberties of U.S. citizens, legal immigrants, aliens, victims of domestic violence, other vulnerable parties, and children.

*Response:* DHS disagrees with these comments. DHS recognizes there may be increased sensitivities associated with facial comparison technology. However, DHS complies with all applicable privacy statutes, regulations, and policies. Further, DHS currently includes information about specific privacy protections in the relevant PIAs. The PIAs also direct individuals to the applicable SORNs, which describe the categories of individuals covered by the system, categories of records in the system, legal authority for maintaining the system, purpose of the system, and routine uses of records maintained in the system. All PIAs and SORNs are submitted to the DHS Privacy Office for review and approval by the DHS Chief Privacy Officer.

The privacy compliance documentation process is an iterative process that not only provides transparency into the details of DHS activities, but also shapes those activities by identifying privacy risks as well as mitigations and privacy-enhancing solutions. Privacy is a DHS-wide responsibility, and the DHS Privacy Office works with DHS components, including CBP, to ensure privacy protections are incorporated in the entire lifecycle of DHS projects, programs, and activities. DHS is committed to the fair and equal treatment of all individuals in its screening and vetting activities, ensuring the rights of all people are protected, while taking lawful actions necessary to secure the homeland. In addition to adhering to all relevant statutory and regulatory privacy protections, DHS complies with existing DHS policies, which include the DHS Fair Information Practice Principles (FIPPS) [68] that ensure privacy safeguards are incorporated throughout the information lifecycle. These safeguards also account for administrative, physical, and technical controls to ensure appropriate collection, use, maintenance, and protection of all information, both biometric and biographic, submitted to DHS. Furthermore, DHS complies with protections in 8 U.S.C. 1367 regarding disclosure of information pertaining to beneficiaries of applications for victim-based immigration relief. DHS will continue to adhere to all statutes, regulations, and policies regarding the privacy rights of individuals departing or entering the United States.

*Comment:* Some commenters stated the rule violates the fundamental human rights to privacy, provided specifically in Articles 17 and 26 of the International Covenant on Civil and Political Rights (ICCPR) [69] and Article 12 of the Universal Declaration of Human Rights (UDHR),[70] which the United States has ratified.

*Response:* DHS disagrees with commenters that this rule violates any provisions of international law that are applicable within the United States. The tenets of the rights to privacy expressed under the ICCPR and UDHR are already incorporated into U.S. domestic law via the Privacy Act and through DHS regulations and policy guidance. DHS is committed to fair equal treatment of all individuals and the rule complies with all applicable privacy statutes, regulations, and policies.

*Comment:* Two commenters mentioned the 2020 DHS Office of the Inspector General (OIG) Report on DHS Privacy oversight inefficiencies.

*Response:* CBP is aware of the DHS OIG report on its November 2020 audit, entitled ''DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives'' [71] (Nov. 2020 DHS OIG Report). CBP takes privacy very seriously and is dedicated to protecting the privacy of all travelers. DHS OIG identified three recommendations for the DHS Privacy Office to improve privacy compliance, information sharing access agreements, and privacy training.[72] Two of the recommendations apply to internal record keeping (compliance and training) and the third applies to oversight of information sharing and access agreements.[73] None of those recommendations was specific to this rulemaking. CBP reviews all programs and changes to programs to determine any privacy concerns and mitigate any privacy risks.

c. Privacy Act and Paperwork Reduction Act

*Comment:* Some commenters stated that the proposed rule fails to justify its claimed authority to collect biometrics from U.S. citizens or lawful permanent residents (LPRs) protected by the Privacy Act (5 U.S.C. 552a).

*Response:* DHS respectfully disagrees with the commenters. In the NPRM, DHS explains in great detail its authority to collect biometrics from all aliens, including LPRs.[74] Moreover, DHS is authorized to take and consider evidence concerning the privilege of any person, including U.S. citizens, to enter, reenter, pass through, or reside in the United States, or concerning any matter which is material or relevant to the enforcement of the INA and DHS regulations. *See* INA 287(b) (8 U.S.C. 1357(b)). The Privacy Act does not prevent government agencies from collecting information about U.S. citizens and LPRs when needed for the agency to execute its statutory and regulatory responsibilities, but rather requires that the government follow a process for appropriately protecting information and informing the public about collection and retention of the information. Additionally, as noted here and elsewhere throughout this final rule, U.S. citizens are not required to but can voluntarily participate in the facial biometric process.

DHS acknowledges that the Privacy Act requires that ''each agency that maintains a system of records shall . . . collect information to the *greatest extent practicable* directly from the subject.'' 5 U.S.C. 552a(e)(2) (emphasis added), subject to any exemptions from this provision contained in 5 U.S.C. 552(j) and (k). Nevertheless, as explained in the NPRM, CBP considered and piloted many types of biometrics collections.[75] Using information gleaned from the pilots as well as public feedback, CBP

[68] DHS, The Fair Information Practice Principles, *https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles* (last visited May 16, 2025).

[69] The text of the ICCPR is available on the United Nations Office of the High Commissioner for Human Rights website, *https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights* (last visited May 16, 2025).

[70] The text of the Universal Declaration of Human Rights is available on the United Nations website, *https://www.un.org/en/about-us/universal-declaration-of-human-rights* (last visited May 16, 2025).

[71] DHS OIG, OIG–21–06, DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives (2020), available at *https://www.oig.dhs.gov/sites/default/files/assets/2020-12/OIG-21-06-Nov20.pdf* (last visited May 16, 2025).

[72] Nov. 2020 DHS OIG Report at 17.

[73] Nov. 2020 DHS OIG Report at 17.

[74] *See* the NPRM, 85 FR at 74164, for more information on DHS' authority to collect biometrics from all aliens.

[75] *See* the NPRM, 85 FR at 74171, for more information about CBP's biometrics pilots.

has concluded that partnering with carriers and airports to capture facial images is the most viable large-scale solution as it is highly effective, cost effective, and less disruptive than other possible methods.

*Comment:* One commenter stated that CBP should require airlines and airports to display the Office of Management and Budget (OMB) control number regarding this information collection.

*Response:* The OMB control number, 1651–0138, is listed in the TVS PIA. Furthermore, pursuant to the Paperwork Reduction Act of 1995 (''Paperwork Reduction Act''), CBP displays the OMB control number on signage. *See* 44 U.S.C. 3507. CBP also provides language for signs that are printed and displayed by airlines, airports and other carriers at each location where biometric collection takes place. Additionally, for the convenience of the public, CBP updated its biometrics website regarding CBP's Biometric Privacy Policy, *https://www.cbp.gov/travel/biometrics/biometric-privacy-policy,* to include the OMB control number.

d. Public Notification and Information

*Comment:* Several commenters raised concerns regarding a perceived lack of public information, notification, and awareness for all travelers, including U.S. citizens, with regard to biometric collection pursuant to this rule.

*Response:* CBP strives to be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of PII. Besides this rule, additional information can be found on CBP's website, in the TVS PIA, and in the CPE TVS Report.[76] Where airlines or airports are partnering with CBP on biometric air exit, the public is informed that the partner is collecting the biometric data in coordination with CBP.[77] CBP provides notice to departing travelers at airport departure gates and travelers arriving at ports of entry through message boards or electronic signs, as well as verbal announcements in some cases, to inform the public that CBP or a stakeholder will be taking photos for identity verification purposes.[78] CBP also provides notice to the public regarding opt-out procedures for U.S. citizens.[79] CBP works with airlines, cruise line operators, airports, and other port facilities to incorporate appropriate notices and processes into their current business models.[80] Additionally, signage posted at CBP's FIS area provides information to travelers on search procedures and the purpose for those searches.[81] Upon request, CBP officers provide individuals with a tear sheet with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on CBP's biometric matching process, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information.[82] Current text for signs and tear sheets are also available on CBP's Biometrics Resources website, *https://www.cbp.gov/travel/biometrics/resources.*

Privacy information on the program such as SORNs and PIAs, including the TVS PIA and information on CBP's previous pilots during the development and testing of facial comparison technology, are published on the DHS Privacy website, *https://www.dhs.gov/privacy.* A link to the TVS PIA is provided on CBP's Biometric Privacy Policy website, *https://www.cbp.gov/travel/biometrics/biometric-privacy-policy.* Also available on CBP's Biometric Privacy Policy website is the CPE TVS Report.

In response to the 2020 GAO audit recommendations,[83] and as noted in the Status of Recommendation 1 in the Recommendations for Executive Action Table on the applicable GAO website,[84] CBP launched its updated biometrics website on September 1, 2020 (*https://www.cbp.gov/travel/biometrics*). The purpose of the site is to deliver information to the public and other stakeholder groups. The site provides a user-friendly communication channel for promoting facial comparison technology and biometrics information in a dynamic and interactive manner. As a testament to CBP's commitment to privacy protections, outlined in the DHS FIPPS, the CBP biometrics website includes the current locations using facial comparison technology, as well as information on how to request alternative screening and copies of CBP's privacy signage on display. The information provided, including a link to CBP's TVS PIA, is yet another tool CBP uses to ensure technology sustains and does not erode privacy protections.

Additionally, CBP has briefed the staff of the CBP Information Center to ensure the staff has the latest information to answer questions. CBP will continue to ensure that content is up to date on the CBP biometrics website, as required, and when substantive updates are made, CBP will provide new details to the CBP Information Center.

Furthermore, CBP regularly conducts periodic signage audits that include local CBP personnel to ensure signs are accurate and placed appropriately.[85] It is important to note that, unlike FIS areas, the airport departure areas are not managed by CBP personnel. However, CBP will continue to work with its airline/airport partners to ensure that privacy signage is available, on display, and reflective of current privacy messaging for travelers.

*Comment:* Additionally, some commenters stated that all signage and communication should clearly identify a contact and process for any traveler to file a grievance should the traveler feel that the traveler was improperly or unfairly treated during the biometric collection process.

*Response:* If a traveler believes that CBP actions are the result of the TVS maintaining incorrect or inaccurate information, (*i.e.,* if the TVS finds a mismatch, false match, or no match) inquiries may be directed to CBP Information Center, Office of Public Affairs—MS1345, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue NW, Washington, DC 20229, or online at *https://help.cbp.gov/s/?language=en_US.* Travelers may also contact the DHS Traveler Redress Inquiry Program (DHS TRIP), 6595 Springfield Center Drive TSA–910, Springfield, VA 22150–6901, or online at *https://www.dhs.gov/dhs-trip,* if they have experienced a travel-related screening difficulty, including those they believe may be related to incorrect or inaccurate biometric information retained in their record(s). Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue. Further, an individual may submit a Privacy Act amendment request to have their travel history record amended if they believe there is incorrect or inaccurate information in their record(s). Privacy Act amendment requests may be sent to *privacy.cbp@cbp.dhs.gov.*

[76] *See https://www.cbp.gov/travel/biometrics/biometric-privacy-policy;* TVS PIA at 1; and CPE TVS Report at 1, 5–7.

[77] *See* CPE TVS Report at 6.

[78] *See* CPE TVS Report at 6.

[79] *See* CPE TVS Report at 6.

[80] *See* CPE TVS Report at 6.

[81] *See* CPE TVS Report at 6–7.

[82] *See* CPE TVS Report at 6.

[83] *See* GAO, GAO–20–568, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues (2020), available at *https://www.gao.gov/products/gao-20-568* (last visited May 16, 2025).

[84] *See* GAO, GAO–20–568, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues, Recommendations, Recommendations for Executive Action Table, *https://www.gao.gov/assets/gao-20-568.pdf* (last visited May 16, 2025).

[85] *See* CPE TVS Report at 7.

CBP agrees that it is important to advise the traveling public of appropriate redress mechanisms if a traveler believes that CBP actions are the result of the TVS maintaining incorrect or inaccurate information. Nevertheless, CBP must be mindful of the limited space on the sign itself. Current signage language directs travelers to the CBP biometrics website for more information. The CBP biometrics website includes several additional links to additional resources such as information on the FOIA, the CBP Information Center and a link to the DHS website, *https://www.dhs.gov.* On the DHS website, the public can submit a DHS TRIP complaint as discussed above.

CBP will continue to keep the public informed regarding the use of facial comparison technology as it expands to additional locations.

*Comment:* One commenter requested additional information on exactly who will be targeted for this biometric collection.

*Response:* As discussed throughout this rule, upon the effective date of this final rule, collection of facial biometrics may be required from all aliens entering or exiting the United States, regardless of age, gender, race, or nationality.

*Comment:* One commenter indicated this rule fails to provide individuals with a choice or general awareness on whether travelers' personal information will be used to develop and/or train machines or algorithms.

*Response:* CBP has issued PIAs for many of the pilots that have tested facial comparison technology.[86] Furthermore, the relevant SORNs are clear that DHS/CBP may use biometrics for purposes of testing new technology and identity verification.[87]

*Comment:* Two commenters noted that they had only just heard about this rule and that the previous administration did not want input from the public.

*Response:* DHS respectfully disagrees. In addition to following the legal requirements for providing notice to specifically seek input from the general public in accordance with the Administrative Procedure Act (APA), 5 U.S.C. 553(b), by publishing the proposed rule in the **Federal Register** on November 19, 2020, CBP also issued a press release.[88] In February 2021, in alignment with DHS's transparency efforts, DHS published another notice in the **Federal Register** to allow the public another opportunity to provide comments on the NPRM regarding the expansion of facial biometrics to further secure and streamline the international travel process. 86 FR 8878 (Feb. 10, 2021). Furthermore, CBP issued a separate press release discussing the NPRM and reiterating that the comment period was reopened.[89]

e. U.S. Citizen Opt-Out

*Comment:* A few commenters raised concerns about U.S. citizen options for opting out of using this biometric technology, including training of officers, signage and notification, alternative inspection methods, and authority to collect data.

*Response:* DHS disagrees with these comments. Pursuant to section 287(b) of the INA (8 U.S.C. 1357(b)), all U.S. citizens are subject to inspection upon arrival to and departure from the United States to confirm their identity and citizenship. However, as noted here and elsewhere throughout this final rule, U.S. citizens can voluntarily participate in the facial biometric process. As mentioned on the privacy signage, also available on *https://www.cbp.gov/travel/biometrics,* if a U.S. citizen does not wish to have a photograph taken, the U.S. citizen may see a gate agent or CBP officer to request alternative procedures for identity verification.

The alternative procedures implemented pursuant to this rule are intended to be similar to the existing process at entry today, in which a CBP officer physically examines the traveler's documentation to ensure the bearer is the true owner and scans the document to pull up the traveler's data for inspection. On exit, airline partners would then conduct manual identity verification using the travel document, as is done today with minimal impact to the boarding and exit process. If there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, the airline will contact CBP for additional inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask the traveler questions to validate identity and citizenship. As mentioned above, every effort will be made to not delay or hinder travel; however, as the alternative procedures include a more manual process it may be slower than the automated process using facial comparison technology.

Prior to deploying facial comparison technology to ports of entry, CBP conducts extensive and ongoing officer training, including emphasis on U.S. citizens being able to request to opt-out of having their photo taken and instead proceed through the traditional inspection process consistent with existing requirements for entry into the United States. Additionally, CBP sends reminder memos to the field offices to ensure compliance.

*Comment:* Commenters also raised concerns regarding the possibility of an eventual biometric collection mandate for all U.S. citizens.

*Response:* At this time CBP does not have plans to require U.S. citizens to be photographed when entering or exiting the United States as evidenced by DHS's withdrawal of the 2008 NPRM which would have proposed to require biometrics from U.S. citizens. *See* Withdrawal Notice (85 FR 73644).

f. Disability, Religious and Language Accommodations

*Comment:* A few commenters raised concerns surrounding religious and language accommodations, including the need for alternative processing for travelers with religious affiliations, disabilities, or limited English-language proficiency.

*Response:* CBP treats all international travelers with dignity, respect and professionalism while keeping the highest standards of security. For travelers with religious affiliations and/or disabilities, CBP policy generally allows for alternative processing on a case-by-case basis. These methods include fingerprint scans or requesting additional documents to establish identity and citizenship. On exit, the

[86] *See* DHS/CBP/PIA–025 1:1 Facial Comparison Project, DHS/CBP/PIA–026 Biometric Exit Mobile Air Test, DHS/CBP/PIA–027 Southwest Border Pedestrian Exit Field Test, DHS/CBP/PIA–030 Departure Information Systems Test, and DHS/CBP/PIA–056 Traveler Verification Service. These PIAs are available at *https://www.dhs.gov/privacy-documents-us-customs-and-border-protection* (last visited May 16, 2025).

[87] *See* DHS/CBP–006 Automated Targeting System SORN, 77 FR 30297, 30301–02 (May 22, 2012); and DHS/CBP–007 Border Crossing Information (BCI) SORN, 81 FR 89957, 89960–61 (Dec. 13, 2016). *See also* DHS/ALL–041 External Biometric Records (EBR) SORN, 83 FR 17829, 17831–32 (Apr. 24, 2018); DHS/ALL–043 Enterprise Biometric Administrative Records (EBAR) SORN, 85 FR 14955, 14957 (Mar. 16, 2020); DHS/CBP–011 U.S. Customs and Border Protection TECS SORN, 73 FR 77778, 77780–81 (Dec. 19, 2008); and DHS/CBP–021 Arrival and Departure Information Systems (ADIS) SORN, 80 FR 72081, 72083 (Nov. 18, 2015). These SORNs are available at *https://www.dhs.gov/system-records-notices-sorns* (last visited May 16, 2025).

[88] CBP, National Media Release, CBP Enhances Biometrics for Non-U.S. Travelers Entering and Exiting the United States, Nov. 20, 2020, available at *https://www.cbp.gov/newsroom/national-media-release/cbp-enhances-biometrics-non-us-travelers-entering-and-exiting-united* (last visited May 16, 2025).

[89] CBP, National Media Release, CBP Reopens Comment Period Regarding Enhancements to Biometrics for non-U.S. Citizens Entering, Exiting United States, Feb. 9, 2021, available at *https://www.cbp.gov/newsroom/national-media-release/cbp-reopens-comment-period-regarding-enhancements-biometrics-non-us* (last visited May 16, 2025).

airline gate agent may conduct manual identity verification of travelers by using their travel documents, as is performed for flights where biometric processing is not available, and may notify CBP to conduct further examination, if necessary. For example, if there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, airline partners will contact CBP for additional inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask the traveler questions to validate identity and citizenship.

CBP requires the full face to be viewable. As such, CBP may request that the individual adjust or remove religious headwear to the degree necessary for identification verification. Should religious headwear need to be removed, CBP endeavors to provide as much privacy as possible. During processing, if a traveler requires special consideration due to religion, cultural, or privacy concerns, CBP officers and managers should endeavor to reasonably accommodate the traveler's request.

CBP has long recognized the importance of effective and accurate communication between CBP personnel and the public they serve. Language and communication barriers can negatively affect interactions with the public, provision of services, and law enforcement activities. Ensuring effective communication with all persons facilitates the CBP mission. CBP has a protocol for the use of interpreters and translation services, which is triggered by a request for interpreters or language services.[90] Air carriers and airport authorities may also provide interpreters for travelers, typically through Airport Ambassadors. CBP also utilizes other means of interpretation and translation, including Agency employees certified to provide language services. Additionally, CBP developed an internal smartphone translation application, CBP Translate, to facilitate basic officer-traveler conversations. Privacy information about CBP Translate is provided in DHS/CBP/PIA–069 Privacy Impact Assessment for the CBP Translate Application (2021), available at *https://www.dhs.gov/publication/dhscbppia-069-cbp-translate-application* (last visited May 15, 2025).

*Comment:* One commenter expressed concern over requiring travelers to remove their face masks during the facial comparison process.

*Response:* The Centers for Disease Control and Prevention's Order entitled ''Requirement for Persons To Wear Masks While on Conveyances and at Transportation Hubs'' [91] has expired and most travelers no longer wear masks. However, CBP recognizes that some travelers still choose to wear masks and understands the concerns of those travelers. During both entry and exit, traveler identity must be verified, whether it is by a CBP officer or by a gate agent (on departure). To verify identity, it is necessary to see a person's face, whether it is being viewed by a camera or by a person. An argument can be made that it takes less time for a camera to capture a photo and do a backend comparison than it does for a person to make the same comparison and decide whether or not the faces match. In that case, using facial comparison technology lessens the time a traveler has to be without wearing a mask.

As such, once at the primary inspection booth, CBP requires that all travelers momentarily lower their masks either to conduct the facial comparison match or to visually confirm that the traveler is the true bearer of the travel document. Requiring travelers to briefly remove their masks does not violate any laws. Upon departure, CBP defers to stakeholders, but does request that travelers pull their masks down as much as possible and ensure that no other facial obstructions (*e.g.,* hats or glasses) are present. If CBP officers are present upon departure, CBP will request that travelers pull their masks down. Nevertheless, facial comparison technology continues to improve. For example, a 2020 DHS S&T study showed that systems are often able to correctly identify individuals with masks.[92] CBP will continue to consider alternatives to mask removal using improved technology for those rare cases where travelers are still using masks.

g. Data Security, Retention, and Dissemination Concerns

*Comment:* Several commenters raised concerns surrounding data security, retention, and dissemination to include protecting the biometric data from breaches, cyberattacks, or insider threats, and implementing appropriate safeguards and storage protocols.

*Response:* CBP is committed to protecting all sensitive information in its possession, including mitigating, to the extent possible, the risk of data breaches from information systems containing PII. Privacy is implemented by design. It is ensured in this instance because data protection is built into the design, architecture, and implementation of the biometric technology, ensuring data protection through the architecture and implementation of the biometric technology. As further detailed below, there are four primary safeguards to secure traveler data: secure encryption during data storage and transfer; irreversible biometric templates; brief CBP retention periods; and secure storage.

- *Encryption:* CBP stores TVS information in secure CBP systems and temporarily in a secure virtual cloud environment.[93] CBP uses two-factor authentication and strong encryption to transfer the data between the camera, the TVS cloud matching service, and CBP systems as well as for PII at rest (in storage). Moreover, just as CBP encrypts all biometric data at rest and in transit, CBP requires its approved partners under the TVS partner process to encrypt the data, both at rest and in transit.
- *Templates:* A biometric template is a digital representation of a biometric trait of an individual generated from a biometric image and processed by an algorithm. The template is usually represented as a sequence of characters and numbers.[94] For TVS, the secure biometric templates created from the photos cannot be reverse engineered to recreate a biometric image. The templates generated for the TVS are proprietary to a specific vendor's algorithm and cannot be used with other vendors' algorithms.
- *Retention periods:* The entirety of TVS is in the cloud.[95] For U.S. citizens, the biometric image is destroyed immediately following confirmation of U.S. citizenship, but no later than 12 hours only under specific

[90] *See* CBP, Language Access, *https://www.dhs.gov/publication/language-access-plan-us-customs-and-border-protection* (providing links to the DHS and CBP Language Access Plans) (last visited May 16, 2025).

[91] *See* 86 FR 8025 (Feb. 1, 2021).

[92] DHS S&T, News Release, Airport Screening While Wearing Masks? Facial Recognition Tech Shows up to 96% Accuracy in Recent Test, Jan. 4, 2021, available at *https://www.dhs.gov/science-and-technology/news/2021/01/04/news-release-airport-screening-while-wearing-masks-test* (last visited May 16, 2025); DHS S&T, Demographic Variation in the Performance of Biometric Systems: Insights Gained from Large-Scale Scenario Testing (2021), available at *https://www.dhs.gov/publication/demographic-variation-performance-biometric-systems* (last visited May 16, 2025).

[93] *See* TVS PIA at 26; CPE TVS Report at 15.

[94] *See* TVS PIA at 6, 26; CPE TVS Report at 15–16.

[95] *See* TVS PIA at 6; CPE TVS Report at 15.

circumstances.[96] If there is a system or network issue, photos will reside in an inaccessible queue for up to 12 hours and will be processed once the system and/or network connectivity is re-established and proper dispositioning (confirmation of U.S. citizenship) can occur. For all other travelers, CBP temporarily retains facial images in the internal cloud for no more than 14 days for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. Gallery photos of all air and sea travelers are purged from the TVS external cloud matching service no later than 12 hours after entry or departure. CBP's cloud service provider, using a configurable managed service, automatically deletes the data. Additionally, the data cache is in an encrypted form and the cloud service provider does not have the encryption keys. CBP does not create galleries for the land environment. Photos of aliens who are required to provide a biometric as well as those U.S. citizens who participate in CBP's Global Entry Program, are securely transferred from CBP's cloud service providers to DHS IDENT, and any successor systems.[97] Certain other federal agencies may access IDENT with the approval of DHS, if the purpose of their access is consistent with the applicable SORNs, which are available on the DHS website, *https://www.dhs.gov/system-records-notices-sorns.*[98] DHS retains certain records in IDENT for up to 75 years, which is necessary to support the holding of biometrics of subjects of interest in immigration and border management or law enforcement activities.[99]

- *Access controls:* Only authorized CBP personnel and authorized representatives of approved CBP partners have access to the cameras, and only authorized CBP staff and cloud service provider personnel have access to the cloud database.[100] Although authorized cloud personnel may access the database, they do not have keys to decrypt the data. CBP access controls ensure only authorized access to the facial images. Initial TVS access is not activated for an individual without completion of the CBP Security and Privacy Awareness course.[101] The course presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official information and PII. The course also provides information regarding sharing, access, and other privacy controls. CBP updates this training regularly, and TVS users are required to take the course annually.[102] Furthermore, the cloud service provider selected for this initiative is required to adhere to the security and privacy controls required by NIST Special Publication 800–144, Guidelines on Security and Privacy in Public Cloud Computing (2011) [103] and the DHS Chief Information Officer.

CBP experienced a cybersecurity incident during a biometric pilot in 2019.[104] DHS OIG reviewed the incident to determine whether CBP ensured adequate protection of biometric data during the 2019 pilot.[105] In response to the 2019 cybersecurity incident, CBP has taken and continues to take robust measures to protect information systems containing PII. CBP response actions are detailed in CBP Comments to the Draft Report found in Appendix B to the Sept. 2020 DHS OIG Report regarding the incident.[106]

In addition to the assessment of biometric exit stakeholders, discussed in more detail below, CBP is working with DHS S&T, Office of Test and Evaluation, to develop and execute a cybersecurity test plan that will ensure all required security controls are in place on existing hardware and software. Additionally, CBP has contracted with a third-party vendor to perform an adversarial assessment to identify and mitigate any cyber vulnerabilities.

*Comment:* Several commenters also suggested auditing stakeholders (such as port authorities, air carriers and sea carriers) to ensure compliance.

*Response:* CBP understood the need to build a system that all stakeholders within the travel continuum could participate in without building their own independent systems. To address these challenges and satisfy the Congressional mandate, CBP, as outlined above, is working closely with its partners to integrate biometrics with existing identity verification requirements to the extent feasible. CBP agrees that it needs to ensure that its partners comply with and adhere to DHS and CBP privacy and security policies. To that end, CBP developed Business Requirements Documents, available on CBP's biometrics website at *https://www.cbp.gov/travel/biometrics/biometric-privacy-policy,* which partners sign and return to CBP as acknowledgement by the stakeholder that it agrees to all CBP terms and technical specifications as well as any other requirements as determined by CBP.[107]

These business requirements implemented by CBP with its partners govern the retention and use of the facial images collected using CBP's facial comparison technology. CBP prohibits all approved partners such as airlines, airport authorities, or cruise lines and participating organizations (*e.g.,* vendors, systems integrators, or other third parties) from retaining the photos they collect under this process for their own business purposes.[108] The partners must immediately purge the images following transmittal to CBP, and the partner must allow CBP to audit compliance with this requirement.[109] In order to use TVS, private sector partners must agree to these Business Requirements.[110]

CBP comprehensively assesses compliance with DHS's security and privacy requirements on the part of CBP and CBP's partners. This includes security interviews with partner IT departments, security scans of biometric processing systems, and penetration tests of those systems. CBP has conducted 14 assessments thus far.[111] CBP has not found any instances of stakeholders' retaining photos in violation of the Business Requirements Document.

CBP's cybersecurity resilience efforts, including the assessment of biometric exit stakeholders and adversarial assessment, align with Executive Order 14028, ''Improving the Nation's Cybersecurity,'' 86 FR 26633 (May 17, 2021), which highlights the need to strengthen collaboration between the private sector and the Federal Government.

[96] *See* TVS PIA at 9–10; CPE TVS Report at 11, 16.

[97] *See* TVS PIA at 8–9.

[98] *See* TVS PIA at 22.

[99] *See* TVS PIA at 21.

[100] *See* TVS PIA at 26; CPE TVS Report at 15.

[101] *See* TVS PIA 2 at 7; CPE TVS Report at 15.

[102] *See* CPE TVS Report at 15.

[103] Available at *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf* (last visited May 16, 2025).

[104] *See* DHS OIG, OIG 20–71, Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot 5 (2020) (Sept. 2020 DHS OIG Report), available at *https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf* (last visited May 16, 2025).

[105] Sept. 2020 DHS OIG Report at 5.

[106] Sept. 2020 DHS OIG Report at 22–23.

[107] CBP Biometric Air Exit Business Requirements 8; CBP Biometric Sea Entry-Exit Business Requirements 8.

[108] CBP Biometric Air Exit Business Requirements 10; CBP Biometric Sea Entry-Exit Business Requirements 10.

[109] CBP Biometric Air Exit Business Requirements 10; CBP Biometric Sea Entry-Exit Business Requirements 10.

[110] CBP Biometric Air Exit Business Requirements 8; CBP Biometric Sea Entry-Exit Business Requirements 8.

[111] Information provided by CBP's Biometric Entry-Exit Strategic Transformation Admissibility and Passenger Programs office subject matter expert on January 4, 2024.

Furthermore, CBP is taking steps to promote data minimization and privacy protections by using an airline-generated alphanumeric unique ID (UID) to disassociate the biographic information associated with the new facial images. As CBP verifies the identity of the traveler, either through the automated TVS facial comparison process or manual officer processing, the backend matching service returns the ''match'' or ''no-match'' result, along with the associated unique identifier. There is no additional PII shared with industry partners, which minimizes harm to individuals should cybersecurity incidents occur. A UID is generated by either the travel agent, travel website hosting service, or the airline at the time of the reservation. The UID is comprised of a sequential number (which is only valid for the particular airline and the specific flight), plus the Record Locator, a six-digit code used to access additional information about the traveler.

*Comment:* Several commenters also suggested limiting forward dissemination.

*Response:* DHS discloses information sharing pursuant to the relevant SORNs, under the Privacy Act. As discussed above, these SORNs are available on the DHS website at *https://www.dhs.gov/system-records-notices-sorns.* DHS abides by all applicable confidentiality statutes and regulations that may limit the use and sharing of information about vulnerable populations including those covered by IIRIRA 110 (8 U.S.C. 1367) (Violence Against Women Act, T nonimmigrant visas, and U nonimmigrant visas); INA 244 (8 U.S.C. 1254a(c)(6)) and 8 CFR 244.16 (Temporary Protected Status); INA 245A (8 U.S.C. 1255a(c)(5)(A) and (B), LIFE Act, Pub L. 106–553 § 1104(c)(5) and 8 CFR 245a.2(t); 245a.3(n), and 8 CFR 245a.21) (Legalization under the LIFE Act); INA 210 (8 U.S.C. 1160(b)(6)(A) and (B)), 8 CFR 210.2(e) (Special Agricultural Workers); and 8 CFR 208.6 (Asylum, credible fear, and reasonable fear, and applicable by DHS policy to Refugee information).

Additionally, in accordance with DHS policy, CBP uses the DHS FIPPs [112] to assess the privacy risks and ensure appropriate measures are taken to mitigate risks from data collection through the use of biometrics. DHS applies FIPPS-based protection to ensure that any forward dissemination is for a valid purpose consistent with the purpose for the original collection, is for a limited use consistent with the applicable SORN, and that privacy protections are adhered to. CBP's partnering stakeholders are also held to the same standards. For additional information on how CBP complies with the FIPPS, please see the page 15 of the CPE TVS Report.

DHS prioritizes data protection and security as part of its mission to protect the homeland and is cognizant of the serious impact that unauthorized disclosure of information could create for vulnerable populations. DHS acknowledges that the risk of a data breach is always technically possible, but DHS works tirelessly to minimize those risks and continues to safeguard its information from any unauthorized use. DHS's IDENT already contains controls so that only those individuals whose jobs require knowledge of information retained in IDENT (including facial images as discussed in the response in this section above at the bullet on *Retention Periods*) are able to access that data on a need-to-know basis. In addition, government employees accessing IDENT data must have a valid federal security or suitability clearance. Misuse of the data in IDENT is mitigated by requiring that IDENT users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems. Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity.

Further, external connections must be documented and approved with both parties' signatures in an Interconnection Security Agreement (ISA), which outlines controls in place to protect the confidentiality, integrity, and availability of the information being shared or processed. DHS OBIM is responsible for all PII associated with IDENT, and the Homeland Advanced Recognition Technology System (HART), the successor system to IDENT currently in development, whether the data is held in data centers or in a cloud infrastructure, and therefore imposes strict requirements for safeguarding PII.[113] This includes adherence to the DHS 4300A Sensitive Systems Handbook,[114] which provides implementation criteria for the rigorous requirements mandated by the DHS Information Security Program.

Additionally, DHS OBIM requires contracted cloud service providers to segregate IDENT and HART data from all other third-party data.[115] All contracted cloud service providers must also follow DHS privacy and security policy requirements and must follow the Federal Risk and Authorization Management Program (FedRAMP)'s strict configurations, security assessments, authorizations, and continuous monitoring requirements.

h. Rulemaking Process—Comment Period

*Comment:* Several commenters raised concerns regarding the 30-day comment period and asserted that DHS did not provide sufficient time for public review. One commenter also alleged that DHS's staggered issuance of interrelated rules (referencing the USCIS NPRM) created further difficulties for interested parties as commenters were prevented from determining how the rules interrelate within the comment periods for the related rules.

*Response:* Following the initial 30-day comment period, which closed on December 21, 2020, CBP, in alignment with DHS transparency efforts, and based on the previous comments received, re-opened the comment period for an additional 30 days to provide the public another opportunity to provide comments on the NPRM regarding the expansion of facial biometrics to further secure and streamline the international travel process.[116] The second period was from February 10 to March 12, 2021.[117] The combined comment periods amounted to 60 days. Although section 6(a)(1) of Executive Order 12866 and section 2(b) of Executive Order 13563 recommend as a general matter that agencies provide a minimum comment period of 60 days, the APA does not prescribe a minimum number of days necessary to allow for adequate comment. *See* 5 U.S.C. 553(b). Therefore, in accordance with the APA and the applicable Executive Orders, DHS set a 30-day comment period and further re-opened the comment period for an additional 30 days which reasonably provided the public with a meaningful opportunity to comment. Additionally, CBP notes that the USCIS NPRM has been withdrawn. 86 FR 24750 (May 10, 2021).

[112] DHS, The Fair Information Practice Principles, *https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles* (last visited May 16, 2025).

[113] *See* HART PIA at 38–39.

[114] DHS, DHS 4300A Sensitive Systems Handbook, Version 12.0 (Nov. 15, 2015), available at *https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf* (last visited May 16, 2025).

[115] *See* HART PIA 38.

[116] 86 FR 8878 (Feb. 10, 2021).

[117] 86 FR at 8878.

i. Rulemaking Process—Unauthorized Official and Other DHS Authority Concerns

*Comment:* Several commenters claimed that the rule was promulgated by an unauthorized official making the rule null and void.

*Response:* It is unnecessary to discuss the merits of the appointments because the NPRM only proposed changes to DHS regulations and requested comments. It did not effectuate any change that would amount to a final action taken by DHS.

*Comment:* Some commenters alleged that the rule is a violation of the APA because the administration does not have the authority to issue regulations that go beyond the agency's statutory mandate or that CBP has misinterpreted Congress's directions regarding a biometric entry-exit program. The commenters also alleged that DHS's failure to substantiate a need for biometrics expansion conflicts with the requirements of the APA as the APA prohibits agency actions that are arbitrary, capricious or an abuse of discretion or unsupported by substantial evidence. *See* APA (5 U.S.C. 706(2)).

*Response:* DHS is not exceeding the statutory authorities as they currently exist. In accordance with the APA, DHS explicitly articulated both general and specific statutory authority for biometric collection including photographs, in the NPRM,[118] reiterates that authority in Section III.B. of this final rule, and disagrees with commenters that it does not have authority to promulgate this rulemaking. Additionally, DHS has provided extensive discussion of the need and purpose for this rulemaking pursuant to the APA requirements. For more information on the need for a biometric entry-exit program, see Section II.B. above.

j. Government Accountability and Oversight

*Comment:* Several commenters raised concerns regarding effective oversight activities, and accountability measures. Additionally, some commenters noted the importance of instituting uniform standards across the U.S. Government. One commenter supports the Homeland Security Advisory Council November 2020 findings [119] and recommendations, including the establishment of a DHS Biometrics Oversight and Coordination Council.

*Response:* As the Biometric Entry-Exit Program is a congressionally mandated government program, there are several oversight processes to ensure compliance with civil rights and civil liberties. These processes include congressional hearings, congressionally mandated status update reports and responses to formal congressional inquiries, as well as audits from the GAO and OIG.

CBP participated in two congressional hearings, one in 2019 [120] and in 2020,[121] as well as responded to more than seven congressional inquiries since 2017 regarding CBP's use of facial comparison technology.

Additionally, CBP has published several reports that provide the public with information on how CBP is implementing the Biometrics Entry-Exit Program. For example, in August 2019, DHS provided the U.S. House of Representatives Committee on Homeland Security a comprehensive report on the program that included material on the operational and security benefits of the biometric entry-exit system. CBP and TSA's efforts to address privacy concerns and potential performance differential errors, and a comprehensive description of audits performed.[122]

CBP has addressed the recommendations from two audits, both in 2020, one by GAO and one by DHS OIG. See Sections V.B.2.c and V.B.4.b and d, above. CBP is aware of the DHS OIG report on its September 2023 audit, entitled ''DHS Needs to Update Its Strategy to Better Manage Its Biometric Capability Needs.'' [123] DHS OIG identified four recommendations; two for the Office of Strategy, Policy, and Plans to update and finalize internal DHS strategic plans and a department-wide policy for biometric collection in all transportation modalities and two recommendations for the Undersecretary for Management to update and finalize the DHS biometric implementation plan (roadmap) and for the Executive Steering Committee to continue the working group to develop a transition plan to integrate CBP's biometric entry-exit system with OBIM's HART system. Although none of these recommendations is directly specific to this rulemaking, CBP takes biometric capabilities seriously and is dedicated to work cooperatively with DHS to provide critical input regarding an overall management strategy to acquire and deploy a biometric solution that meets Department needs, particularly regarding integration of CBP's biometric entry-exit system with HART (the successor system to IDENT, as noted elsewhere).

Furthermore, CBP complies with the requirements of the Privacy Act, as well as all DHS and Government-wide policies. In accordance with DHS policy, CBP uses the FIPPs to assess the privacy risks and ensure appropriate measures are taken to mitigate risks from data collection through the use of biometrics. CBP's partnering stakeholders are also held to the same standards. For additional information on how CBP complies with the FIPPS, please see page 15 of the CPE TVS Report.

Also, the business requirements implemented by CBP with its partners govern the retention and use of the facial images collected using CBP's facial comparison technology. The Business Requirements Documents are available on CBP's biometrics website at *https://www.cbp.gov/travel/biometrics/biometric-privacy-policy.* CBP prohibits its approved partners such as airlines, airport authorities, or cruise lines and participating organizations (*e.g.,* vendors, systems integrators, or other third parties) from retaining the photos they collect under this process for their own business purposes.[124] The partners must immediately purge the images following transmittal to CBP, and the partner must allow CBP to audit compliance with this requirement.[125] In order to use TVS, private sector partners must agree to these Business Requirements.[126]

Several DHS Offices and Programs also have oversight of CBP activities. For example, CBP collaborates regularly with the DHS Privacy Office to ensure

[118] *See* the NPRM, 85 FR at 74164 for more information regarding DHS' statutory authority to require biometrics.

[119] *See* HSAC Biometrics Report.

[120] *See About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Hearing Before the H. Comm. on Homeland Sec.,* 116th Cong. (2019) (statement of John P. Wagner, Deputy Exec. Assistant Comm'r, Off. of Field Operations, CBP), available at *https://docs.house.gov/meetings/HM/HM00/20190710/109753/HHRG-116-HM00-Wstate-WagnerJ-20190710.pdf* (last visited May 16, 2025).

[121] *See About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II, Hearing Before the H. Comm. on Homeland Sec.,* 116th Cong. (2020) (statement of John P. Wagner, Deputy Exec. Assistant Comm'r, Off. of Field Operations, CBP), available at *https://docs.house.gov/meetings/HM/HM00/20200206/110460/HHRG-116-HM00-Wstate-WagnerJ-20200206.pdf* (last visited May 16, 2025).

[122] *See* DHS, TSA and CBP: Deployment of Biometric Technologies Report to Congress (2019) is posted in the docket for this rulemaking.

[123] DHS OIG, OIG 23–58, DHS Needs to Update Its Strategy to Better Manage Its Biometric Capability Needs (2023), available at *https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-58-Sep23.pdf* (last visited May 16, 2025).

[124] CBP Biometric Air Exit Business Requirements 10; CBP Biometric Sea Entry-Exit Business Requirements 10.

[125] Id.

[126] CBP Biometric Air Exit Business Requirements 8; CBP Biometric Sea Entry-Exit Business Requirements 8.

compliance with privacy laws and policies. The DHS Privacy Office commissioned the DHS Data Privacy and Integrity Advisory Committee (DPIAC) to advise DHS on best practices for the use of facial comparison technology. The DHS DPIAC published its report on February 26, 2019.[127] CBP has implemented or is actively working to implement all of the DHS DPIAC recommendations.

Additionally, in June 2019, the Privacy and Civil Liberties Oversight Board (PCLOB) started an ongoing oversight project to review the use of facial comparison technology in aviation security, with the goal of informing policymakers and the public about these technologies, their uses, and their implications for security, privacy, and civil liberties.[128] CBP hosted the PCLOB for a tour of biometric processes at Atlanta/Hartsfield International Airport on January 15, 2020.[129]

Furthermore, CBP works closely with DHS S&T, OBIM and NIST on technical standards and system performance. Additionally, CBP is a member of the DHS Biometric Capabilities Executive Steering Committee (BC–ESC), which continues to meet quarterly.[130] The mission of the BC–ESC is to provide effective governance, oversight, coordination, and guidance to all DHS and component-level programs that are developing and/or providing biometric capabilities in support of DHS mission objectives.[131] It serves as a forum for cross-component collaboration and the sharing of biometric challenges, needs, concepts, best practices, plans, and efforts.

Although CBP's Biometric Entry-Exit Program does have sufficient oversight and accountability mechanisms, CBP is committed to transparency in its use of facial comparison technology and welcomes the opportunity to engage with Congress on legislative enhancements and to provide technical assistance, as necessary. CBP will ensure compliance with any new applicable legislation or regulations passed.

*Comment:* One commenter suggested that Congress pass an ethics bill prior to using facial comparison technology. One commenter suggested the United States needed a Cyber Bill of Rights.

*Response:* Comments suggesting Congressional action are outside the scope of this rulemaking. However, CBP will ensure compliance with any and all new applicable legislation passed by Congress.

*Comment:* Several commenters referenced specific abuse or misuse of power concerns. Some commenters mentioned alleged human rights violations committed by CBP and ICE. The commenters were concerned generally with CBP and ICE abuses, including a concern that this rule would open the door for further abuses of power and human rights violations.

*Response:* As documented in the DHS Core Values,[132] DHS employees, including those of CBP, execute the duties and responsibilities entrusted to the agency with highest ethical and professional standards. Each DHS employee has a responsibility to the United States Government and its citizens to place loyalty to the Constitution, laws, and ethical principles above private gain. To ensure that every citizen can have complete confidence in the integrity of the Federal Government, each employee shall respect and adhere to the principles of ethical conduct set forth in the Code of Federal Regulations as well as the implementing standards in supplemental agency regulations. *See* 5 CFR part 2635. Furthermore, CBP officers and agents follow the CBP Standards of Conduct.[133] Section 3.1 of the CBP Standards of Conduct specifically states, ''The conduct of CBP employees must reflect the qualities of integrity and loyalty to the United States; a sense of responsibility for the public trust; courtesy and promptness in dealing with and serving the public; and a standard of personal behavior that reflects positively upon, and will be a credit to, both CBP and its employees.'' [134] Section 7.11.2 further provides, ''Employees will not make abusive, derisive, profane, or harassing statements or gestures, or engage in any other conduct evidencing hatred or invidious prejudice to or about another person or group on account of race, color, religion, national origin, sex, sexual orientation, age, or disability.'' [135] The safety of CBP employees and the public is paramount during CBP operations.

Alleged violations by CBP or ICE officers or agents are outside the scope of this rulemaking.[136]

k. Accuracy, General Bias, and Misidentification Concerns

*Comment:* Several commenters raised concerns regarding the accuracy, reliability, and potential bias of facial comparison technology, particularly its impact on specific demographic groups.

*Response:* DHS is aware of several NIST studies on the use of facial comparison technology and DHS continues to monitor the scientific community studies, particularly those of NIST, on applicability. The NIST FRVT Demographic Effects Report, which used CBP data to reach its conclusions,[137] noted that because different algorithms

[127] DHS DPIAC, Report 2019–01: Privacy Recommendations in Connection with the Use of Facial Recognition Technology (2019), available at *https://www.dhs.gov/sites/default/files/publications/Report%202019-01_Use%20of%20Facial%20Recognition%20Technology_02%2026%202019.pdf* (last visited May 19, 2025).

[128] *See* PCLOB, Press Release, ''From Booking to Baggage Claim:'' PCLOB to Examine Use of Facial Recognition and Other Biometric Technologies in Aviation Security: Board Announces Three New Oversight Projects, June 26, 2019, available at *https://documents.pclob.gov/prod/Documents/EventsAndPress/eb140554-4fc7-4700-88d2-197d7fe45770/New%20projects%20announcement%20June_25_%202019%20Final.pdf* (last visited May 19, 2025); and PCLOB, Current Oversight Projects, *https://www.pclob.gov/OversightProjects* (last visited May 19, 2025).

[129] *See About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II, Hearing Before the H. Comm. on Homeland Sec.,* 116th Cong. (2020) (statement of John P. Wagner, Deputy Exec. Assistant Comm'r, Off. of Field Operations, CBP at 9), available at *https://docs.house.gov/meetings/HM/HM00/20200206/110460/HHRG-116-HM00-Wstate-WagnerJ-20200206.pdf* (last visited May 19, 2025).

[130] *See* HSAC Biometrics Report 23.

[131] *See* HSAC Biometrics Report 23.

[132] DHS, Core Values, *https://www.dhs.gov/core-values* (last visited May 19, 2025).

[133] CBP, Directive 51735–013B, Standards of Conduct (2020), available at *https://www.cbp.gov/sites/default/files/assets/documents/2021-Jan/cbp-standards-conduct-2020_0.pdf* (last visited May 19, 2025).

[134] CBP, Directive 51735–013B, Standards of Conduct 1 (2020), available at *https://www.cbp.gov/sites/default/files/assets/documents/2021-Jan/cbp-standards-conduct-2020_0.pdf* (last visited May 19, 2025).

[135] *Id.* at 11.

[136] Although outside the scope of this rulemaking, DHS notes the launch of the Office of the Immigration Detention Ombudsman (OIDO), a new and independent office within DHS as mandated by Congress. *See* section 106 of the Consolidated Appropriations Act, 2020, Public Law 116–93, 133 Stat. 2317, 2505 (amending section 405 of the Homeland Security Act (6 U.S.C. 205)). OIDO is an independent office within DHS and is not a part of ICE or CBP. OIDO's role is to assist individuals with complaints about the potential violation of immigration detention standards or misconduct by DHS (or contract) personnel; provide independent oversight of immigration detention facilities, including conducting unannounced inspections and reviewing contract terms for immigration detention facilities and services; and serve as an independent office to review and resolve problems stemming from the same. *See* sec. 405(a)–(b) of the Homeland Security Act (6 U.S.C. 205(a)–(b)); DHS, Office of the Immigration Detention Ombudsman, *https://www.dhs.gov/office-immigration-detention-ombudsman* (last visited May 19, 2025).

[137] *See* DHS/OBIM/PIA–005, Privacy Impact Assessment for the Office of Biometric Identity Management (OBIM)—National Institute of Standards of Technology (NIST) Data Transfer 4–5 (2022), available at *https://www.dhs.gov/publication/dhsobimpia-005-office-biometric-identity-management-obim-national-institute-standards* (last visited May 19, 2025). *See also* TVS PIA at 22.

perform better or worse in various circumstances, ''policy makers, face recognition system developers, and end users should be aware of these differences and use them to make decisions and to improve future performance.'' NIST FRVT Demographic Effects Report 3.

To ensure higher accuracy rates, as well as efficient traveler processing, CBP uses high performing cameras, proper lighting, and image quality controls. CBP then compares traveler photos to a very small gallery of high-quality images that those travelers already provided to the U.S. Government to obtain a passport or visa using a high-quality facial comparison algorithm. CBP builds the galleries of photographs based on where and when a traveler will enter or exit. If CBP has access to advance information, CBP will build galleries of photographs based on upcoming flight or vessel arrivals or departures. CBP uses a commercial face comparison algorithm from a developer that participates in the NIST Face Recognition Technology Evaluation (FRTE) 1:N.[138] The NIST Face Recognition Vendor Test (FRVT) Demographic Effects Report, published in 2022, shows a wide range in accuracy across algorithm developers, with the most accurate algorithms producing many fewer errors and undetectable false positive differentials. Since many of the performance rates specified in the report would not be acceptable for use in CBP operations, CBP does not use them. Additionally, NIST noted, ''Some developers supplied identification algorithms for which false positive differentials are undetectable'' (NIST FRVT Demographic Effects Report 8). The most recent NIST FRTE 1:N demonstrates that the face comparison algorithm developer selected by CBP is capable of high performance, ranking within the top five in most categories evaluated, including match performance in galleries that are much bigger than those used by CBP.

The NIST performance metrics described in the NIST FRVT Demographic Effects Report are consistent with CBP operational performance metrics for entry-exit. CBP's operational data continues to show there is no measurable differential performance in matching based on demographic factors. As mentioned in the CBP: Evaluating Possible Bias document included in the docket for this rulemaking, docket number [USCBP–2020–0062], CBP has conducted extensive statistical analysis (chi squared independence tests) to determine whether traveler demographics (age, sex, and nationality) affect facial comparison match rates.[139] CBP does not collect race/ethnicity information, and this information is not included in the APIS manifest. As a result, CBP uses citizenship as a proxy for this data. Using citizenship or country of birth as a proxy for race is consistent with industry standards as evidenced by the NIST FRVT Demographic Effects Report, which notes, ''While country-of-birth information may be a reasonable proxy for race in these countries, it stands as a meaningful factor in its own right particularly for travel-related applications of face recognition.'' NIST FRVT Demographic Effects Report 1–2.

Additionally, CBP continually monitors algorithm performance and technology enhancements. As mentioned in CBP: Evaluating Possible Bias, the performance of CBP's TVS continues to improve over time due to technical, operational, and procedural advancements including threshold adjustments and testing multiple vendors.[140] CBP has enhanced the photo selection process used to build the galleries, which reduces the number of travelers with no photos and improves the accuracy of the system. Additionally, CBP has enhanced the manner in which the galleries are populated, ensuring that the information included in the flight manifest is used to its maximum potential to include more, higher-quality photographs. There have also been software changes to the cameras to allow travelers posing for the photos to receive visual feedback. Furthermore, as CBP continues and expands its usage of TVS, personnel using the technology become more aware of the optimal camera positions to ensure better images and increase the traveler throughput. Some cameras are also now equipped with multiple lenses to capture images for various angles, which may increase photo quality depending on the height of the traveler. These advancements have been instrumental in minimizing occurrences of no matches, mismatches, and false matches.

CBP is also aware of several other tests, studies, and articles on the use of facial comparison technology. While informative, these studies do not evaluate the specific algorithm that CBP is using and as such cannot be used to draw conclusions about CBP's biometric entry-exit program.

*Comment:* Some commenters said that facial comparison technology should not be implemented until it is 100% accurate or until courts have shown that it is as effective as fingerprints for determining validity.

*Response:* DHS disagrees. No system or biometric technology, not even widely used fingerprints, is 100% accurate. In 2004, NIST found that ''the best system was accurate 98.6 percent of the time on single-finger tests, 99.6 percent of the time on two-finger tests, and 99.9 percent of the time for tests involving four or more fingers. These accuracies were obtained for a false positive rate of 0.01 percent.'' [141] NIST conducted another study in 2020 that found contact device match accuracy is generally better than 99.5% when scanning multiple fingers.[142] Fingerprint image quality may be affected by demographic factors. Operationally it is commonly observed that subject age, race, sex, and occupation often contributes to fingerprint image quality. For example, those with dry fingers due to the natural aging process as well as those with finer ridge structure specific to certain demographic groups may have poorer fingerprint match performance. There is also an occupation effect, in that people who work with their hands, such as brick layers, have matching issues. However, there are no detailed analysis reports that show how these image quality effects translate into fingerprint match performance.

Additionally, biographic systems are not 100% accurate either. As mentioned in the preamble, often there are errors or incomplete data. For example, the U.S. government may have the name and date of birth but not the passport number. The use of biographic data alone leads to a very high rate of mismatches, as dozens of people often have the exact same name and date of birth. The use of biometrics solves this problem by effectively and efficiently confirming a traveler's identity. Nevertheless, biometric algorithms

[138] NIST FRVT Demographic Effects Report 1, 8, 26.

[139] CBP, CBP: Evaluating Possible Bias (2020), available at *https://downloads.regulations.gov/USCBP-2020-0062-0003/content.pdf* (last visited May 19, 2025).

[140] CBP, CBP: Evaluating Possible Bias (2020), available at *https://downloads.regulations.gov/USCBP-2020-0062-0003/content.pdf* (last visited May 19, 2025).

[141] NIST, News Release, NIST Study Shows Computerized Fingerprint Matching Is Highly Accurate, July 6, 2004, available at *https://www.nist.gov/news-events/news/2004/07/nist-study-shows-computerized-fingerprint-matching-highly-accurate* (last visited May 19, 2025).

[142] *See* NIST, News Release, NIST Study Measures Performance Accuracy of Contactless Fingerprinting Tech, May 19, 2020, available at *https://www.nist.gov/news-events/news/2020/05/nist-study-measures-performance-accuracy-contactless-fingerprinting-tech* (last visited May 19, 2025).

should be framed against human matchers, not 100% perfect matching, which is an impossibility. When comparing biometric matching to a human manual identity verification process, biometrics is a clear improvement and gets the process significantly closer to 100% than without biometric matching.[143] CBP is unaware of any legal requirement to show that facial comparison is the same as fingerprints for determining validity.

*Comment:* Two commenters expressed concern that facial comparison technology could be susceptible to imposter or spoof attacks.

*Response:* Even as technology advances, CBP is mindful of potential imposter or spoof attacks. CBP mitigates this risk through algorithm enhancements and its biometric approach using the gallery concept. CBP knows whom to expect to be on the flight based on the advance passenger information. Travelers, to include imposters, who are not expected on the flight would not match to the gallery.

Additionally, CBP mitigates spoof and imposter risk by ensuring that those utilizing the technology are appropriately trained to detect these attacks. CBP officers using the technology upon entry have several tools at their disposal, to include facial comparison technology, to identify imposters. Additionally, CBP officers undergo extensive training prior to starting the job, including specific tactics, techniques, and procedures for identifying imposters. For example, CBP has used Eye-dentify, which is an imposter detection training technology.[144] Additionally, CBP's Carrier Liaison Program provides carrier staff with training on U.S. entry requirements, human trafficking, traveler assessment, fraudulent document detection and impostor identification using state-of-the-art document examination material, equipment, and training tools.[145]

*Comment:* Commenters requested additional information regarding CBP's mismatch rate, the outcome of potential misidentification and redress opportunities.

*Response:* As discussed in DHS's TSA and CBP: Deployment of Biometric Technologies Report to Congress, CBP's Biometric Air Exit KPPs mandate that the system's TAR must equal or exceed 97 percent of all in-scope travelers (as previously defined by 8 CFR 215.8 and 235.1) and that the system's FAR must not exceed 0.1 percent of all in-scope travelers.[146] The estimated TAR based on the internal CBP analysis is at least 98% for all travel modes. The estimated FAR based on the internal CBP analysis is 0.02 percent, which is within the established KPP target of less than 0.1 percent. Regarding false non-matches or false negatives, NIST states, ''False negative error rates vary strongly by algorithm, from below 0.5% to above 10%. For the more accurate algorithms, false negative rates are usually low with average demographic differentials being, necessarily, smaller still.'' NIST FRVT Demographic Effects Report 7. Moreover, ''In cooperative access control applications, false negatives can be remedied by users making second attempts.'' NIST FRVT Demographic Effects Report 3.

Additionally, while one commenter calculated the false non-match or false negative rate ''by subtracting the true acceptance rate from 1,'' NIST's report indicates that ''that definition is naïve in that it assumes every traveler was photographed. It ignores instances of failure-to-capture, and also cases where travelers are photographed, not matched, and then make further attempts.'' NIST, NISTIR 8381, FRVT Part 7: Identification for Paperless Travel and Immigration 8 (2021) (NIST 2021 FRVT Report), available at *https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8381.pdf* (last visited May 15, 2025).

There are several factors that could contribute to travelers not matching to the gallery. For example, whether a traveler has a photo in the gallery and how many photos of the traveler are in the gallery are two main factors. Some of the reasons why a traveler may not have a photo staged in the gallery include: first-time travelers to the United States entering the country under the Visa Waiver Program (VWP), travelers on military orders, and travelers whose flight manifest data was incorrect. As noted in the NIST 2021 FRVT Report press release, ''performance improves dramatically if the database contains multiple images of a passenger. The database gallery can contain more than one image of a single passenger. When an average of six prior images of a passenger are in the gallery, then all algorithms realize large gains.'' [147] Additionally, on exit, airline staff may choose to process travelers without having a photo taken. Physical changes, such as facial hair, hair style, make-up, and weight fluctuation do not affect a traveler's ability to successfully match to a photo in the gallery. Changes to bone structure, for example a cosmetic surgery, may affect matching; however, in those instances CBP or the airline agent may use traditional inspection processes consistent with existing requirements for entry and exit.

Prior to deploying facial comparison technology to ports of entry, CBP conducts extensive officer training, including mismatch, false match, or no match procedures. As discussed in the rule, in the event of a mismatch, false match, or no match CBP may use alternative means to verify the traveler's identity and ensure that the traveler is not unduly delayed. If the system fails to match a traveler, then a manual review of the traveler's document is performed. On entry, the CBP officer may continue to conduct additional screening or request fingerprints (if appropriate) to verify identity. Each inspection booth at entry is equipped with a fingerprint reader. At departure, the airline partner may conduct a manual review of the travel document (*i.e.,* scanning a boarding pass and checking a traveler's passport). If there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, the airline will contact CBP for additional inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask questions to validate identity and citizenship.

In accordance with its statutory authority, CBP uses the totality of information available, to include the results of a facial comparison match, to make admissibility decisions and take any law enforcement actions. Facial comparison alone does not determine admissibility. Nevertheless, if a traveler believes that CBP actions are the result of the TVS maintaining incorrect or inaccurate information, (*i.e.,* if the TVS finds a mismatch, false match, or no match) inquiries may be directed to CBP Information Center, Office of Public Affairs—MS1345, U.S. Customs and

[143] *See* David White et al., Passport Officers' Errors in Face Matching, PLoS ONE 9(8): e103510 (2014), *https://doi.org/10.1371/journal.pone.0103510* (last visited May 19, 2025).

[144] *See* DHS S&T, Snapshot: Customs and Border Protection Officers Leverage S&T-Developed Imposter Detection Training Tech to Maximize Officer Performance, *https://www.dhs.gov/science-and-technology/news/2020/02/25/snapshot-cbp-officers-leverage-st-developed-imposter-detection-training-tech* (last visited May 19, 2025).

[145] *See* CBP, Carrier Liaison Program Overview, *https://www.cbp.gov/travel/travel-industry-personnel/carrier-liaison-prog* (last visited May 21, 2025).

[146] DHS, TSA and CBP: Deployment of Biometric Technologies Report to Congress 29–30 (2019), is posted in the docket for this rulemaking.

[147] NIST, Press Release, NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding, July 13, 2021, available at *https://www.nist.gov/news-events/news/2021/07/nist-evaluates-face-recognition-softwares-accuracy-flight-boarding* (last visited May 21, 2025).

Border Protection, 1300 Pennsylvania Avenue NW, Washington, DC 20229, or online at *https://help.cbp.gov/s/?language=en_US.* Travelers may also contact the DHS Traveler Redress Inquiry Program (DHS TRIP), 6595 Springfield Center Drive TSA–910, Springfield, VA 22150–6901, or online at *https://www.dhs.gov/dhs-trip,* if they have experienced a travel-related screening difficulty, including those they believe may be related to incorrect or inaccurate biometric information retained in their record(s). Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue. These mechanisms allow any errors, if they occur, to be rectified.

Individuals seeking notification of and access to biometric information contained in the TVS, or seeking to contest the results of the biometric matching process may gain access to certain information in the TVS by filing a Privacy Act access request by emailing *privacy.cbp@cbp.dhs.gov* or a Freedom of Information Act (FOIA) request online at *foia.gov* or *https://www.securerelease.us/,* or by mailing a request to: FOIA Officer, U.S. Customs and Border Protection, 90 K Street NE, Washington, DC 20229, Fax Number: (202) 325–0150.[148] All Privacy Act and FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Requests for information are evaluated by CBP to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

*Comment:* Several commenters also stated that this rule was premature prior to NIST issuing a final report on the performance of CBP's Biometric Exit Program.

*Response:* CBP is committed to implementing the biometric entry-exit mandate in a way that provides a secure and streamlined travel experience for all travelers, and CBP will continue to partner with NIST and use NIST research to ensure the continued optimal performance of the CBP face comparison service.[149] The NIST 2021 FRVT Report demonstrates that the current biometric facial comparison technology passes the threshold for use in CBP's Biometric Exit Program, based on computer-focused simulations.

l. Under 14 Children: Privacy, Authorities, and Accuracy Concerns

*Comment:* Several commenters raised concerns regarding collecting biometrics on minors specifically as it relates to violating privacy rights, CBP's authority to do so, the potential for misidentification due to lower accuracy rates, reliability, and potential bias of facial comparison technology, particularly its impact on specific demographic groups, and the outcome of potential misidentification. One commenter expressed concern over the rule's lack of information regarding how CBP will collect biometrics from small children as well as a lack of data that supports CBP claims that biometrics collection on children would actually combat trafficking. Two commenters mentioned that children are unable to consent to biometric collection and stated CBP should require parental consent similar to trusted traveler programs.

*Response:* Modality, age, and frequency of collection are all significant factors to consider when discussing accuracy associated with biometric matching of children. DHS does not necessarily believe that these factors render the act of biometrics collection less accurate or unnecessary for this population. Instead, DHS believes that to accurately address the changing nature of children's biometrics, DHS should collect their biometrics at shorter intervals. The Department of State tacitly recognizes the same principle in issuing passports for individuals under the age of 16, which are only valid for 5 years, whereas passports for individuals aged 16 and older are valid for a period of 10 years.[150] In any case, these validity periods and collection practices do not render the biometric collection inaccurate; the photograph of the child is accurate the day it is collected, but over time the usefulness of any given photograph decreases. DHS recognized this as an issue and this is one of the reasons why DHS intends to collect biometrics upon entry into and exit from the United States.

DHS disagrees with commenters that removing age restrictions violates the INA. DHS interprets section 287(f)(1) of the INA (8 U.S.C. 1357(f)(1)) to require photographs and fingerprints from aliens 14-years or older in removal proceedings, but that authority does not prohibit the collection from those younger than 14 as authorized by other laws. The language of the statute is silent regarding collecting biometrics from those under the age of 14 outside of enforcement proceedings, as it explicitly states, ''the Commissioner shall provide for the fingerprinting and photographing of each alien 14 years of age or older against whom a proceeding is commenced'' under section 240 of the INA (8 U.S.C. 1229a). INA 287(f)(1) (8 U.S.C. 1357(f)(1)). In addition, DHS is authorized to take and consider evidence (including biometrics) concerning the privilege of any person to enter, reenter, pass through, or reside in the United States, or concerning any matter which is material or relevant to the enforcement of the INA and the administration of DHS. *See* INA 287(b) (8 U.S.C. 1357(b)). Accordingly, DHS is authorized under the INA to collect biometrics on individuals under the age of 14.

DHS abides by all relevant privacy laws, regulations, and policies in collection of biometric information for individuals, including children. DHS disagrees that adding a biometrics requirement constitutes subjecting children to additional scrutiny or is inappropriate due to their inability to consent. CBP's responsibilities, regardless of age, gender, race and nationality, include ensuring the interdiction of persons illegally entering or exiting the United States, facilitating, and expediting the flow of legitimate travelers, and detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States. *See* sec. 411(c) of the Homeland Security Act (6 U.S.C. 211(c)). Instead of verifying a child's identity using a manual review of travel documents, CBP will use facial comparison technology for identity verification at the border.

Not only will the facial comparison technology be used to determine and verify identity, but it will also support CBP efforts to ensure the safety of everyone crossing the border, including children. Typically, fraud schemes that DHS encounters involve adults and unrelated children posing as family units to DHS authorities. *See* John Davis, ''Border Crisis: CBP Fights Child Exploitation,'' Frontline Magazine, Dec. 16, 2019, *https://www.cbp.gov/frontline/border-crisis-cbp-fights-child-exploitation* (last visited May 15, 2025).

[148] For more information, see DHS, FOIA Contact Information, *https://www.dhs.gov/foia-contact-information* (last visited May 21, 2025).

[149] *See, e.g.,* DHS/OBIM/PIA–005 Office of Biometric Identity Management (OBIM)—National Institute of Standards of Technology (NIST) Data Transfer 3–5 (2022), available at *https://www.dhs.gov/publication/dhsobimpia-005-office-biometric-identity-management-obim-national-institute-standards* (last visited May 21, 2025).

[150] 22 CFR 51.4(b).

Nevertheless, minors can travel in and out of the United States without either one of their parents. To ensure the safety of children, CBP strongly recommends, but does not legally require, a notarized written consent letter from both parents. Since FY 2019, CBP processed over 35 million children under the age of 14 at ports of entry, many without parents present.[151] Minors require parental consent when applying for CBP's Trusted Traveler Programs as the programs are voluntary, and CBP requires consent for participation in all voluntary programs.

To take the photos of travelers, including children, CBP will not physically touch them. CBP may provide verbal instructions to the travelers to stand at a certain distance from the camera. Additionally, many cameras at CBP's primary inspection booths can be adjusted by the CBP officer to allow the CBP officer to place the camera in the optimal position to capture a high-quality image without touching the traveler. If CBP is unable to position the traveler to take a photo or in the event of a mismatch, false match, or no match, CBP may use alternative means to verify the traveler's identity and ensure that the traveler is not unduly delayed. If the system fails to match a traveler, then a manual review of the traveler's document is performed. This rule does not authorize the collection of other biometrics such as fingerprints on individuals younger than 14.

m. Surveillance

*Comment:* Several commenters raised concerns regarding the collection of photos being used for surveillance purposes, either by CBP or other U.S. Government Agencies that may have access to CBP data. Several commenters noted that use of facial comparison technology could support or lead to a police or carceral state. Several commenters noted that CBP could not be trusted with the technology as other government agencies have been criticized for using such technology to track journalists and protestors.

*Response:* CBP's Biometric Entry-Exit Program will not utilize the facial images submitted for widespread surveillance as the commenters suggest. Biometric entry-exit is not a surveillance program. The Biometric Entry-Exit Program uses facial comparison technology to ensure a person is whom the person claims to be and is the bearer of the passport that is presented. This technology provides a seamless way for in-scope travelers, as described in the rule, to meet the requirement to provide biometrics upon arrival and departure from the United States. Travelers are aware their photos are being taken and U.S. citizens have the ability to request alternative procedures as described in the rule. CBP uses facial comparison technology only where a current identity check already exists. CBP uses only photos collected from cameras deployed specifically for this purpose and does not use photos obtained from closed-circuit television or other live or recorded video. The cameras in support of CBP's Biometric Entry-Exit Program are clearly visible to all travelers. Additionally, CBP works closely with partner carriers and airport authorities to post privacy notices and provide tear sheets for affected travelers and members of the public in close proximity to the cameras and operators, whether the cameras are owned by CBP or the partners.

Consistent with regulatory requirements, photos of aliens who are required to provide a biometric are securely transferred to DHS's IDENT.[152] In the future, DHS intends to store these photos in IDENT's successor system, HART.[153] Certain other federal agencies and foreign partners may access these photos with the approval of DHS, if the purpose of their access is consistent with applicable SORNs.[154]

DHS OBIM is the lead designated provider of biometric identity services for DHS and manages IDENT.[155] As IDENT contains data from a variety of sources, collected for a variety of uses, DHS has instituted necessary controls so that only those individuals with a need to know are able to access that data.[156] Further, being an authorized user of IDENT does not provide automatic access to all of an individual's IDENT records. IDENT has a robust set of access controls, including role-based access and interfaces, which limit individual access to the appropriate discrete data collections.[157] For example, organization-level data filtering is applied to encounter data, which allows for certain data (for example, asylum data) to be protected so that only approved organizations will be able to access the data. DHS sets the appropriate data filtering and access restrictions consistent with privacy and confidentiality laws and policies. DHS will continue to follow the latest technologies and trends with regard to protecting all data, whether it is biometric or biographic, in an effort to prevent any breach.

Misuse of the data in IDENT is mitigated by requiring that IDENT users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems.[158] Also, DHS conducts a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity. Further, external connections must be documented and approved with both parties' signatures in an interconnection security agreement (ISA), which outlines controls in place to protect the confidentiality, integrity, and availability of the information being shared or processed.

DHS has policies in place to prevent improper sharing or unauthorized use of any data and nothing in this rule changes those policies.[159] IDENT maintains an audit record in the database for each system message sent to an external agency. Audit logs are maintained by OBIM's System Operations and Maintenance Branch. Access to audit logs is limited strictly to core System Operations and Maintenance Branch personnel. The audit log data are backed up regularly as part of the overall IDENT database backup and archiving process.

*Comment:* One commenter also expressed concern that technologies used in the United States could be adopted by other countries for surveillance as well.

*Response:* Regarding technologies used in the United States being adopted by other countries, CBP has no control over technologies adopted by other nations, therefore that issue is outside the scope of this rulemaking.

n. Violations of Constitutional Rights

*Comment:* Several commenters raised concerns regarding the impact of facial comparison technology to individuals' First, Fourth, Fifth, and Fourteenth Amendment rights. Specifically, commenters are concerned that the use of facial comparison technology will deter individuals from engaging in constitutionally protected activities, limit the right to travel, and violate the

[151] Information provided by CBP's Biometric Entry-Exit Strategic Transformation Admissibility and Passenger Programs Office, Office of Field Operations, subject matter expert on January 24, 2024.

[152] TVS PIA *at* 8.

[153] HART PIA *at* 2.

[154] IDENT PIA *at* 3–5; HART PIA *at* 30.

[155] DHS/ALL–043 Enterprise Biometric Administrative Records (EBAR) SORN, 85 FR 14955 (Mar. 16, 2020). *See* DHS, Office of Biometric Identity Management, *https://www.dhs.gov/obim* (last visited May 21, 2025).

[156] *See* IDENT PIA and Appendices.

[157] IDENT PIA *at* 27–28.

[158] IDENT PIA *at* 30.

[159] *See* IDENT PIA *at* 27; HART PIA *at* 31.

Fourth Amendment's protection against unreasonable searches of the people.

*Response:* DHS disagrees with these comments. DHS is not violating the Constitution of the United States with the changes made in this rule. As described in Section II of this preamble and clearly laid out in the NPRM, DHS has both general and specific statutory authority to collect or require submission of biometrics in its administration of the immigration laws.[160]

*Comment:* Some commenters raised concerns about violations of the First Amendment protections for religion.

*Response:* Regarding the First Amendment, specifically, DHS will use facial comparison technology in the administration of immigration laws, not to curtail any of the freedoms afforded in the First Amendment. For travelers with religious affiliations, CBP policy generally allows for alternative processing to accommodate a traveler on a case-by-case basis. These methods include fingerprint scans or requesting additional documents to establish identity and citizenship. On exit, the airline gate agent may conduct manual identity verification using the presented travel document, as is performed for flights where biometric processing is not available, and may notify CBP to conduct further examination, if necessary. For example, if there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, airline partners will contact CBP for additional inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask questions to validate identity and citizenship. As previously explained, biometric entry-exit is not a surveillance program. Rather, the entry-exit program will be used to confirm the identity of travelers and verify that they are the authorized bearers of their travel documents. Implementing an integrated biometric entry-exit system that compares biometric data of aliens collected upon arrival with biometric data collected upon departure is essential for addressing the national security concerns arising from the threat of terrorism, the fraudulent use of legitimate travel documentation, aliens who overstay their authorized period of admission (overstays) or are present in the United States without being admitted or paroled, and incorrect or incomplete biographic data for travelers.

*Comment:* Some commenters raised concerns regarding the Fourth Amendment protection against unreasonable searches and seizures.

*Response:* Regarding the Fourth Amendment, DHS's biometric entry-exit program complies with the Fourth Amendment and is consistent with the Congressional mandate to enact such a program. *See* section 110(b) of the DMIA (8 U.S.C. 1365a(b)) and section 7208(d) of the IRTPA (8 U.S.C. 1365b(d). To exercise its authority to control the border and to regulate the entry and departure of both aliens and U.S. citizens, CBP has a legitimate interest in confirming the identity of arriving and departing travelers and verifying that such persons are the authorized bearers of proffered travel documents. *See* INA 215, 235 (8 U.S.C. 1185, 1225). The use of facial comparison technology in DHS's entry-exit program is non-invasive and aligns with the Congressional requirement to develop such a program.

*Comment:* Some commenters raised concerns regarding the Fifth Amendment due process requirements.

*Response:* Regarding the Fifth Amendment, the entry-exit program does not deprive an individual of a constitutionally protected liberty interest. Similar to the practice of manual identity verification where biometric processing is not available, facial comparison technology will be utilized for identification purposes. For example, as is currently the practice on exit, during the manual review of the passport, if there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, airline partners will contact CBP for additional inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask questions to validate identity and citizenship. Requiring the submission of biometrics for identification purposes does not violate the Fifth Amendment's due process requirements nor does collecting and retaining certain biometric information deprive individuals of a liberty interest. DHS requires submission of biometrics as authorized by law.

*Comment:* One commenter raised concerns regarding the Sixth Amendment right to counsel.

*Response:* Regarding the Sixth Amendment, this right to counsel would not apply as these travelers have not been placed in criminal proceedings.

*Comment:* One commenter raised concerns regarding the Fourteenth Amendment right to equal protection.

*Response:* Regarding the rule giving rise to claims under the Fourteenth Amendment's Equal Protection clause, this rule does not affront the Fourteenth Amendment. DHS does not treat people differently based on any biological or physical characteristic of the affected person and nothing in this rule authorizes officers to do so. As explained previously, nothing in this rule will prevent refugees from receiving protections since, other than requiring biometrics for certain new populations, this rulemaking does not change eligibility requirements for asylum seekers or refugees and does not alter existing regulations at 8 CFR 208.6 protecting the confidentiality of information contained in or pertaining to asylum applications and certain other records, and which are also applied to information contained in refugee applications as a matter of departmental policy.

o. Authority for Biometric Collection and Related Regulations for Biometric Collection

*Comment:* Several commenters raised concerns regarding DHS's authority to specifically collect a ''faceprint'' as a biometric identifier as Congress has equated biometric identifiers with fingerprints. A commenter stated that 6 U.S.C. 1118 expressly disallows the expansion of biometrics collections in immigration. Some commenters stated that the use of facial comparison technology is an overreach of power.

*Response:* DHS is not exceeding its authority to collect biometrics, including 6 U.S.C. 1118, which states that nothing in this section shall be construed to permit the Commissioner of CBP to ''facilitate or expand the deployment of biometric technologies, or otherwise collect, use, or retain biometrics, not authorized by any provision or amendment made by'' the IRTPA or the Implementing Recommendations of the 9/11 Commission Act.[161]

DHS laid out both the general and specific statutory authority for biometric collection, including photographs, in the NPRM, and restates much of that explanation of authority in this final rule, and disagrees with commenters that it does not have authority to promulgate this rulemaking.[162] DHS's statutory authorities, including INA 287(b) (8 U.S.C. 1357(b)), authorize the collection of biometrics when such

[160] *See* the NPRM, 85 FR at 74164, for more information regarding DHS' statutory authority to require biometrics.

[161] Sec. 1919(b) of the FAA Reauthorization Act of 2018, Public Law 115–254, 132 Stat. 3186, 3559 (6 U.S.C. 1118(b)).

[162] *See* the NPRM, 85 FR at 74164, for more information regarding DHS' statutory authority to require biometrics.

information is material or relevant to the furtherance of DHS's delegated authority to administer and enforce the INA. Establishing and verifying an individual's identity through the use of biometrics falls within DHS's authority in the administration and enforcement of immigration laws.

*Comment:* One commenter said that DHS failed to mention a companion proposal to expand types of biometrics collected by USCIS.

*Response:* Any proposals by USCIS to expand biometrics is outside the scope of this rulemaking. While the NPRM did reference the USCIS NPRM, as noted above, the USCIS NPRM has now been withdrawn. *See* 86 FR 24750.

p. Alternatives to Facial Comparison Technology

*Comment:* Several commenters raised concerns regarding CBP's decision to utilize one to few (1:n) matching instead of one to one (1:1), which CBP has tested and some consider safer from a privacy perspective. Additionally, several commenters indicated that CBP has not sufficiently evaluated alternatives.

*Response:* CBP respectfully disagrees. As mentioned in the NPRM, CBP considered many types of biometrics and has concluded that partnering with carriers and airports to capture facial images is the most viable large-scale solution as it is highly effective, cost effective, and less disruptive than other possible methods.[163] Two other methods that were considered were fingerprint and/or iris scans and using CBP personnel and equipment to collect the facial scans. CBP has tested fingerprint and iris scans on a limited basis to determine their effectiveness and scalability. CBP found that although these scans are highly effective in finding matches when data is available, they have numerous problems. First, CBP often lacks data to match against. Although CBP often has fingerprints from entry that it can use to match a departing alien, it does not typically capture iris scans. Additionally, these biometrics are not typically included in passports. To use iris scans, CBP would need to establish a new way to capture a baseline iris scan to compare against at exit, which is not feasible. Fingerprint and iris scans are also more time-consuming and the equipment needed is more expensive than facial comparison.

Although CBP does use 1:1 verification, using strictly 1:1 verification would add a substantial amount of processing time to each inspection, which would negatively affect CBP's mission of facilitating travel. On entry, CBP utilizes 1:1 comparison in the pedestrian environment for travelers that possess an e-chip photo consistent with Western Hemisphere Travel Initiative (WHTI) requirements. For other travelers, CBP is able to create galleries based on the manifest information received from carriers for air, sea, and bus travelers. The galleries allow for a 1:n comparison, which is faster and less intrusive to the travelers.

On exit, a 1:1 verification would require private sector partners to procure additional equipment that can open and read e-chips, when available, and collect and submit more information to CBP. This is both costly and time-consuming as well as an increase in the privacy implications on the public. As with entry, CBP is able to create galleries based on manifest information received from carriers for air, sea, and bus travelers. The galleries allow for 1:n comparison which is faster and less intrusive to the travelers.

*Comment:* One commenter suggested an alternative ''opt-out'' option available to U.S. citizens can be extended to aliens in lieu of additional alternatives.

*Response:* Upon the effective date of this final rule, all aliens seeking admission to and departing from the United States may be subjected to facial comparison to determine identity or for other lawful purposes. CBP bears the ultimate responsibility for biometric collection to satisfy the Congressional biometric entry-exit mandate. Partner airports and carriers facilitate collection through the use of CBP's TVS, which provides an automated mechanism to verify identity.

Additionally, as part of the inspection process, DHS is authorized to take and consider evidence (including biometrics) concerning the privilege of any person to enter, reenter, pass through, or reside in the United States, or concerning any matter which is material or relevant to the enforcement of the INA and the administration of DHS. *See* INA 287(b) (8 U.S.C. 1357(b)).

*Comment:* One commenter asked why DHS intends to collect both fingerprints and facial comparison data.

*Response:* As discussed in the NPRM and this final rule, fingerprint scans have proven to be an effective law enforcement tool, which is why CBP will continue to capture fingerprints as the initial identification biometric.[164] CBP may elect not to collect fingerprints for subsequent identity verification where CBP has implemented facial comparison.

q. Rule Impact on Migration, Immigration, and National Security

*Comment:* Several commenters raised concerns that DHS failed to justify collecting facial images from the proposed individuals and that by collecting photographs circular migration is affected, vulnerable populations, including asylum seekers and refugees, are deterred from fleeing persecution, and immigrants are at risk of future violence and losing their immigration status in the name of national security.

*Response:* DHS disagrees with these comments. As discussed in the NPRM, DHS is mandated by statute to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States.[165] CBP has determined that facial comparison technology is currently the best available method for biometric verification, as it is accurate, unobtrusive, and efficient. Upon the effective date of this final rule all aliens entering or exiting the United States may be subjected to facial comparison, regardless of age, gender, or race and nationality. This rule will not ''extend to everyone associated with an immigration case'' as asserted by a commenter.

This rule improves DHS's ability to meaningfully implement a comprehensive biometric entry-exit system and make the process for verifying the identity of aliens more efficient, accurate, and secure by using facial comparison technology. Implementing an integrated biometric entry-exit system that compares biometric data of aliens collected upon arrival with biometric data collected upon departure is essential for addressing the national security concerns arising from the threat of terrorism, the fraudulent use of legitimate travel documentation, aliens who overstay their authorized period of admission (overstays) or are present in the United States without being admitted or paroled, and incorrect or incomplete biographic data for travelers.

In this final rule, DHS thoroughly discusses how facial comparison mitigates the above-mentioned national security concerns. Nevertheless, the

[163] *See* the NPRM, 85 FR at 74169–74173, for more information regarding CBP's tests to determine the best option for biometrics collection.

[164] *See* the NPRM, 85 FR at 74173, for more information on fingerprint collection as the initial biometric.

[165] *See* the NPRM, 85 FR at 74164, for more information regarding DHS' statutory authority to require biometrics.

totality of the screening system must be taken into account when discerning the national security benefits. As discussed in the 9/11 Commission Report, biometric entry-exit is essential to national security and should include a systemic approach that balances security, efficiency and civil liberties.[166]

CBP's responsibilities, regardless of age, gender, race and nationality, include ensuring the interdiction of persons illegally entering or exiting the United States, facilitating and expediting the flow of legitimate travelers, and detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States. *See* sec. 411(c) of the Homeland Security Act (6 U.S.C. 211(c)). CBP uses the totality of information available, to include the results of a facial comparison match, to fulfill these responsibilities.

Biometric entry-exit is an identity verification tool. As previously explained, the biometric entry-exit program uses facial comparison technology to ensure a person is whom the person says the person is—the bearer of the passport the person presents. Biometric entry-exit is complementary to CBP's multilayered enforcement approach and border security mission.

DHS has no data or evidence, and the commenters provide only assertions and not any empirical evidence, studies, or reports, to support the statement that photograph submission reduces circular migration, deters vulnerable populations from fleeing persecution or causes a decline in U.S. tourism or the U.S. economy. DHS's intent for this rule is explained in detail herein.

Nothing in this rule prevents refugees from receiving protections since, other than requiring biometrics for certain new populations, this rulemaking does not change eligibility requirements for asylum seekers or refugees and does not alter existing regulations at 8 CFR 208.6 protecting the confidentiality of information contained in or pertaining to asylum applications and certain other records, and which are also applied to information contained in refugee applications as a matter of departmental policy.

*Comment:* One commenter discouraged DHS/CBP from seeking to justify this NPRM by securing TSA's adoption of facial biometric comparison using TVS in domestic airports.

*Response:* In the cost-benefit analysis, DHS noted in the NPRM that the development of a reliable facial comparison system could also have benefits for the U.S. government as a whole, including TSA.[167] This is not a justification for the rule, but rather a secondary benefit. Furthermore, DHS strives to build a more unified and operationally effective and efficient organization through collaboration across DHS. TSA has leveraged TVS for baggage drop and TSA check points, which increases DHS's operational effectiveness by reducing unnecessary duplication and redundancy. As with the current CBP–TSA uses of TVS, any future use of TVS, whether for international or domestic travelers, will undergo all necessary legal and privacy assessments and evaluations.

*Comment:* Some commenters stated that taking a photo will add more burden, confusion, and harassment at the ports of entry.

*Response:* CBP respectfully disagrees as nothing in the rule is meant to burden, confuse, intimidate, or harass aliens at the ports of entry. As mentioned in Section III.B.1 above, CBP has determined that facial comparison technology is currently the best available method for biometric verification, as it is accurate, unobtrusive, and efficient. It relies on current traveler behaviors and expectations; most travelers are familiar with cameras and do not need to learn how to have a photograph taken, minimizing any confusion. Should travelers express any confusion either a CBP officer or a gate agent can guide them through the new process or provide a tear sheet with additional information.

Furthermore, each CBP employee has a responsibility to the United States Government and its citizens to place loyalty to the Constitution, laws, and ethical principles above private gain. To ensure that every citizen can have complete confidence in the integrity of the Federal Government, each employee shall respect and adhere to the principles of ethical conduct set forth in the Code of Federal Regulations. See 5 CFR part 2635. Additionally, Section 7.11.2 of the CBP Standards of Conduct specifically states, ''Employees will not make abusive, derisive, profane, or harassing statements or gestures, or engage in any other conduct evidencing hatred or invidious prejudice to or about another person or group on account of race, color, religion, national origin, sex, sexual orientation, age, or disability.'' CBP Directive 51735–013B, Standards of Conduct at 11 (2020), available at *https://www.cbp.gov/sites/default/files/assets/documents/2021-Jan/cbp-standards-conduct-2020_0.pdf* (last visited May 15, 2025).

*Comment:* Several commenters noted that per CBP's FY 2020 Trade and Travel Report, no imposters were identified in the air environment during FY2020.

*Response:* CBP expanded the number of locations with facial comparison technology and as a result biometrically processed more travelers compared to FY2019; however, as noted in the Trade and Travel Report, CBP saw a decrease in traveler volume of 42 percent in FY 2020 when compared to data from FY 2019, which may have affected the number of imposters identified. Nevertheless, as traveler volume has increased CBP has seen an increase in the number of imposters identified with 2,000 imposters identified at land ports and airports.[168]

*Comment:* One commenter noted that CBP is attempting to move the goal posts it had originally established for the use of facial comparison technology in airports from national security to pandemic mitigation.

*Response:* Although CBP's primary responsibility is national security, CBP must also facilitate legitimate trade and travel. The use of facial comparison technology, as explained in this final rule, has enabled CBP to not only address a national security concern head-on by enhancing identity verification but to simultaneously improve the traveler experience throughout the travel continuum. This is not an attempt ''to move the goal posts,'' but rather an opportunity to showcase the several benefits that facial comparison technology provides. As CBP continues to use the technology and threats evolve, additional benefits are identified, such as the use of biometrics to mitigate the transmission of pathogens. As noted by the commenter, CBP may take other steps to mitigate the transmission of pathogens, such as installing plexiglass at the primary inspection booths; however, implementing one mitigation measure does not reduce the need for additional measures, especially when dealing with a global health crisis.

r. Proposed Amendments to the Regulations

*Comment:* Several commenters raised concerns regarding the proposed

[166] The 9/11 Commission Report 385–386 (2004) (emphasis added), available at *https://9-11commission.gov/report/* (last visited May 21, 2025).

[167] *See* the NPRM, 85 FR at 74188, for more information on the benefits to the U.S. government.

[168] *See* CBP, Biometrics, *https://www.cbp.gov/travel/biometrics* (last modified Oct. 5, 2023) (last visited May 21, 2025).

addition of ''or other lawful purposes'' in 8 CFR 215.8(a)(1) and 8 CFR 235.1(f)(1)(ii) as they asserted the language is vague and would expand the use of photographs captured upon the entry into or the exit out of the United States beyond what is authorized in regulations as they existed prior to this final rule.

*Response:* DHS disagrees with these comments. As discussed in the NPRM, DHS is mandated by statute to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States.[169] As articulated in section 7208 of the IRTPA (8 U.S.C. 1365b), the biometric entry-exit system serves several purposes; this includes recording entries and exits of aliens to the United States. The entry-exit system may also be used to determine whether an alien has properly maintained immigration status while in the United States. Once collected, and to the extent the data is maintained for any length of time, the information may be used to support other lawful enforcement purposes. Section 7208 of the IRTPA (8 U.S.C. 1365b) does not limit CBP's use of the data to simply the entry-exit purpose.[170] In addition, as previously explained, the biometric entry-exit does support CBP's border security mission and is complementary to the agency's multilayered enforcement approach.

As stated in 8 CFR 215.8(b) prior to the effective date of this final rule, ''an alien who is required to provide biometric identifiers at departure . . . who fails to comply with the departure requirements may be found in violation of the terms of his or her admission, parole or admission status.'' DHS is simply expanding the scope of aliens that are subject to that requirement.

*Comment:* Additionally, commenters raised concerns about requiring certain aliens entering and departing the United States to ''provide other biometrics'' and ''other such evidence requested,'' which is overly broad and ambiguous.

*Response:* DHS has the authority under both 8 CFR 215.8 and 235.1 to request that aliens provide biometrics and ''such other evidence as may be requested.'' DHS is not expanding its authority by continuing to request other evidence.

*Comment:* One commenter opined that DHS proposes to coerce immigrants to provide an unjustified amount of private information under the threat of losing their immigration status.

*Response:* DHS disagrees with this comment. DHS requires submission of biometrics as authorized by law. Additionally, DHS is mandated to implement a biometric entry-exit system.

*Comment:* Some commenters raised concerns that the definition of ''biometrics'' was being expanded to include DNA, iris scans, and palm prints.

*Response:* As discussed in this final rule, to continue to allow flexibility for DHS to employ different methods of biometric collection in the future, DHS is amending 8 CFR 215.8(a) and 235.1(f) to provide that any alien, other than those exempt by regulation, may be required ''to provide other biometrics'' upon arrival into and departure from the United States. CBP has tested iris technology, for example, but biometric technology continues to advance and there may be other biometric options that may have potential for implementation in the future. Additionally, any collection of any biometrics will be consistent with U.S. law.

s. Land and Sea Implementation

*Comment:* Some commenters requested that CBP suspend the proposed rule change until such time that a biometric exit solution for land and sea ports is identified. In the absence of a tested and compatible solution at land and sea ports, it is not appropriate for CBP to forge ahead across all airports and cement a collection and matching program that it may not be possible to operationalize at land and sea ports. One commenter indicated that further details on process, timing, cost, etc., in the land and sea environments are necessary to ensure traveler confidence and comprehension.

*Response:* The regulatory changes are necessary to enable CBP to continue its refinements and implement permanent programs efficiently once the best solution is identified. Under the regulations prior to the effective date of this final rule, CBP could conduct pilot programs only at a limited number of ports of entry at air and sea and could collect biometrics only from a limited population. Pursuant to this final rule, CBP will continue to work to determine the best method for implementation as necessary. In the time since the NPRM was published, CBP has implemented facial biometric collection fully at air entry, sea entry, and pedestrian land entry. Further details about those environments can be found in Section VI of this rule. Additionally, when CBP moves forward with a large-scale implementation for entry-exit at land ports or for private aircraft or for exit at sea ports, CBP will publish a notice in the **Federal Register** providing information regarding details of implementation in each new environment and requesting comments on the newly implemented transportation modalities. If CBP determines that the implementation of the specified facial comparison entry-exit program at land ports or exit at sea ports results in significant delays, CBP will temporarily discontinue these efforts until the average processing time has improved to be under 125 percent of the baseline (manual processing without biometrics).

t. Implementation Challenges

*Comment:* Some commenters said this rule does not mention any implementation challenges that have been encountered with the currently deployed biometric system, which directly affects CBP's ability to achieve the benefits outlined in this rule. CBP should develop photo capture requirements and camera system standards and requirements for at least three consecutive months to reduce malfunction and successfully capture each traveler.

*Response:* CBP disagrees with the premise of these comments. As discussed in the NPRM and in this final rule, CBP is using biometric technologies in partnership with commercial stakeholders.[171] In order to use CBP's TVS, partners must meet all of CBP's business and technical requirements, such as internet/connection guidelines, photo specifications and equipment parameters. It is important to note that, unlike FIS areas, the airport departure areas are not managed by CBP personnel; however, CBP works closely with the stakeholders to mitigate any issues that may affect system performance. CBP has a suite of tools that allows for system and operational performance management and CBP uses performance reports that are automatically generated and distributed weekly within CBP and to external stakeholders. CBP monitors the reports for performance issues and addresses any anomalies with stakeholders as they arise. The reports are also used to promote/increase usage by stakeholders.

[169] *See* the NPRM, 85 FR at 74164, for more information regarding DHS' statutory authority to require biometrics.

[170] *See* TVS PIA at 16–17 for more information on the permissible uses of this data.

[171] *See* the NPRM, 85 FR at 74178, for more information on business partnership requirements.

u. Cost and Cost-Benefit Analysis Concerns

*Comment:* Some commenters raised concerns surrounding the costs associated with this rule. One comment stated that this is a waste of government resources. One commenter indicated that the money used for this program should be redirected to more deserving programs such as uniting children. Another suggested the money should be spent rooting out corruption, incompetence, extremism, and politics from our law enforcement agencies and armed forces.

*Response:* Allocation of money for agencies is determined by Congress as part of its appropriation process. It is not within DHS's authority to reallocate money appropriated by Congress for a specific purpose to a different purpose. In FY 2016, Congress authorized the funding of the original, biometric entry-exit program through up to $1B in fees, collected by USCIS, on H–1B/L–1 applications, through FY 2027.[172]

Further, DHS is statutorily mandated to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States. Additionally, DHS believes that the purposes of this rule, namely to deploy a comprehensive biometric entry-exit system and enable CBP to make the process for verifying the identity of aliens more efficient, accurate, and secure by using facial comparison technology, as well as the national security and immigration benefits—such as helping detect and deter visa overstays and visa fraud; helping identify persons attempting to fraudulently use travel documents; and alerting authorities to criminals or known or suspected terrorists prior to boarding—are all appropriate uses of DHS and the administration's time and resources. DHS disagrees strongly that this rule is a waste of taxpayer funds.

*Comment:* A few commenters suggested that the analysis did not present all the costs associated with this rule, and that the actual costs would be significantly higher than CBP's estimate, suggesting that there was not sufficient data presented in the cost-benefit analysis to support this rule. Additionally, the rule allows for expansion of biometric collection at sea and land port locations but such costs are not provided in the analysis, therefore CBP is proposing to be given such authority regardless of the data collection method or costs.

*Response:* DHS disagrees that there was not sufficient data presented in the cost-benefit analysis to support this rule. As explained in the rule, CBP is using biometric technologies in voluntary partnerships with other federal agencies and commercial stakeholders. Based on agreements with CBP, these stakeholders deploy their own camera operators and camera technology to operate TVS for identity verification. CBP expects that the use of facial comparison to collect biometric information will help streamline the entry and exit process, generating efficiencies to CBP, carriers, and travelers. Additionally, it will support CBP's capability in determining whether aliens are departing the country when they are required to depart, reduce visa, or travel document fraud, and improve CBP's ability to identify criminals and known or suspected terrorists before they depart the United States. In recent years CBP has implemented a variety of pilot programs to test the collection of this biometric information during entry and exit. Therefore, CBP does have some past data available to provide an estimate of overall costs and benefits during the pilot test program period. CBP expects that the data obtained during the pilot period assists in generating a reliable estimate of future costs and benefits from collection of this biometric information.

The analysis for the NPRM was done using the standards required under Executive Order 12866 and 13563 and is in compliance with the Regulatory Flexibility Act. Specific guidance on how agencies should conduct cost benefit analyses for regulations can be found in OMB Circular A–4. Regulatory analysis should monetize any effects that can be monetized. Those that cannot be monetized should be analyzed quantitatively, if possible. Those that cannot be monetized or quantified should be analyzed qualitatively. The analysis for the NPRM was done based on the best information available at the time. When the NPRM had been written, biometrics had not yet been deployed in all environments, so it was impossible to conduct a quantitative analysis for those environments. For this final rule, CBP has updated the estimates in the NPRM and has expanded it to include several new use-cases. There are still environments where CBP has not implemented a biometric process. For these environments lack of information and details make it impossible to monetize or quantify the effects, so CBP provides qualitative discussion based on limited details that were available at the time of the final rule on future biometric process implementation provides qualitative so we analyze them qualitatively.

DHS acknowledges that there will be costs associated with this final rule. DHS has updated the regulatory impact analysis for this final rule to reflect more recent data and information to improve DHS's best estimate of this rule's costs and benefits, including the expansion of facial comparison biometric collection to additional environments beyond the air environment. According to the regulatory impact analysis for this rule, DHS determined a net cost of $572 million (in undiscounted 2024 U.S. dollars) during the pilot period (2017–2024) and estimates a net cost of $287 million (in undiscounted 2024 U.S. dollars) in the 5-year regulatory period 2025–2029.

Because CBP has not determined the best approach to implement biometric collection at entry-exit for private aircraft, at exit at land ports, at entry for travelers in vehicles or for exit at sea ports, CBP is unable to provide any estimates for these costs to implement a biometric entry-exit system nationwide to these environments. This rule provides CBP authority to establish biometric entry-exit on a nationwide basis but CBP acknowledges that due to lack of information at this time, when CBP moves forward with a large-scale implementation for entry-exit biometric collection for private aircraft, at exit at land ports, at entry at land ports for travelers in vehicles or for exit at sea ports, CBP will publish a notice in the **Federal Register** with information regarding details of implementation and request comments on the newly implemented transportation modalities. DHS asserts that the regulatory impact analysis for this final rule is sufficient to meet DHS's obligations under Executive Orders 12866, 13563, and 14192.

*Comment:* A few commenters were concerned with the voluntary opt-out rate of U.S. citizens used in the regulatory impact analysis, specifically commenters believe that the opt-out rate used in the economic analysis for this rule significantly underestimated the number of U.S. citizens that would opt-out of having their photographs taken for use of facial comparison during biometric collection.

*Response:* CBP originally determined the U.S. citizen opt-out rate to voluntarily participate in the biometric exit program was 0.18% and was based on a 2-day sample in 2019 of 13,000

[172] *See* Consolidated Appropriations Act, 2016, Div. O, sec. 402(g), Public Law 114–113, 129 Stat. 2242, 3006, as amended by sec. 30203(b) of the Bipartisan Budget Act of 2018, Public Law 115–123, 132 Stat. 64, 126.

travelers at a single airport location.[173] CBP conducted a time and motion study to verify and reassess the 0.18% opt-out rate in late August 2021.[174] From this CBP Time and Motion Study CBP determined that the opt-out rate for biometric exit collection in the air environment was approximately 0.28% of outbound travelers. CBP uses this new estimate in the regulatory impact analysis for the final rule, to calculate future U.S. citizens who will opt-out of facial comparison during biometric collection at exit in the air environment.

To determine the opt-out rate for U.S. citizens during facial comparison at Simplified Arrival for biometric collection at entry, CBP used data from internal databases to calculate the actual number of opt-outs compared to the total number of U.S. citizen inbound air travelers processed through Simplified Arrival. CBP calculated the opt-out rate for U.S. citizens at entry during biometric collection through Simplified Arrival was approximately 0.13%. CBP used this estimate to calculate the number of U.S. citizens who will opt-out of facial comparison at entry during Simplified Arrival during the regulatory period of the regulatory impact analysis for the final rule. CBP also used this opt-out rate of approximately 0.13% to estimate the number of U.S. citizens who will elect to opt out of facial comparison biometric collection during entry processing at Simplified Arrival in the sea environment and at Mobile Face Primary in the sea environment.

To account for U.S. citizens opting out of facial comparison biometric collection at entry in the sea environment during Facial Biometric Debarkation, CBP used the same opt-out rate that was determined from the CBP Time and Motion Study for travel industry-led facial comparison biometric collection in the air environment of approximately 0.28% discussed above. Additionally for pedestrians entering the United States in the land environment and who are processed through Pedestrian Entry, CBP used internal data to determine that approximately 0.21% of U.S. citizens elected to opt out of facial comparison biometric collection. CBP used this rate to estimate the number of U.S. citizen pedestrians that would elect to opt out of facial comparison biometric collection when processed through Pedestrian Entry, in the regulatory impact analysis for this final rule.

*Comment:* One commenter argued that a Regulatory Flexibility Analysis (RFA) should have been conducted pursuant to the Regulatory Flexibility Act as individuals could potentially be small businesses, including sole proprietors, self-employed individuals, and freelancers, representing small entities, therefore a significant number of small entities could be affected, and this rule warrants a complete RFA.

*Response:* DHS does not believe an RFA was required for the NPRM. The Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121, 110 Stat. 857), requires agencies to consider the impacts of their rules on small entities. This final rule directly regulates individual travelers, which are not small entities. However, CBP does not anticipate that this rule will result in any significant impact to individual travelers, as according to the analysis individual travelers will likely incur an insignificant time burden during exit and time savings during entry.

*Comment:* A few commenters were also concerned with CBP's proposed timeline for implementation of the biometric exit program (97% implemented by 2024), specifically as the air industry had been hurt significantly in 2020.

*Response:* CBP: has still not yet reached 97% implementation, but is continuing to work with carriers and airports to establish partnerships to implement this program nationwide. These partnerships with carriers and airports streamline the process and eliminate redundancies. As explained in detail in the robust economic analysis, the hardware cost will be borne by the carriers and airports who partner with CBP. CBP will give carriers and airports access to its facial comparison system and the carriers and airports will choose (and pay for) the hardware that best fits their needs. Despite disruptions to the airline travel industry from the COVID–19 pandemic and negative economic impacts, there continues to be significant interest from the airline industry to use facial comparison. CBP continues to work to fully implement biometric collection at air exit as soon as possible. This Public-Private Partnership aligns with CBP's Resource Optimization Strategy.[175]

*Comment:* Additionally, a few commenters were concerned with the lack of discussion regarding costs to individuals that could result in potential delays resulting from a no match situation during boarding.

*Response:* CBP does not expect there to be any delays as a result of no match situations during the boarding process on flights where biometrics are being collected. In the event of a no match during facial comparison, the airline staff will manually observe the individual's travel documents using the same process that takes place absent this rule. Additionally, CBP does not anticipate that in the event of a no match, that a CBP officer would be asked to verify an individual's travel documents more frequently than what occurs prior to the implementation of this rule.

## VI. Request for Comment

As discussed above, DHS is issuing a final rule to finalize the changes proposed in the NPRM. However, DHS is requesting comments regarding the specific method of collection for newly implemented transportation modalities as well as costs and benefits for the newly implemented transportation modalities, namely, the Simplified Arrival process at air entry, the sea entry processes, and the process for entry for pedestrians at land ports. Comments submitted regarding any other topic on these newly implemented transportation modalities are out of scope for this final rule and will not be considered DHS will also provide notice and seek comments for future implementations of facial biometric collection in line with the authorities discussed in this rule.

## VII. Statutory and Regulatory Requirements

### *A. Executive Orders 12866, 13563, and 14192*

Executive Orders 12866 (Regulatory Planning and Review) and 13563 (Improving Regulation and Regulatory Review) 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. Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. Executive Order 14192 (Unleashing Prosperity Through Deregulation) directs agencies to significantly reduce the private expenditures required to comply with Federal regulations and provides that ''any new incremental costs associated

[173] *See* the NPRM, 85 FR at 74183, regarding the opt out rate estimate at the time of NPRM publication.

[174] CBP, Biometric Air Exit Time and Motion Study (2021) (CBP Time and Motion Study). This internal study was conducted August 22 through September 1, 2021, and is discussed in greater detail in the full regulatory impact analysis of this final rule in a separate document included in the docket for this rulemaking, docket number [USCBP–2020–0062].

[175] *See* CBP, Resource Optimization Strategy, *https://www.cbp.gov/border-security/ports-entry/resource-opt-strategy* (last visited May 21, 2023).

with new regulations shall, to the extent permitted by law, be offset by the elimination of existing costs associated with at least 10 prior regulations.''

This rule has been designated a ''significant regulatory action'' that is economically significant, under section 3(f)(1) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget.

Pursuant to section 5(a) of Executive Order 14192, the requirements of that Executive Order do not apply to regulations issued with respect to a national security or homeland security function. As discussed in this preamble, the primary, direct benefit of this rule is improvement in national and homeland security. Accordingly, this rule is exempt from the requirements of Executive Order 14192.

In summary, during the period of analysis, FY 2017–2029, CBP expects there to be costs, and benefits from this final rule, resulting in annualized net costs ranging from $67.9 million in 2024 U.S. dollars (using a three percent discount rate) to $70.3 million in 2024 U.S. dollars (using a seven percent discount rate) to the Federal Government, the air travel industry, the sea travel industry and alien and U.S citizen air travelers, sea travelers and land pedestrian travelers. The final rule will result in the non-monetized benefit of improving national security by validating the identity of individuals entering and exiting the United States. CBP expects this final rule will improve CBP's ability to detect and deter visa overstays and visa fraud, identify persons using fraudulent travel documents and the detection of criminals or known or suspected terrorists at entry or exit. The following is an abbreviated analysis of the costs, cost savings and benefits of this final rule. The full regulatory impact analysis of this final rule is in a separate document included in the docket for this rulemaking, docket number [USCBP–2020–0062].

DHS is statutorily mandated to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States. Since 2004, DHS, through CBP, has been collecting biometric data from aliens arriving in the United States, but currently there is no comprehensive biometric system in place to track when the aliens depart the country. Since taking over management of biometric entry and exit operations in 2013, CBP has been testing various options to collect biometrics at arrival and departure. The results of these tests and the recent advancement of facial comparison technology have provided CBP with a model for moving forward with implementing a comprehensive biometric exit solution in the air environment as well as improving the collection of biometrics at entry in the air, sea, and land environments.

CBP has developed a process for using facial comparison technology to collect biometrics in the commercial air environment, at entry in the sea environment and at entry for pedestrians in the land environment; however, CBP is still determining the best approach to expand the collection of biometrics using facial comparison technology for processing travelers in vehicles entering the United States in the land environment or a comprehensive solution for travelers at exit in the sea and land environments. CBP continues its work to determine the best option for biometric collection in these environments. At this time CBP has implemented comprehensive facial comparison biometrics at entry in the air, sea, and land (pedestrians only) environments and at exit only in the air environment.

During the initial stage of implementation for biometric collection at exit in the commercial air environment, starting in 2016, CBP introduced facial comparison technology to a limited number of airports in a voluntary pilot program. These deployments allowed CBP to fine-tune the process of using facial comparison technology for biometric collection at exit, while also partnering with airline carriers and airports (the air travel industry) toward a nationwide implementation. CBP's biometric exit program in the air environment was initially limited to 15 locations during the pilot period. CBP has since partnered with air travel industry members voluntarily expanding the program to additional locations. CBP has been able to find willing partners from the air travel industry as the industry has recognized the benefits of streamlining the boarding process and creating a seamless touchless experience for air travelers using facial comparison technology throughout the entire airport, from verifying identity, to obtaining boarding passes, checking bags, passing security and boarding. Additionally, the touchless passage through an airport may mitigate the risk of pathogen transmission.[176]

The facial comparison system engineered and developed for biometric exit in the air environment, known as the Traveler Verification Service (TVS) has also been implemented in other environments. CBP used the TVS when developing a program to use facial comparison technology to collect biometrics at entry in the commercial air environment, known as the Simplified Arrival process (Simplified Arrival), expediting the entry process for inbound air travelers, and improving security measures. Prior to Simplified Arrival, most inbound alien air travelers were already photographed during the entry process into the United States. Simplified Arrival compares the photographs collected at arrival to the passport, which expedites the arrival process. Because the infrastructure was already in place to take photographs of aliens, CBP was able to complete the entire nationwide deployment of Simplified Arrival in the air environment by the end of 2022. The entry processes in the air and sea environments are similar and in certain locations CBP was able to introduce Simplified Arrival in the sea environment starting in 2021 to use facial comparison technology for biometric collection of some inbound sea travelers.[177] By the end of 2023, CBP had fully implemented Simplified Arrival in the sea environment with operations at 39 sea port locations where the entry process in the sea environment was similar to entry in the air environment.

Where the entry process differs between the air and sea environments and Simplified Arrival was not a viable option, TVS allowed CBP to implement additional processes for biometric collection using facial comparison technology at entry. Starting in 2018, CBP began working with the sea travel industry to introduce facial comparison biometric collection at entry in the sea environment for certain sea travelers. Sea travel industry members voluntarily participated in conducting FBD, which uses facial comparison technology hardware procured by the sea travel industry in coordination with CBP's TVS to confirm passenger identity at entry.[178] CBP also implemented another

[176] Information provided by CBP's Innovation and Strategy Directorate, Biometrics Program Office, Office of Field Operations, subject matter expert on March 18, 2022.

[177] CBP implemented a few different biometric collection processes at entry in the sea environment because of different treatment of sea travelers prior to the implementation of biometric collection using facial comparison technology. Simplified Arrival was implemented at 39 sea ports to process certain cruise vessel passengers and most cruise vessel crew members.

[178] FBD was implemented by sea travel industry members for only certain types of cruise vessel arrivals. The entry process for a cruise is different

Continued

biometric collection process using TVS for facial comparison at entry in the sea environment known as Mobile Primary Face. When cargo vessels arrive at a U.S. sea port, CBP officers typically conduct entry processing of crew members onboard the cargo vessel. The introduction of Mobile Primary Face allowed CBP officers with mobile devices to conduct biometric collection using facial comparison technology for cargo vessel crew members. The implementation of these biometric collection processes at entry in the sea environment using facial comparison technology has expedited the arrival process for many inbound sea travelers.

CBP was also able to use TVS and the Simplified Arrival process to develop a biometric collection process using facial comparison technology during the entry process for pedestrians in the land environment, known as Pedestrian Entry. The entry process for pedestrians in the land environment is similar to other environments such that travelers go through a CBP inspection where they provide their travel documents (*e.g.,* passport) and the CBP officer manually inspects the documents to verify the identity of the traveler and determine admissibility. During this entry process most inbound alien pedestrian travelers are photographed and often have their fingerprints taken to verify their identity. Pedestrian Entry allows CBP to use facial comparison technology instead of conducting manual inspections of travel documents and obtaining fingerprints, resulting in an expedited entry process for pedestrians in the land environment. Similar to entry in the commercial air environment, the infrastructure was largely already in place for CBP to quickly implement Pedestrian Entry. CBP introduced Pedestrian Entry to one pilot location in 2018 and by the end of 2022 Pedestrian Entry had been fully implemented by CBP at 185 locations on the northern and southern border of the United States that process inbound pedestrians.[179]

This final rule will allow for the collection of facial biometrics of all aliens at entry and exit. Prior to the effective date of this final rule, most aliens were already subject to photograph at entry; however, some aliens, such as aliens who are under the age of 14 or over the age of 79, were exempt and not required to be photographed at entry or exit. This final rule provides that all aliens, including those previously exempt, may be photographed at entry and exit. U.S. citizens may be photographed at entry and exit under this final rule if they voluntarily participate in biometric collection but retain their ability to opt out of being photographed for the purpose of identity verification using biometric facial comparison. Removing the exemptions for aliens for photographs at entry and exit will allow CBP to further expand the facial comparison technology used for the collection of biometrics and provide for a more complete evaluation as CBP moves toward nationwide expansion. Additionally, this final rule will remove the reference in regulations to pilot programs, eliminate the 15-location pilot program air and sea port limit for conducting biometric collection at exit in the air and sea environments, and include authority for CBP to continue the expansion of biometric collection at exit in the sea and land environments and at entry in the land environment.[180]

Because CBP is still determining the best option for implementing biometric collection at exit in the sea, land, and private aircraft environments or at entry in the land environment for travelers entering in vehicles or private aircraft, the analysis for this final rule will only discuss the costs and benefits of biometric programs that have been established in the air, sea, and land environments. Capturing images using facial comparison technology during biometric collection at entry and exit as a result of this final rule will affect CBP, air travelers, sea travelers, pedestrian land travelers, the air travel industry, and the sea travel industry. The implementation of the facial comparison technology will also improve CBP's security efforts; provide CBP with greater accuracy in determining whether aliens are departing the country when they are required to depart; reduce visa or travel document fraud; and improve CBP's ability to identify criminals and known or suspected terrorists before they enter or depart the United States.

In the analysis for the final rule, CBP considers the effects from the implementation of facial comparison technology used for biometric collection at exit and entry in the commercial air environment and at entry in the sea environment and at entry for pedestrians in the land environment during the 8-year pilot period spanning fiscal years 2017–2024 and the 5-year regulatory period spanning fiscal years 2025–2029. In addition, CBP provides the total costs, cost savings and net costs during both the pilot and regulatory periods to reflect the total cost of these biometric programs as a whole from 2017–2029. CBP has revised the cost and benefit estimates provided in the analysis for the NPRM in response to public comments to include recently available information and data, including costs and benefits attributable to the implementation of Simplified Arrival, FBD, Mobile Primary Face, Pedestrian Entry, and to include the results from the CBP Biometric Air Exit Time and Motion Study (CBP Time and Motion Study).

In this analysis, CBP analyzes the effect of the biometrics program over two time periods: the pilot period and the regulatory period. In the analysis of the pilot period for the NPRM, CBP only identified costs to CBP and outbound air travelers. CBP had expected that during the pilot period, CBP would be solely responsible for the implementation of biometric exit pilot programs, bearing the costs for installing hardware, and staffing biometric exit collection operations. However, the pilot period has lasted long enough that the air travel industry has voluntarily installed facial comparison technology hardware for biometric collection at exit sooner than CBP had anticipated, allowing CBP to provide estimated costs to the air travel industry during the pilot period in the analysis for the final rule. CBP has also added an analysis of the estimated costs and benefits from implementing facial comparison technology in Simplified Arrival in both the air and sea environments, FBD and Mobile Primary Face at entry in the sea environment, and Pedestrian Entry in the land environment during the pilot period in the analysis for the final rule.

CBP, air travelers, pedestrian land travelers, the air travel industry, and the sea travel industry all experienced costs during the pilot period. Costs during the pilot period to CBP included costs to engineer and develop TVS, procure hardware, provide management, operation, support, training, and staffing for the implementation of facial comparison technology at entry and exit in the air environment and at entry in

depending on if the cruise is classified as an open or closed loop cruise. FBD is conducted only for entry processing of closed loop cruise passengers who have passports.

[179] Data provided by CBP's Innovation and Strategy Directorate, Biometrics Program Office, Office of Field Operations, subject matter expert February 18, 2025. CBP implemented Pedestrian entry at all 185 crossings/sites across all 113 land ports of entry.

[180] CBP acknowledges that although this final rule grants authority to CBP to expand biometric collection in these environments, CBP does not have a feasible solution to implement such programs at this time. Additionally, when moving forward with additional large-scale implementation of facial comparison technology for biometric collection at land or sea ports, CBP will publish a notice in the **Federal Register** with information regarding details of implementation and request comments on the newly implemented transportation modalities.

the sea environment. Outbound air travelers affected by the biometric exit pilot program incurred time burden costs when boarding flights conducting biometric exit collection, resulting in slightly longer boarding times per traveler. Inbound pedestrian travelers experienced on average slightly longer processing times as a result of being processed through Pedestrian Entry.[181] The air travel industry voluntarily incurred costs to procure and install their own facial comparison hardware at departure gates to begin conducting biometric collection at exit, time burden costs from longer boarding times per flight causing additional staffing hours, and costs related to training staff, while conducting biometric operations at departure gates. The sea travel industry also incurred costs to procure and install the necessary hardware required to conduct FBD operations at entry in the sea environment and costs related to training staff to conduct FBD operations. CBP estimated that these costs, shown in Table 2, totaled approximately $832 million in undiscounted 2024 U.S. dollars over the course of the pilot period, or on average around $104 million annually.

Cost savings from the implementation of facial comparison technology for biometric collection during the pilot period were experienced by CBP, inbound air travelers processed through Simplified Arrival, inbound sea travelers when processed through Simplified Arrival, FBD or Mobile Primary Face, and sea travel industry members from a swifter debarkation process during FBD. CBP estimates that the cost savings to CBP, inbound air travelers, sea travelers, and the sea travel industry were due to reduced time burdens per traveler as a result of shorter processing times from the use of facial comparison technology at entry. CBP also estimates that the sea travel industry experienced time savings of approximately 1.25 hours per vessel arrival that conducts FBD operations. CBP does not have information available to monetize these time savings but expects the value of these time savings to be significant to sea travel industry members that operate in a very time sensitive business, specifically, when a cruise vessel arrives at a sea port and has to debark passengers, and quickly clean and prepare the vessel for new onboarding passengers and a swift departure. CBP estimated that the total cost savings during the pilot period were approximately $260 million in undiscounted 2024 U.S. dollars, or on average around $15.5 million annually. As shown in Table 2, total net costs from this final rule during the pilot period are estimated to be approximately $572 million in undiscounted 2024 U.S. dollars, or on average $83.8 million annually.[182]

TABLE 2—PILOT PERIOD NET COSTS, 2017–2024

[Undiscounted thousands of 2024 U.S. dollars]

| Fiscal year | Costs | Cost savings | Net costs |
|---|---|---|---|
| 2017 | $91,818 | $0 | $91,818 |
| 2018 | 101,138 | 3,032 | 98,106 |
| 2019 | 124,484 | 12,770 | 111,714 |
| 2020 | 88,828 | 8,437 | 80,391 |
| 2021 | 73,592 | 18,019 | 55,573 |
| 2022 | 115,981 | 50,846 | 65,135 |
| 2023 | 117,240 | 77,355 | 39,885 |
| 2024 | 119,480 | 89,597 | 29,883 |
| Total | 832,562 | 260,057 | 572,505 |

**Note:** totals may not sum due to rounding.

CBP also estimated the effects of implementing facial comparison technology for biometric collection at exit and entry in the commercial air environment and at entry in the sea and land (pedestrians only) environments during the regulatory period. CBP's analysis for the NPRM did not include costs and benefits from the implementation of the Simplified Arrival process, FBD, Mobile Primary Face, or Pedestrian Entry due to lack of data and information available. In this analysis for the final rule, CBP was able to include these costs and benefits from implementing these biometric collection operations using facial comparison technology and the availability of additional data led CBP to revise its estimated costs and benefits for this final rule during the regulatory period.

CBP, outbound air travelers, inbound pedestrians, the air travel industry, and the sea travel industry will experience costs due to this final rule during the regulatory period. During the regulatory period, CBP expects additional costs to CBP will largely consist of the ongoing maintenance and support activities associated with operating TVS. CBP also anticipates that outbound air travelers will incur a minor time burden per traveler when boarding flights conducting facial comparison for biometric collection at exit.[183] CBP expects that inbound pedestrian

[181] CBP notes that the implementation of Pedestrian Entry made the overall entry process in the land environment more efficient. Because of these efficiencies CBP was able to implement changes to the entry process (adding certain functionality and introducing different procedures that the CBP officers have now implemented during the primary inspection process). CBP was unable to separate the two effects and CBP was only able to identify the combined effect on pedestrian entry processing times which CBP estimates resulted in a slightly longer processing time for inbound pedestrian travelers.

[182] Net costs during the pilot period could be less than CBP presents here if the actual time burden to the average outbound air traveler and pedestrian traveler is less than CBP estimates or if it actually results in a time savings. CBP notes that actual costs to air travelers from biometric collection at exit when boarding non-CBP biometric flights and for inbound pedestrian travelers processed through Pedestrian Entry are uncertain. The time burden when boarding non-CBP biometric flights could be less than estimated as COVID–19 restrictions eased, and as boarding agents and travelers became more familiar with the facial comparison technology. At entry in the land environment CBP made changes to the primary inspection entry process for pedestrians after the implementation of facial comparison technology for biometric collection for Pedestrian Entry, which prevented CBP from separating the two effects and CBP was only able to identify the combined effect on pedestrian entry processing times.

[183] CBP notes that the actual time burden incurred during biometric collection at exit for outbound air travelers boarding non-CBP biometric flights could be less than CBP estimates in this analysis as restrictive COVID–19 health requirements ease, as boarding agents and travelers become more familiar with the facial comparison technology in the exit process and if enhancements to technology continue to be implemented making the process more efficient.

travelers on average will experience slightly longer entry processing times when processed through Pedestrian Entry, generating an added time burden as a result of this final rule.[184] The air travel industry will also continue to incur hardware procurement and installation costs until the biometric air exit program is fully implemented nationwide, will incur added time burden costs to boarding agents as a result of longer boarding times per flight when conducting biometric collection at exit and will bear incremental training costs. CBP also expects the sea travel industry to incur costs from procuring additional facial comparison hardware as they continue to expand FBD operations and from training debarkation agents on how to properly conduct FBD operations. As shown in Table 3, CBP estimates the total costs during the regulatory period will be approximately $792 million in undiscounted 2024 U.S. dollars or on average $158.5 million annually.

During the regulatory period CBP expects that CBP, inbound air travelers, and sea travelers will experience cost savings during the entry process from the use of facial comparison technology at Simplified Arrival, FBD, Mobile Primary Face, and Pedestrian Entry. CBP estimates that cost savings to CBP, inbound air, and sea travelers will be approximately $505 million in undiscounted 2024 U.S. dollars or on average $101 million annually during the regulatory period. CBP also anticipates that the sea travel industry will experience time savings during the debarkation process when conducting FBD operations resulting in around 1.25 hours of time savings per vessel arrival. CBP presents net costs for each year of the regulatory period in Table 3, and CBP estimates that total net costs during the regulatory period will be approximately $287 million in undiscounted 2024 U.S. dollars, or on average $57 million annually.[185]

TABLE 3—REGULATORY PERIOD PROJECTED NET COSTS, FY 2025–2029

[Undiscounted thousands of 2024 U.S. dollars]

| Fiscal year | Costs | Cost savings | Net costs |
|---|---|---|---|
| 2025 | $150,718 | $90,232 | $60,485 |
| 2026 | 164,062 | 97,642 | 66,420 |
| 2027 | 156,009 | 102,532 | 53,477 |
| 2028 | 159,360 | 106,033 | 53,327 |
| 2029 | 162,380 | 108,704 | 53,675 |
| Total | 792,528 | 505,144 | 287,385 |
| Average Annual | 158,506 | 101,029 | 57,477 |

**Note:** totals may not sum due to rounding.

The primary benefit of this final rule is the enhanced security from having biometric confirmation using facial comparison technology of the identification of alien travelers entering and leaving the country to prevent imposters attempting to fraudulently enter the United States, identifying individuals who have overstayed their visas, and individuals who have entered the United States without inspection at entry. CBP is unable to monetize these security benefits in the analysis for the final rule. Comparing biometrics at entry and departure enables CBP to know with greater certainty the identity of those entering and leaving the United States, which will help detect and deter visa overstays and visa fraud; helps identify persons attempting to fraudulently use travel documents; and alerts authorities to criminals or known or suspected terrorists prior to entry or exit. For FY 2023, DHS estimates that about 565,155 aliens who entered by air or sea and were expected to depart that year overstayed their lawful period of admission, or 1.45 percent of aliens arriving by air and sea.[186] The implementation of facial comparison technology pilots has already yielded positive security benefits. The facial comparison technology pilots at exit have helped identify over 444,552 visa overstays and 12,669 individuals who previously entered the United States without inspection.[187] Additionally, since 2018, CBP facial comparison technology used at entry has detected over 2,000 imposters at ports of entry, who were using genuine travel documents when attempting to fraudulently enter the United States.[188]

Table 4 presents monetized present value and annualized net costs for the final rule during the regulatory period.[189] CBP estimates total net costs from this final rule will range between around $264 million and $237 million over the regulatory period, using a three and seven percent discount rate. On an annualized basis, net costs will range within $57 million. CBP notes that the actual net costs for this final rule could be less depending on how efficiently the air travel industry and sea travel industry can implement facial

[184] CBP notes that actual time burden to the average inbound pedestrian traveler when processed through Pedestrian Entry is uncertain. CBP made changes to the primary inspection entry process for pedestrians after the implementation of facial comparison technology for biometric collection for Pedestrian Entry, which prevented CBP from separating the two effects and CBP was only able to identify the combined effect on pedestrian entry processing times. Therefore, the actual time burden from implementing Pedestrian Entry could be less than CBP estimates in this final rule.

[185] CBP believes that net costs could be less than presented here due to the uncertainty surrounding the actual time burden incurred by outbound air travelers boarding non-CBP biometric flights and inbound pedestrians processed through Pedestrian Entry. CBP anticipates that the added time burden from conducting biometric collection for outbound air travelers boarding non-CBP biometric flights could be less or even result in a time savings in the future as restrictive COVID–19 health requirements ease, and as boarding agents and the traveling public become more familiar with the biometric collection process, and enhancements to the technology continue to be implemented making the process more efficient. At entry in the land environment CBP made changes to the primary inspection entry process for pedestrians after the implementation of facial comparison technology for biometric collection for Pedestrian Entry, which prevented CBP from separating the two effects and CBP was only able to identify the combined effect on pedestrian entry processing times.

[186] DHS, FY 2023 Entry/Exit Overstay Report 12 (2024), *https://www.dhs.gov/sites/default/files/2024-10/24_1011_CBP-Entry-Exit-Overstay-Report-FY23-Data.pdf* (last visited May 19, 2025).

[187] Information provided by CBP's Strategic Transformation Office, Planning, Program Analysis, and Evaluation, Office of Field Operations, subject matter expert on January 31, 2023, and March 6, 2025.

[188] *See* CBP, Biometrics, *https://www.cbp.gov/travel/biometrics* (last modified April 16, 2025) (last visited May 21, 2025).

[189] CBP displays the net costs associated with only the regulatory period to show the effects of this final rule after it is implemented. The effects incurred during the pilot period are considered sunk costs and cannot be recouped. CBP will also display the net costs for these biometric programs as a whole from 2017–2029.

comparison technology for biometric collection and if the air travel industry is able to speed its processing as it moves past the pandemic environment.[190] CBP notes that the time-in-motion study was conducted during a time with COVID–19 travel restrictions and that those may have lengthened both the baseline inspection process and the biometric inspection process. CBP expects that time burdens from using facial comparison technology for biometric collection at exit in the commercial air environment could have decreased or even became time savings now that COVD–19 restrictions have been lifted, boarding agents and travelers become more familiar with the technology and future enhancements to technology make the process more efficient. Additionally, the actual time burden to inbound pedestrians processed through Pedestrian Entry is somewhat uncertain and CBP anticipates it could be less than CBP presents in this analysis because CBP changed the entry process and policies after Pedestrian Entry was implemented, likely increasing the average entry processing time per inbound pedestrian. If efficiencies are gained over time to make the process less burdensome, net costs from this final rule could be significantly less during the regulatory period. The primary benefit of this final rule is improving CBP's national security efforts by validating the identity of aliens entering and exiting the United States.

TABLE 4—TOTAL MONETIZED PRESENT VALUE AND ANNUALIZED NET COSTS OF REGULATORY PERIOD, 2025–2029

[Thousands of 2024 U.S. dollars]

| | 3% Discount rate | 7% Discount rate |
|---|---|---|
| Present Value Net Cost | $263,951 | $237,148 |
| Annualized Net Cost | 57,635 | 57,838 |

CBP also displays the total effect of this final rule as a whole from 2017–2029. Table 5 below shows the total costs, cost savings, and net costs from the biometric collection programs using facial comparison technology, from 2017–2029 in undiscounted 2024 U.S. dollars. In total CBP estimates that this final rule will result in total costs of around $1,625 million during the entire period of analysis (2017–2029). Average annual costs are estimated to be around $125 million. Total cost savings from this final rule are expected to be around $765 million or on average $59 million annually. CBP anticipates that the total net costs from 2017–2029 will be around $860 million or on average $66 million annually.

TABLE 5—BIOMETRIC PROGRAMS COSTS, COST SAVINGS AND NET COSTS, 2017–2029

[Undiscounted thousands of 2024 U.S. dollars]

| Fiscal year | Costs | Cost savings | Net costs |
|---|---|---|---|
| 2017 | $91,818 | $0 | $91,818 |
| 2018 | 101,138 | 3,032 | 98,106 |
| 2019 | 124,484 | 12,770 | 111,714 |
| 2020 | 88,828 | 8,437 | 80,391 |
| 2021 | 73,592 | 18,019 | 55,573 |
| 2022 | 115,981 | 50,846 | 65,135 |
| 2023 | 117,240 | 77,355 | 39,885 |
| 2024 | 119,480 | 89,597 | 29,883 |
| 2025 | 150,718 | 90,232 | 60,485 |
| 2026 | 164,062 | 97,642 | 66,420 |
| 2027 | 156,009 | 102,532 | 53,477 |
| 2028 | 159,360 | 106,033 | 53,327 |
| 2029 | 162,380 | 108,704 | 53,675 |
| Total | 1,625,090 | 765,201 | 859,890 |
| Average | 125,007 | 58,862 | 66,145 |

CBP also provides the monetized present value and annualized net costs for the final rule during the entire period of analysis (2017–2029) in discounted 2024 U.S. dollars. CBP estimates total net costs from this final rule will range between around $722 million using a three percent discount rate and $587 million using a seven percent discount rate. On an annualized basis, total net costs from this final rule will range from $67 million using a three percent discount rate and $70 million using a seven percent discount rate. In addition to the costs, cost savings and net costs, this final rule provides added national security benefits as discussed above. Table 6, below, displays CBP's estimates for the present value and annualized net costs from this final rule from 2017–2029.

[190] CBP Time and Motion Study, conducted to determine the processing times for biometric collection at exit in the air environment, was conducted in 2021 when airport COVID–19 protocols were still in place. Therefore, CBP's estimates in this analysis for time burdens incurred during the biometric collection process at exit in the air environment may reflect a less efficient process than will occur in future years.

TABLE 6—BIOMETRIC PROGRAMS TOTAL MONETIZED PRESENT VALUE AND ANNUALIZED NET COSTS, 2017–2029

[Thousands of 2024 U.S. dollars]

| | 3% Discount rate | 7% Discount rate |
|---|---|---|
| Present Value Net Cost | $722,151 | $587,300 |
| Annualized Net Cost | 67,904 | 70,271 |

*B. Regulatory Flexibility Act*

The Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121, 110 Stat. 857), requires an agency to prepare and make available to the public a regulatory flexibility analysis (RFA) that describes the effect of a proposed rule on small entities (*i.e.,* small businesses, small organizations, and small governmental jurisdictions) when the agency is required to publish a general notice of proposed rulemaking for a rule.

The Regulatory Flexibility Act requires agencies to consider the impacts of their rules on small entities. This final rule would only directly regulate individual travelers, who are not considered small entities. CBP received a public comment suggesting that individual travelers could be small businesses, sole proprietors, self-employed individuals, and freelancers, therefore a significant number of small entities would be affected as a result of this rule and that warrants a complete RFA for this rule. CBP does not have data on how many international travelers would fall in these categories. However, the effects on individual travelers are not significant. CBP estimates that the time burden to air travelers is less than 4–6 seconds (0.00167 hours) per boarding, or less than $0.12 per individual traveler during the boarding process.[191] Additionally, CBP estimates the average time burden to inbound pedestrians is approximately 15 seconds (0.00417 hours) per entry, or around $0.12 per individual traveler during the entry process.[192] The air travel and sea travel industry are indirectly affected by the final rule as the final rule does not place any requirements on travel industry members, and does not grant them any new rights. Any participation by air travel industry and sea travel industry members is strictly voluntary and CBP expects that air travel industry and sea travel industry members will only participate if they believe the benefits of participation outweigh the costs. CBP therefore certifies that this final rule will not result in a significant economic impact on a substantial number of small entities.

*C. Unfunded Mandates Reform Act of 1995*

This rule will not result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year (adjusted for inflation), and it will not significantly or uniquely affect small governments. Therefore, no actions are necessary under the provisions of the Unfunded Mandates Reform Act of 1995, Public Law 104–4, 109 Stat. 48.

*D. Paperwork Reduction Act*

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3507), an agency may not conduct, and a person is not required to respond to, a collection of information unless the collection of information displays a valid control number assigned by OMB. The collections of information related to this final rule, including biometric exit, Simplified Arrival, FBD, Mobile Primary Face, and Pedestrian Entry are approved by OMB under OMB Control Number 1651–0138. CBP anticipates that this final rule would reduce the overall time burdens incurred by respondents during the information collection for biometric identity verification. The implementation of facial comparison technology for biometric collection is significantly quicker and more efficient than previous processes (*e.g.,* collection of fingerprints). Because facial comparison technology generates a more efficient process, the time burden for an information collection response is expected to decrease.

However, this final rule would also introduce new time burdens to travelers departing the United States and CBP expects that the total number of travelers affected by biometric identity information collection will increase as a result of this final rule. Additionally, as CBP partners with air travel industry members and sea travel industry members, they will also incur some time burdens as a result of this final rule while they facilitate the collection of the biometric identity information. CBP assumes that the new time burden to conduct biometric identity using facial comparison technology is approximately 0.00095 hours (3.42 seconds) based on the CBP Time and Motion Study conducted on facial comparison technology implementation for biometric collection at exit in the air environment. CBP uses this estimate of 3.42 seconds for the average time burden to capture an image by facial comparison technology and conduct the biometric identity verification in all environments.

CBP estimates that the overall total time burden to the public from this information collection will decrease from around 705,336 hours to around 536,583 hours annually. Additionally, CBP anticipates that under this collection the total number of responses and respondents will increase from 115,200,000 to around 414,044,049. This information collection is being revised to reflect a reduction in burden hours and an increased number of travelers affected by facial comparison biometric collection as a result of this final rule. The new information collection requirements for this final rule will result in the following estimated time burdens to the public for information collection under OMB Control Number 1651–0138 from expanding facial comparison technology for biometric identity for each environment below:

Biometric Data Fingerprint in All Environments

*Estimated number of respondents:* 16,587,550.

*No. of reponses per respondent:* 1.

*Total responses:* 16,587,550.

[191] U.S. Department of Transportation, Office of Transportation Policy. *The Value of Travel Time Savings: Departmental Guidance for Conducting Economic Evaluations Revision 2 (2016 Update),* ''Table 4 (Revision 2—2016 Update): Recommended Hourly Values of Travel Time Savings.'' CBP used the Department of Transportation (DOT) hourly wage rate for all-purpose air travelers, adjusted to 2024 values ($65.69) to monetize the potential cost to the individual traveler, during the boarding process.

[192] U.S. Department of Transportation, Office of Transportation Policy. *The Value of Travel Time Savings: Departmental Guidance for Conducting Economic Evaluations Revision 2 (2016 Update),* ''Table 4 (Revision 2—2016 Update): Recommended Hourly Values of Travel Time Savings.'' CBP used the DOT hourly wage rate for all-purpose intercity surface travelers, adjusted to 2024 values ($28.75) to monetize the potential costs to the individual pedestrian traveler during the entry process.

*Estimated time burden per response:* 0.0097 hours (35 seconds).
*Total estimated time burden:* 160,899 hours.

Biometric Exit Air Passenger Travelers

*Estimated number of respondents:* 98,982,807.
*No. of reponses per respondent:* 1.
*Total responses:* 98,982,807.
*Estimated time burden per response:* 0.00095 hours (3.42 seconds).
*Total estimated time burden:* 94,034 hours.

Biometric Exit Air Travel Industry

*Estimated number of respondents:* 98,982,807.
*No. of reponses per respondent:* 1.
*Total responses:* 98,982,807.
*Estimated time burden per response:* 0.00095 hours (3.42 seconds).
*Total estimated time burden:* 94,034 hours.

Simplified Arrival Air Passengers

*Estimated number of respondents:* 116,329,615.
*No. of reponses per respondent:* 1.
*Total responses:* 116,329,615.
*Estimated time burden per response:* 0.00095 hours (3.42 seconds).
*Total estimated time burden:* 110,513 hours.

Simplified Arrival Sea Passengers

*Estimated number of respondents:* 947,878.
*No. of reponses per respondent:* 1.
*Total responses:* 947,878.
*Estimated time burden per response:* 0.00095 hours (3.42 seconds).
*Total estimated time burden:* 900 hours.

Simplified Arrival Sea Crew Members

*Estimated number of respondents:* 365,479.
*No. of reponses per respondent:* 1.
*Total responses:* 365,479.
*Estimated time burden per response:* 0.00095 hours (3.42 seconds).
*Total estimated time burden:* 347 hours.

Facial Biometric Debarkation Passengers

*Estimated number of respondents:* 10,124,005.
*No. of reponses per respondent:* 1.
*Total responses:* 10,124,005.
*Estimated time burden per response:* 0.00095 hours (3.42 seconds).
*Total estimated time burden:* 9,618 hours.

Facial Biometric Debarkation Sea Travel Industry

*Estimated number of respondents:* 10,124,005.
*No. of reponses per respondent:* 1.
*Total responses:* 10,124,005.
*Estimated time burden per response:* 0.00095 hours (3.42 seconds).
*Total estimated time burden:* 9,618 hours.

Mobile Primary Face Sea Crew Members

*Estimated number of respondents:* 378,782.
*No. of reponses per respondent:* 1.
*Total responses:* 378,782.
*Estimated time burden per response:* 0.00095 hours (3.42 seconds).
*Total estimated time burden:* 360 hours.

Pedestrian Entry

*Estimated number of respondents:* 59,221,120.
*No. of reponses per respondent:* 1.
*Total responses:* 59,221,120.
*Estimated time burden per response:* 0.00095 hours (3.42 seconds).
*Total estimated time burden:* 56,260 hours.

*E. Privacy*

CBP will ensure that all legal requirements (*e.g.,* the Privacy Act, section 208 of the E-Government Act, and section 222 of the Homeland Security Act) and applicable policies are adhered to during the implementation of the biometric entry-exit system. All relevant privacy documents regarding the use of biometrics entry-exit technology are publicly available on DHS's Privacy website, *https://www.dhs.gov/privacy.*

CBP retains biographic records for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-immigrant aliens, as provided in the DHS/CBP–007 Border Crossing Information (BCI) SORN.[193] Records associated with a law enforcement action are retained for 75 years as set forth in the DHS/CBP–011 TECS SORN.[194] CBP retains biographic entry and exit records in the Arrival and Departure Information System (ADIS) for lawful permanent residents and non-immigrant aliens, consistent with the DHS/CBP–021 ADIS SORN.[195] Since 2004, CBP has collected biometric information in the form of fingerprints and a facial photograph on entry for in-scope travelers (pursuant to 8 CFR 235.1); CBP has transmitted this information to the DHS OBIM's IDENT, and may transmit this information to its successor information technology system, HART, currently in development, where it is stored and retained for 75 years as provided in the DHS-wide retention schedule for biometric records.[196]

Under CBP's facial comparison-based entry-exit program, CBP's biographic data retention policies remain the same. CBP temporarily retains facial images of non-immigrant aliens and lawful permanent residents for no more than 14 days within Automated Targeting System (ATS)-Unified Passenger Module (UPAX) for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits.[197] However, if the TVS matching service determines that a particular traveler is a U.S. citizen, CBP holds the photo in secure CBP systems for no more than 12 hours after identity verification, in case of an extended system outage, and then deletes it.[198] Photos of all travelers are purged from the TVS cloud matching service within a number of hours, depending on the mode of travel.[199] Photos of in-scope travelers are transferred from ATS–UPAX and retained in IDENT and CBP systems for up to 75 years, consistent with existing CBP records that are housed in IDENT in accordance with the BCI SORN.[200]

CBP is implementing the biometric entry-exit system through the TVS. CBP has issued a number of PIAs for the TVS and earlier traveler verification tests,[201] which outline how CBP will ensure compliance with the DHS Fair Information Practice Principles (FIPPs) [202] as part of the biometric entry-exit system.[203] In November 2018, CBP published the TVS PIA, a revised comprehensive PIA, which, along with the previous versions, examines the privacy impact and mitigation strategies of TVS as it relates to the Privacy Act and the FIPPs. The FIPPs address how information being collected is maintained, used and protected,

[193] 81 FR 89957, 89962 (Dec. 13, 2016).
[194] 73 FR 77778, 77782 (Dec. 19, 2008).
[195] 80 FR 72081 (Nov. 18, 2015).

[196] *See* National Archives and Records Administration, Request for Records Disposition Authority, U.S. Department of Homeland Security, Biometric with Limited Biographical Data (2013), *https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.*
[197] TVS PIA at 21.
[198] TVS PIA at 21 & n.63.
[199] TVA PIA at 21.
[200] *See* TVS PIA at 21.
[201] *See* DHS, DHS/CBP/PIA–056 Traveler Verification Service Related PIAs, *https://www.dhs.gov/publication/departure-information-systems-test* (last visited May 21, 2025).
[202] DHS, The Fair Information Practice Principles, *https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles* (last visited May 21, 2025).
[203] *See, e.g.,* DHS/CBP/PIA–030, Privacy Impact Assessment for the Departure Information Systems Test (2016), *https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-dis%20test-june2016.pdf* (last visited May 21, 2025).

particularly to issues such as security, integrity, sharing of data, use limitation and transparency.[204] The comprehensive TVS PIA provides background information on early test deployments.[205] Additionally, the TVS PIA explains throughout how CBP's use of facial comparison technology complies with privacy requirements at both entry and exit operations in all modes of travel where the technology is currently deployed. The TVS PIA is being updated in accordance with the regulations as revised by this final rule.

*F. National Environmental Policy Act*

DHS and its components analyze final actions to determine whether the National Environmental Policy Act of 1969 (''NEPA''), 42 U.S.C. 4321 *et seq.,* applies to them and, if so, what degree of analysis is required. DHS Directive 023–01, Revision 01, and Instruction Manual 023–01–001–01, Revision 01 (DHS Instruction Manual), establish the policies and procedures that DHS and its components use to comply with NEPA.[206]

NEPA allows Federal agencies to establish categories of actions (''categorical exclusions'') that experience has shown do not, individually or cumulatively, have a significant effect on the human environment and, therefore, do not require an environmental assessment (''EA'') or environmental impact statement (''EIS''). An agency is not required to prepare an EA or EIS for a proposed action ''if the proposed agency action is excluded pursuant to one of the agency's categorical exclusions.'' 42 U.S.C. 4336(a)(2). The Instruction Manual, Appendix A, lists the DHS Categorical Exclusions. For an action to be categorically excluded, the DHS Instruction Manual requires the action to satisfy each of the following three conditions: (1) the entire action clearly fits within one or more of the Categorical Exclusions; (2) the action is not a piece of a larger action; and (3) no extraordinary circumstances exist that would have or could create the potential for a significant environmental effect. DHS Instruction Manual, Section V.B.(1)–(3).

DHS analyzed this final rule and has concluded that the changes to 8 CFR parts 215 and 235 concerning the collection of biometric data from aliens upon entry and departure falls within DHS's categorical exclusion A3. *See* DHS Instruction Manual, Appendix A, Table 1. Categorical exclusion A3 covers, among other things, the promulgation of rules that interpret or amend an existing regulation without changing its environmental impacts. First, the changes to 8 CFR parts 215 and 235 do not result in a change in environmental effect. Second, this final rule is a standalone rule and is not part of any larger action. Third, DHS is not aware of any extraordinary circumstances that would cause a significant environmental impact. Therefore, this final rule is categorically excluded, and no further NEPA analysis or documentation is required.

**List of Subjects**

*8 CFR Part 215*

Administrative practice and procedure, Aliens, Travel restrictions.

*8 CFR Part 235*

Administrative practice and procedure, Aliens, Immigration, Reporting and recordkeeping requirements.

**Regulatory Amendments**

For the reasons discussed in the preamble, DHS is amending 8 CFR parts 215 and 235 as set forth below:

## PART 215—CONTROLS OF ALIENS DEPARTING FROM THE UNITED STATES; ELECTRONIC VISA UPDATE SYSTEM

■ 1. The authority citation for part 215 is revised to read as follows:

**Authority:** 6 U.S.C. 202(4), 236; 8 U.S.C. 1101, 1103, 1104, 1184, 1185 (pursuant to Executive Order 13323, 69 FR 241, 3 CFR, 2003 Comp., p. 278), 1357, 1365a and note, 1365b, 1379, 1731–32; and 8 CFR part 2.

■ 2. Amend § 215.8 as follows:
■ a. Revise the section heading;
■ b. Revise paragraph (a);
■ c. In paragraph (b), add a paragraph heading and revise the first sentence; and
■ d. In paragraph (c), add a paragraph heading.

The revisions and additions read as follows:

**§ 215.8 Requirements for biometrics from aliens on departure from the United States.**

(a) *Photographs and other biometrics*—(1) *Photographs.* DHS may require an alien to be photographed when departing the United States to determine the alien's identity or for other lawful purposes.

(2) *Other biometrics.* DHS may require any alien, other than aliens exempted under paragraph (a)(3) of this section or Canadian citizens under section 101(a)(15)(B) of the Act who were not otherwise required to present a visa or have been issued Form I–94 (see § 1.4 of this chapter) or Form I–95 upon arrival at the United States, to provide other biometrics, documentation of immigration status in the United States, as well as such other evidence as may be requested to determine the alien's identity and whether the alien has properly maintained immigration status while in the United States, when departing the United States.

(3) *Exemptions.* The requirements of paragraph (a)(2) of this section shall not apply to:

(i) Aliens younger than 14 or older than 79 on date of departure;

(ii) Aliens admitted on A–1, A–2, C–3 (except for attendants, servants, or personal employees of accredited officials), G–1, G–2, G–3, G–4, NATO–1, NATO–2, NATO–3, NATO–4, NATO–5, or NATO–6 visas, and certain Taiwan officials who hold E–1 visas and members of their immediate families who hold E–1 visas who are maintaining such status at time of departure, unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (a)(2) of this section;

(iii) Classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or

(iv) An individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply.

(b) *Failure of a non-exempt alien to comply with departure requirements.* An alien who is required to provide biometrics when departing the United States pursuant to paragraph (a)(1) or (2) of this section and who fails to comply with the departure requirements may be found in violation of the terms of the alien's admission, parole, or other immigration status. * * *

(c) *Determination of overstay status.* * * *

[204] DHS, The Fair Information Practice Principles, *https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles* (last visited May 21, 2025).

[205] TVS PIA at 2–3.

[206] DHS, Directive 023–01, Rev. 01, Implementation of the National Environmental Policy Act (2014), available at *https://www.dhs.gov/sites/default/files/publications/mgmt/environmental-management/mgmt-dir_023-01-implementation-national-environmental-policy-act_revision-01.pdf* (last visited May 21, 2025); DHS, Instruction Manual 023–01–001–01, Rev. 01, Implementation of the National Environmental Policy Act (NEPA) (2014) (DHS Instruction Manual), available at *https://www.dhs.gov/sites/default/files/publications/mgmt/environmental-management/mgmt-dir_023-01-implementation-national-environmental-policy-act_revision-01.pdf* (last visited May 21, 2025).

## PART 235—INSPECTIONS OF PERSONS APPLYING FOR ADMISSION

■ 3. The authority citation for part 235 is revised to read as follows:

**Authority:** 6 U.S.C. 218 and note; 8 U.S.C. 1101 and note, 1103, 11f58, 1182, 1183, 1185 (pursuant to Executive Order 13323, 69 FR 241, 3 CFR, 2003 Comp., p. 278), 1185 note, 1201, 1224, 1225, 1226, 1228, 1357, 1365a and note, 1365b, 1379, 1731–32; 48 U.S.C. 1806 and note, 1807, and 1808 and 48 U.S.C. 1806 notes (title VII, Pub. L. 110–229, 122 Stat. 754); 8 U.S.C. 1185 note (sec. 7209, Pub. L. 108–458, 118 Stat. 3638, and Pub. L. 112–54, 125 Stat. 550).

■ 4. Amend § 235.1 by revising paragraph (f)(1) to read as follows:

### § 235.1 Scope of examination.

* * * * *

(f) *Alien applicants for admission*—(1) *Requirements for admission.* Each alien seeking admission at a United States port-of-entry must present whatever documents are required and must establish to the satisfaction of the inspecting officer that the alien is not subject to removal under the immigration laws, Executive Orders, or Presidential Proclamations, and is entitled, under all of the applicable provisions of the immigration laws and this chapter, to enter the United States.

(i) *Permanent residents.* A person claiming to have been lawfully admitted for permanent residence must establish that fact to the satisfaction of the inspecting officer and must present proper documents in accordance with § 211.1 of this chapter.

(ii) *Photographs.* DHS may require an alien seeking admission to be photographed to determine the alien's identity or for other lawful purposes.

(iii) *Other biometrics.* DHS may require any alien, other than aliens exempted under paragraph (f)(1)(vi) of this section or Canadian citizens under section 101(a)(15)(B) of the Act who are not otherwise required to present a visa or be issued Form I–94 (see § 1.4 of this chapter) or Form I–95 for admission or parole into the United States, to provide other biometrics, documentation of immigration status in the United States, as well as such other evidence as may be requested to determine the alien's identity and admissibility and/or whether the alien has properly maintained immigration status while in the United States.

(iv) *Failure to comply with biometric requirements.* The failure of an alien at the time of inspection to comply with paragraph (f)(1)(ii) or (iii) of this section may result in a determination that the alien is inadmissible under section 212(a) of the Immigration and Nationality Act or any other law.

(v) *Biometric requirements upon departure.* Aliens who are required under paragraphs (f)(1)(ii) or (iii) of this section to provide biometrics at inspection may also be subject to the departure requirements for biometrics contained in § 215.8 of this chapter, unless otherwise exempted.

(vi) *Exemptions.* The requirements of paragraph (f)(1)(iii) of this section shall not apply to:

(A) Aliens younger than 14 or older than 79 on the date of admission;

(B) Aliens admitted on A–1, A–2, C–3 (except for attendants, servants, or personal employees of accredited officials), G–1, G–2, G–3, G–4, NATO–1, NATO–2, NATO–3, NATO–4, NATO–5, or NATO–6 visas, and certain Taiwan officials who hold E–1 visas and members of their immediate families who hold E–1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (f)(1)(iii);

(C) Classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or

(D) An individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply.

* * * * *

**Kristi Noem,**

*Secretary of Homeland Security.*

[FR Doc. 2025–19655 Filed 10–24–25; 8:45 am]

BILLING CODE 9111–14–P

# FEDERAL REGISTER

Vol. 90 Monday,

No. 205 October 27, 2025


Part III

## Federal Communications Commission

47 CFR Parts 0, 1, and 43

Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Final Rule

## FEDERAL COMMUNICATIONS COMMISSION

**47 CFR Parts 0, 1, and 43**

**[OI Docket No. 24–523, MD Docket No. 24–524; FCC 25–49; FR ID 311064]**

## Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks

**AGENCY:** Federal Communications Commission.

**ACTION:** Final rule.

**SUMMARY:** In this document, the Federal Communications Commission (Commission or FCC) adopted a *Report and Order* that updates the Commission's submarine cable licensing process and adopts rule changes to protect critical U.S. communications infrastructure against foreign adversary threats, specifically those posed by an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. The *Report and Order* adopts a requirement for certain licensees to file an annual report about the licensee, submarine cable system ownership, and submarine cable operations. The *Report and Order* adopts a one-time information collection for licensees to identify, among other things, how many entities currently own or operate submarine line terminal equipment (SLTEs) on existing licensed cable systems. The *Report and Order* also requires applicants and licensees to certify that they have created, updated, and implemented a cybersecurity and physical security risk management plan and requires applicants to certify that the submarine cable system will not use equipment or services identified on the Commission's Covered List. With respect to the circuit capacity data collection, the *Report and Order* adopts streamlined rules and eliminates the requirement for licensees to file a cable operator report about the capacity on a cable and clarify the types of capacity that need to be reported on an annual basis.

**DATES:** These rules are effective November 26, 2025, except for amendatory instructions 6 (§ 1.767), 7 (§ 1.768), 10 (§ 1.70002), 11 (§ 1.70003), 12 (§§ 1.70005 and 1.70006), 13 (§ 1.70007), 14 (§§ 1.70008 and 1.70009), 15 (§§ 1.70011 through 1.70013), 16 (§ 1.70016), 17 (§ 1.70017), 18 (§ 1.70020), 19 (§§ 1.70023 and 1.70024), and 22 (§ 43.82), which are indefinitely delayed. The One-Time Information Collection will also be indefinitely delayed. The Commission will publish a document in the **Federal Register** announcing the effective date of these rule sections and the One-Time Information Collection.

**FOR FURTHER INFORMATION CONTACT:** Desiree Hanssen, Office of International Affairs, Telecommunications and Analysis Division, at *desiree.hanssen@fcc.gov* or at (202) 418–0887. For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, contact Cathy Williams at 202–418–2918 or *Cathy.Williams@fcc.gov,* or send an email to *PRA@fcc.gov.*

**SUPPLEMENTARY INFORMATION:** This is a summary of the Commission's *Report and Order,* in OI Docket No. 24–523 and MD Docket No. 24–524; FCC 25–49, adopted on August 7, 2025 and released on August 13, 2025. The full text of this document is available online at *https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf.* The full text of this document is also available for inspection and copying during business hours in the FCC Reference Center, 45 L Street NE, Washington, DC 20554. To request materials in accessible formats for people with disabilities, send an email to *FCC504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice), 202–418–0432 (TTY).

### Synopsis

### I. Introduction

1. In this item, we modernize and streamline the Commission's submarine cable rules to facilitate faster and more efficient deployment of submarine cables, while at the same time ensuring the security and resilience of this critical infrastructure. We recognize that investment in such infrastructure is vital to American prosperity and economic dynamism. The rules that we adopt today will ensure that the United States remains ready and able to deploy submarine cable infrastructure with increasing amounts of capacity to meet current and future internet and data demands so that the United States remains ''the unrivaled world leader in critical and emerging technologies—such as artificial intelligence.'' With global competition for submarine cables increasing, connections to the United States should continue to be at the forefront of the submarine cable marketplace. Nonetheless, ''[i]nvestment at all costs is not always in the national interest,'' because of the potential for foreign adversary exploitation. We also recognize that ''[e]conomic security is national security,'' and thus protecting our communications networks against foreign threats is crucial. With these principles in mind today, we undertake the first major comprehensive update of our submarine cable rules since 2001. Since that time, technology, consumer expectations, international submarine cable traffic patterns, submarine cable infrastructure, and the foreign threat landscape have changed greatly.

2. To advance the Commission's comprehensive strategy to build a more secure and resilient communications supply chain, we adopt rules that place a strong emphasis on preventing and mitigating national security risks from foreign adversaries, while welcoming investment from United States allies and partners. We also lighten the regulatory burden on industry by modernizing and simplifying the submarine cable license approval process.

3. In this *Report and Order,* we take action to protect the security, integrity, and resilience of submarine cable systems by targeting foreign adversary threats to this critical U.S. communications infrastructure. Specifically, we adopt a clear and consistent standard that incorporates the Department of Commerce's definitions for identifying a ''foreign adversary,'' ''foreign adversary country,'' and an individual or entity ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.'' Using these definitions, we adopt rules that will better protect U.S. national security and critical U.S. communications infrastructure from foreign adversaries.

4. We update the Commission's submarine cable licensing process to protect critical U.S. communications infrastructure against foreign adversary threats. Specifically, we adopt a presumption that will preclude the grant of applications filed by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; any entity identified on the Commission's ''Covered List''; [1] and/or

[1] Pursuant to sections 2(a) and (d) of the Secure and Trusted Communications Networks Act, and §§ 1.50002 and 1.50003 of the Commission's rules, the Public Safety and Homeland Security Bureau (PSHSB) publishes a list of communications equipment and services that have been determined by one of the sources specified in that statute to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons (''covered'' equipment and services). *See* Secure and Trusted Communications Networks Act of 2019, Public Law 116–124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. 1601–1609 (Secure Networks Act); *see also* 47 CFR 1.50002–1.50003; Federal Communications Commission, *List of Equipment and Services Covered by Section 2 of the Secure Networks Act, https://www.fcc.gov/supplychain/coveredlist* (last updated June 5, 2025) (*List of Covered Equipment*

any entity whose authorization, license, or other Commission approval, whether or not related to operation of a submarine cable, was denied or revoked and/or terminated or is denied or revoked and/or terminated in the future on national security and law enforcement grounds, as well as the current and future affiliates or subsidiaries of any such entity. To ensure that applicants have the requisite character qualifications, we adopt a character presumptive disqualifying condition that an applicant is not qualified to hold a cable landing license if it meets certain criteria. We adopt a presumption that denial of an application is warranted where an applicant seeks to land a submarine cable in a foreign adversary country. Additionally, we adopt a condition prohibiting cable landing licensees from entering into a new or extension of an existing arrangement for Indefeasible Rights of Use (IRU) or leases for capacity where such arrangements would give an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, the ability to install, own, or manage Submarine Line Terminal Equipment (SLTE) on a submarine cable landing in the United States. For current licensees that meet the presumptive disqualifying criteria or whose cable lands in a foreign adversary country, we adopt a tool for increased oversight. We require these licensees to file an annual report (Foreign Adversary Annual Report) containing information about the licensee, submarine cable system ownership, and submarine cable operations. We also adopt a written hearing process to take action to deny or revoke and/or terminate a cable landing license and a process to address a cable landing license or a licensee that is insolvent or no longer exists.

5. We modernize our submarine cable rules by adopting a definition of the term, ''submarine cable system,'' that acknowledges the range of technological advancement in existing submarine cable systems. This definition incorporates the future technological evolution of submarine cable systems, all of which include SLTE as a significant component of the system itself. While at this time we decline to require SLTE owners and operators to become licensees, we take steps to identify, through a one-time information collection, how many entities currently own or operate SLTEs on existing licensed cable systems. The one-time information collection we adopt will further inform the Commission about the identities of SLTE owners and operators and their role in operating a portion of the submarine cable system, including information about system capacity, spectrum, or the lighting of a fiber. The one-time collection will also assess for insolvent cables or licensees, and require licensees to disclose whether or not their submarine cable systems use covered equipment or services. Importantly, this one-time information collection will inform our proposed regulatory approach to SLTEs as discussed in the *Further Notice of Proposed Rulemaking.*

6. We also codify the Commission's longstanding practice of requiring a cable landing license for submarine cables that lie partially outside of U.S. territorial waters. Moreover, while we do retain a number of our current rules, we eliminate the requirement that entities that solely own, and do not control, a U.S. cable landing station must be applicants for, and licensees on, a cable landing license. We update our application rules to require a statement that grant of the application is in the public interest, and require applicants to provide detailed information about the submarine cable system and to report whether or not they use and/or will use third-party foreign adversary service providers in the operation of the submarine cable. We also require applicants and licensees to certify that they have created, updated, and implemented a cybersecurity and physical security risk management plan and will take reasonable measures to protect their systems and services from cybersecurity and physical security risks that could affect their provision of communications services through the submarine cable system. Additionally, applicants for a cable landing license are required to certify that the submarine cable system will not use equipment or services identified on the Commission's Covered List. These rules will ensure that licensees will protect their networks from cybersecurity and physical security threats and threats from foreign adversaries. Finally, to make it easier for applicants and licensees to navigate our rules, we clarify and update the rules for applications to modify, assign, transfer control of, or renew or extend a cable landing license or request special temporary authority. We adopt rules to obligate licensees to keep the Commission abreast of changes to important information such as the contact information of the licensee and other information that will enable the Commission to maintain accurate records regarding licensees.

7. With respect to the circuit capacity data collection, we streamline our rules and eliminate the requirement for licensees to file a Cable Operator Report about the capacity on a cable and clarify the types of capacity that need to be reported on an annual basis. Instead, we require licensees and common carriers to report their capacity on domestic and international cables in a single report, the Capacity Holder Reports—a report filed by each Filing Entity on an individual basis—that will enable the Commission to continue collecting accurate and important data for national security and public safety purposes. Importantly, consistent with other actions, we require cable landing licensees and common carriers to provide certain information about their SLTEs in the Capacity Holder Report.

8. In short, we ''maintain[ ] the strong, open investment environment that benefits our economy and our people, while enhancing our ability to protect the United States from new and evolving threats'' in the submarine cable ecosystem.

## II. Background

9. In November 2024, the Commission adopted the *2024 Cable NPRM,* 88 FR 50486, August 1, 2023, initiating a comprehensive review of the submarine cable rules to develop forward-looking rules to better protect submarine cables, identify and mitigate harms affecting national security and law enforcement, and facilitate the deployment of submarine cables and capacity to the market. As explained in the *2024 Cable NPRM,* the Commission's authority to grant, withhold, revoke, or condition submarine cable landing licenses derives from the Cable Landing License Act and Executive Order 10530. The Commission discussed in detail its rules and coordination of applications with the Executive Branch agencies, including the Committee, to assess applicants and licensees for assessment of any national security, law enforcement, foreign policy, and/or trade policy concerns. The Commission also discussed the existing procedures by which it coordinates with the State Department on all submarine cable applications and obtains approval of any proposed grant of an application or revocation of a cable landing license pursuant to the Cable Landing License Act and Executive Order 10530.

*and Services*). PSHSB added the latest entry to the Covered Equipment or Services list on July 23, 2024. *Public Safety and Homeland Security Bureau Announces Update to List of Covered Equipment and Services Pursuant to Section 2 of the Secure Network* Act, WC Docket No. 18–89 et al., Public Notice, 39 FCC Rcd 8395 (PSHSB July 23, 2024) (*2024 Covered List PSHSB Public Notice*), *https://docs.fcc.gov/public/attachments/DA-24-712A1_Rcd.pdf.*

10. *Recent Commission Actions Regarding National Security.* The Commission has recognized that national security is built on both protecting the nation's communications infrastructure from foreign adversary threats and promoting the prosperity and robustness of the communications sector. The Commission in its recent rulemaking proceedings and actions is continuing its ongoing efforts to secure and protect communications networks from foreign adversaries, while recognizing that investment in U.S. communications networks bolsters national security. In December 2024, the Commission engaged with stakeholders in light of U.S. government confirmed reports that state-sponsored foreign actors tied to the People's Republic of China (PRC) infiltrated at least eight U.S. communications companies in a massive espionage effort, an incident known as Salt Typhoon. The Commission has continued to remain vigilant against this and other foreign adversary cyberthreats.

11. Earlier this year, shortly after President Trump announced in February 2025 the America First Investment Policy, which states that ''[e]conomic security is national security'' and discusses the need to limit certain investments in strategic sectors by six identified foreign adversaries, the Commission initiated a series of actions. In March 2025, the Commission responded to threats posed by the People's Republic of China and to the evolving threat environment more generally, by establishing a Council for National Security to bring together the Commission's regulatory, investigatory, and enforcement authorities to counter foreign adversaries. The Council was established with a three-part goal: ''(1) Reduce the American technology and telecommunications sectors' trade and supply chain dependencies on foreign adversaries; (2) Mitigate America's vulnerabilities to cyberattacks, espionage, and surveillance by foreign adversaries; and (3) Ensure the U.S. wins the strategic competition with China over critical technologies, such as 5G and 6G, AI, satellites and space, quantum computing, robotics and autonomous systems, and the Internet of Things.'' In the same month, the Commission opened a separate proceeding, the *Delete, Delete, Delete* proceeding, with an aim to remove outdated and unnecessary regulations to clear away obstacles to investment.

12. On May 22, 2025, the Commission took action in two distinct proceedings to protect our nation's communications infrastructure from foreign adversary threats. First, in the *Equipment Authorization Report and Order and FNPRM,* the Commission adopted new rules to help ensure that the telecommunication certification bodies (TCBs), measurement facilities (test labs), and laboratory accreditation bodies that participate in our equipment authorization program are not subject to ownership, direction, or control by untrustworthy actors, including foreign adversaries, that pose a risk to national security. The *Equipment Authorization Report and Order* prohibits Commission recognition of any TCB, test lab, or laboratory accreditation body owned by, controlled by, or subject to the direction of a prohibited entity, and prohibits such TCBs, test labs, and laboratory accreditation bodies from participating in the Commission's equipment authorization program.

13. Second, in the *Foreign Adversary NPRM,* the Commission proposed to adopt certification and information collection requirements that would fill gaps in the Commission's existing rules and give the Commission, and the public, a new and comprehensive view of threats from foreign adversaries in the communications sector. Specifically, the Commission proposed to apply new certification and disclosure requirements on entities holding every type of license, permit, or authorization, rather than only certain specific licenses, and to go beyond foreign adversary ownership to also cover all regulated entities controlled by or subject to the jurisdiction or direction of a foreign adversary. The Commission stated that, by focusing on foreign adversary ownership or control, rather than foreign influence more broadly, the proposed rules are tailored to avoid needless burden on regulated entities.

14. *2024 Cable NPRM.* On November 22, 2024, the Commission adopted the *2024 Cable NPRM,* which initiated the first major review of the submarine cable rules since 2001, and sought comment on how best to improve and streamline the rules to facilitate efficient deployment of submarine cables while ensuring the security, resilience, and protection of this critical infrastructure. Among other things, the Commission sought comment on codifying the scope of the Commission's licensing requirements under the Cable Landing License Act and Executive Order 10530 and other legal requirements, improving the Commission's oversight of submarine cable landing licenses, and adopting targeted requirements to protect submarine cables from national security and law enforcement risks. The Commission further sought comment on streamlining procedures to expedite submarine cable review processes and improving the quality of the circuit capacity data and facilitating the sharing of such information with other federal agencies. To address evolving national security, law enforcement, and other risks, the Commission sought comment on updating application requirements for national security purposes and ensuring the Commission has targeted and granular information regarding the ownership, control, and use of a submarine cable system, adopting new compliance certifications, and on any additional steps the Commission can take to protect this critical infrastructure, including activities in coordination with other federal agencies.

15. Earlier this year, the Commission received 18 comments, nine reply comments, and several ex partes pertaining to a wide range of topics discussed in the *2024 Cable NPRM.* Several commenters supported the proposal to codify a definition of a submarine cable system in the Commission's rules. Some commenters offered reservations about potentially duplicative requirements between the proposed periodic reporting, which sought updated ownership and other information, and similar requirements in mitigation agreements with the Committee, as well as concerns about requiring SLTE owners and operators to be licensees. Other commenters offered generally critical views about the proposal to lower the ownership threshold for reportable interests from 10% to 5%, with some further refinements suggested. Some commenters expressed reservations about including capacity holders or IRU holders and lessees under a licensing requirement. Meanwhile, several commenters supported the effort to streamline applications and offered recommendations. As explained below, we have considered these and other comments in the thorough record received and either take action today or seek additional comment.

## III. Report and Order

16. We adopt rules that streamline, modernize, and enhance investment in submarine cable infrastructure, while protecting this critical infrastructure against foreign adversaries in an evolving threat environment. In recent actions, the Commission has taken concrete steps to identify and halt foreign adversaries from participating in U.S. communications markets and supply chains. Our rules take similar steps for submarine cables while reducing regulatory burdens.

*A. Foreign Adversary Rules*

17. We take action to protect the security, integrity, and resilience of the nation's critical infrastructure by adopting proposals to implement certain information requirements, certification requirements, conditions, and prohibitions that will enable the Commission to identify and mitigate foreign adversary threats, as discussed below. We adopt a modified and tailored version of the Commission's proposals by simplifying and providing a clear and consistent standard that incorporates the Department of Commerce's definitions for identifying a ''foreign adversary,'' ''foreign adversary country,'' and ''[p]erson owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.'' Our approach is aligned with long-standing interagency rules and regulations, pursuant to Executive Order 13873, to identify and mitigate foreign adversary threats to U.S. critical infrastructure, including exploitation through individuals and entities owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. This approach is further supported by the record. For example, FDD states that the Commission should prohibit entities subject to the jurisdiction, direction, or control of a foreign adversary from owning submarine cables connected to the United States. The Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (Committee) also supports the Commission relying on the Department of Commerce's determinations and definitions in its efforts to mitigate threats to submarine cable infrastructure presented, such as prohibiting the use of such vendors for equipment or services.

1. Foreign Adversary Definition

18. *Foreign Adversary.* We define ''foreign adversary'' consistent with the Department of Commerce's rule, 15 CFR 791.2, which defines ''foreign adversary'' as ''any foreign government or foreign non-government person determined by the Secretary to 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 United States persons.''

19. In identifying foreign adversaries for the purposes of implementing the rules we adopt today, we follow the Department of Commerce's determinations. Currently, the Department of Commerce's rule, 15 CFR 791.4(a), identifies the following ''foreign governments or foreign non-government persons'' as ''foreign adversaries'': (1) The People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region (China); (2) Republic of Cuba (Cuba); (3) Islamic Republic of Iran (Iran); (4) Democratic People's Republic of Korea (North Korea); (5) Russian Federation (Russia); and (6) Venezuelan politician Nicolás Maduro (Maduro Regime). For purposes of the submarine cable rules, we define ''foreign adversary'' to include the foreign governments and foreign non-government persons identified in 15 CFR 791.4(a), including the Maduro Regime.

20. *Foreign Adversary Country.* In this *Report and Order,* our use of the term ''foreign adversary country'' incorporates the meaning of the Department of Commerce's rule, 15 CFR 791.4, which specifically identifies ''foreign governments or foreign non-government persons'' (in lieu of ''countries'') as ''constitut[ing] foreign adversaries.'' For purposes of the submarine cable rules, we define ''foreign adversary country'' to include both the foreign governments identified as foreign adversaries in 15 CFR 791.4, and countries controlled by a foreign adversary (including foreign non-government persons) identified in 15 CFR 791.4. For example, we will apply any reference to ''a government organization of a foreign adversary country'' to include the Maduro Regime. Further, we will apply the term ''foreign adversary country'' to include Venezuela as a country controlled by a foreign adversary identified in 15 CFR 791.4.

21. *Owned By, Controlled By, or Subject to the Jurisdiction or Direction of a Foreign Adversary.* For purposes of the submarine cable rules, we define an individual or entity ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'' consistent with Department of Commerce's rule, 15 CFR 791.2, with certain narrow modifications. Specifically, we define ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'' to apply to:

(1) Any individual or entity, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of an individual or entity whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary;

(2) Any individual, wherever located, who is a citizen of a foreign adversary or a country controlled by a foreign adversary, and is not a United States citizen or permanent resident of the United States;

(3) Any entity, including a corporation, partnership, association, or other organization, that has a principal place of business in, or is headquartered in, incorporated in, or otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary; or

(4) Any entity, including a corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs (1) through (3) of this section possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority (10% or greater) of the total outstanding voting interest and/or equity interest, or through a controlling interest, in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity.

22. In the *2024 Cable NPRM,* the Commission proposed similar language with the term ''influence.'' However, we adopt here a clearer and narrower version of the proposal to align with other recent Commission actions. Moreover, our adopted approach is also aligned with interagency national security regulations deriving from President Trump's Executive Order 13873, covering the closely related matter of ''Securing the Information and Communications Technology and Services Supply Chain.'' We also recognize that industry has recommended and prefers clear lines and directions rather than ambiguous and potentially capacious terminology. After all, while every major global company is ''subject to the influence'' of the government of the People's Republic of China, including many prominent cable landing licensees, not all companies may be subject to a degree of influence such that they threaten national security and law enforcement interests. While we wish to sweep broadly enough to cover private entities subject to multi-faceted forms of foreign adversary control, we do not desire or intend a scope as broad as ''subject to the influence'' by itself implies.

23. Our approach is also recommended by the Committee, whose expertise the Commission frequently

seeks on national security matters, and others. The Heritage Foundation, for example, states that, ''the Commission could adopt the phrasing 'persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,' as has been recommended by other commenters.'' Horizon Advisory also references 15 CFR 791.2, stating that ''[a] practical approach to start in the right direction would be to apply the US Commerce Department's definition of 'person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary' for defining restrictions.''

24. Importantly, our rule will also assess private entities that are operating in foreign adversary countries. Some entities that are '' 'ostensibly private and civilian' '' may '' 'directly support China's military, intelligence, and security apparatuses and aid in their development and modernization.' '' Horizon Advisory stresses that ''no Chinese company is private in any traditional sense,'' adding that ''[a]s the Chinese government refines its use and messaging around authorities like the National Security Law, the Anti-Espionage Law, and the Personal Information Protection Law, any firm operating in China is at risk of official influence that belies traditional conceptions of a private company.'' Recently, the Supreme Court unanimously accepted findings that a privately held company that has operations in China ''is subject to Chinese laws that require it to 'assist or cooperate' with the Chinese Government's 'intelligence work' and to ensure that the Chinese Government has the power to access and control private data the company holds.''

25. We note that the Commission's rules recognize that ''[b]ecause the issue of control inherently involves issues of fact, it must be determined on a case-by-case basis and may vary with the circumstances presented by each case.'' While we include factors indicative of control in our definition of ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,'' a determination of control is not limited to these factors. The Commission will consider the totality of the circumstances reflected in the record.

26. We make certain modifications from the Department of Commerce's definition to appropriately tailor the Commission's definition and clearly define terms for purposes of the submarine cable rules, including the disclosure requirements and conditions adopted herein. *First,* we use the specific terms ''individual'' and/or ''entity'' to clarify the applicability of each subpart of the definition. *Second,* our definition of an individual ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,'' does not include a resident of a foreign adversary country.

27. *Finally,* we define ''that is owned . . . by a foreign adversary'' in subpart (4) to include both voting and equity interests, as well as controlling interests, and also define the term ''dominant minority'' in subpart (4) as 10% or greater direct or indirect voting and/or equity interests. We find that this ownership threshold is consistent with the Commission's consideration of the ownership threshold of concern in the *2024 Cable NPRM* and our rules requiring disclosure of such ownership information in submarine cable applications. Our approach is also consistent with Commission precedent and recent actions in other proceedings related to the ownership threshold that we adopted or proposed to adopt to determine foreign adversary ownership or control. The Commission has found that an individual or entity may exert direction or control, or significant influence, over a subject entity even without holding a majority of the equity and/or voting interests and that ownership interests as low as five and ten percent are relevant to protecting national security by identifying foreign adversary involvement in a licensee.

2. Foreign Adversary Presumptive Disqualifying Condition

28. To protect the security, integrity, and resilience of this critical U.S. communications infrastructure against national security, law enforcement, and other threats, we adopt a presumption that a foreign adversary applicant, as further described below, is not qualified to hold a cable landing license unless the applicant overcomes the adverse presumption. No commenter opposes the Commission's proposals. We find that adopting this presumptive disqualifying condition is consistent with the Commission's authority to withhold cable landing licenses and condition the grant of licenses to ''promote the security of the United States'' under the Cable Landing License Act and Executive Order 10530, and will protect this critical submarine cable infrastructure and help ensure that it is secure from foreign adversaries and entities identified on the Commission's Covered List.

29. Specifically, the disqualifying condition will presumptively preclude the grant of a submarine cable application filed by any applicant:

(1) That is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g);

(2) That is identified on the Covered List that the Commission maintains pursuant to the Secure Networks Act; and/or

(3) Whose authorization, license, or other Commission approval, whether or not related to operation of a submarine cable, was denied or revoked and/or terminated or is denied or revoked and/or terminated in the future on national security and law enforcement grounds, as well as the current and future affiliates or subsidiaries of any such entity.

30. We will apply this presumptive disqualifying condition to: (1) any initial application for a cable landing license that is filed after the effective date of the *Report and Order,* and (2) all other types of submarine cable applications—including an application for modification, assignment, transfer of control, or renewal or extension of a cable landing license—that are filed after the effective date of the *Report and Order* by a licensee whose initial application for a cable landing license is granted after the effective date of the *Report and Order* or by an existing licensee that currently does not exhibit (prior to the effective date of the *Report and Order*) any of the aforementioned criteria set out in the disqualifying condition. In this *Report and Order,* we use the term ''existing licensees'' to refer to a cable landing licensee whose license was or is granted prior to the effective date of the *Report and Order* or the new rules, as applicable and discussed herein. An applicant can overcome this adverse presumption only by establishing through clear and convincing evidence that the applicant does not fall within the scope of the adverse presumption, as described above, or that grant of the application would not pose risks to national security or that the national security benefits of granting the application would substantially outweigh any risks. Given our adoption of this presumption is necessitated by national security threats to critical U.S. communications infrastructure presented by untrustworthy actors, including foreign adversaries, we find it is appropriate and justified to apply a clear and convincing evidence standard to overcome the adverse presumption rather than NASCA's recommendation to apply a standard for rebutting a presumption that considers licensing conditions and other safeguards. We will exercise our discretion to exclude such applications from referral to the

Executive Branch agencies. We address below the process that will apply where the Commission considers whether denial of a submarine cable application is warranted. If an applicant fails to overcome any of the criteria in the presumptive disqualifying condition, we will find that denial of the application is warranted to promote the security of the United States and we will deny the application.

31. To the extent an application for modification, assignment, transfer of control, or renewal or extension of a cable landing license is filed after the effective date of the *Report and Order* by existing licensees that currently exhibit (prior to the effective date of the *Report and Order*) any of the criteria set out in the presumptive disqualifying condition, instead of applying the presumption, we will refer those applications to the Executive Branch agencies, irrespective of whether the applicant has reportable foreign ownership.

32. Importantly, we will presume that denial of an application as specified herein is warranted where it is filed by any applicant that is subject to any of the aforementioned criteria. *First,* foreign adversaries are deemed to present a national security threat that undermines the security, integrity, and resilience of critical submarine cable infrastructure and the national security interests of the United States. Entities subject to foreign adversary ownership, control, jurisdiction, or direction are identified through the application process, or through the Commission's Covered List, or by Commission action. *Second,* entities identified on the Commission's Covered List have been found to produce or provide equipment and services that have been deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. *Third,* we conclude that the Commission's determinations in denial and revocation and/or termination proceedings concerning any regulated activity are directly relevant to the determination as to whether denial of a submarine cable application by an affected entity or its current and future affiliates and subsidiaries would ''promote the security of the United States.''

33. For example, the presumptive disqualifying condition will apply to any initial application for a cable landing license filed by China Mobile International (USA) Inc. (China Mobile USA), China Telecom (Americas) Corporation (CTA), China Unicom (Americas) Operations Limited (CUA), Pacific Networks Corp. (Pacific Networks), and ComNet (USA) LLC (ComNet) and their current and future affiliates and subsidiaries. In the *China Telecom Americas Order on Revocation and Termination, China Unicom Americas Order on Revocation,* and *Pacific Networks and ComNet Order on Revocation and Termination,* the Commission extensively evaluated national security and law enforcement concerns and determined, based on thorough record development, that each entity is ''subject to exploitation, influence, and control by the Chinese government and is highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight.'' In the *China Mobile USA Order,* the Commission found that the entity is ''vulnerable to exploitation, influence, and control by the Chinese government'' and there is a significant risk that the Chinese government would use the entity ''to conduct activities that would seriously jeopardize the national security interests and law enforcement activities of the United States.''

3. Character Presumptive Disqualifying Condition

34. Today, we adopt a standard by which the Commission will consider whether an applicant seeking a cable landing license or modification, assignment, transfer of control, or renewal or extension of a cable landing license has the requisite character qualifications. To ensure that applicants have the requisite character qualifications, we adopt a presumption that an applicant is not qualified to hold a cable landing license if it meets any of the criteria listed below, unless the applicant overcomes the adverse presumption. This presumption will supplement the foreign adversary presumptive disqualifying condition and codifies a narrower application of the longstanding Commission practice of considering the character qualifications of applicants for submarine cable applications.

35. We presume an applicant does not possess the requisite character qualifications to become a cable landing licensee if the applicant has within the last 20 years:

(1) Materially violated the Cable Landing License Act where the violation (a) was not remediated with an adjudication involving a consent decree and/or compliance plan, (b) resulted in a loss of Commission license or authorization, or (c) was found by the Commission to be intentional;

(2) Committed national security-related violations of the Communications Act or Commission rules as identified in Commission orders, including but not limited to violations of rules concerning the Covered List that the Commission maintains pursuant to the Secure Networks Act;

(3) Made materially false statements or engaged in fraudulent conduct concerning national security or the Cable Landing License Act;

(4) Been subject to an adjudicated finding of making false statements or engaging in fraudulent conduct concerning national security before another U.S. government agency; or

(5) Materially failed to comply with the terms of a cable landing license, including but not limited to a condition requiring compliance with a mitigation agreement with the Executive Branch agencies, including the Committee, where the violation (a) was not remediated with an adjudication involving a consent decree and/or compliance plan, (b) resulted in a loss of Commission license or authorization, or (c) was found by the Commission to be intentional.

36. We will apply this presumptive disqualifying condition to (1) any initial application for a cable landing license that is filed after the effective date of the *Report and Order,* and (2) all other types of submarine cable applications—including an application for modification, assignment, transfer of control, or renewal or extension of a cable landing license—that are filed after the effective date of the *Report and Order* by a licensee whose initial application for a cable landing license is granted after the effective date of the *Report and Order* or by an existing licensee that currently does not exhibit (prior to the effective date of the *Report and Order*) any of the aforementioned criteria set out in the disqualifying condition. Where such an application is filed for an assignment or transfer of control of a cable landing license, we will apply this presumptive disqualifying condition in our evaluation of the licensee, assignor/transferor, and assignee/transferee. We will not apply this presumptive disqualifying condition where an application for modification, assignment, transfer of control, or renewal or extension of a cable landing license is filed after the effective date of the *Report and Order* by existing licensees that currently exhibit (prior to the effective date of the *Report and Order*) any of the criteria set out in the presumptive disqualifying condition.

37. The criteria set out in this presumptive disqualifying condition are not the only grounds on which the Commission may deny an application

due to character concerns. The public interest may require, in a particular case, that the Commission deny an application on other grounds or evidence that may be indicative of the applicant's truthfulness and reliability, including violation of other provisions of the Communications Act, Commission rules, or laws.

38. An applicant subject to any of the aforementioned criteria can overcome this adverse presumption only by establishing that the applicant has the requisite character, despite its past conduct. We will not require applicants to disclose pending investigations, but rather only disclose violations as preliminarily or finally determined by the Commission, and as adjudicated by another U.S. government agency or a court in the United States.

39. We disagree with Microsoft's and NASCA's comments that the Commission's proposal regarding character qualifications was ''overbroad.'' Nevertheless, we choose to narrow the scope of the character qualifications to initially prioritize considerations related to national security in our assessment of an applicant's truthfulness and reliability and to better allocate administrative resources. Microsoft and NASCA disagree, for example, with any requirement to disclose any felony absent a material or specific threshold. The Commission considers all felonies as relevant to its evaluation of character qualifications in the broadcast licensing context, as such is indicative of an applicant's or licensee's ''propensity to obey the law.'' Further, the Commission retains the authority to take enforcement action or to revoke a licensee's cable landing license when warranted, including but not limited to reasons involving these or other character qualifications or misconduct of a licensee. Finally, while we agree with Microsoft's and NASCA's recommendation to limit the scope of the character qualifications to conduct related to ownership and operation of a submarine cable, we consider that fraudulent conduct and false statements before the Commission or other U.S. government agencies are relevant to determining the qualification of an applicant to become a cable landing licensee because such conduct bears directly on the licensee's truthfulness and propensity to obey the law and thus our ability to rely on the licensee to comply with our rules and the Cable Landing License Act. We find that the character qualifications discussed above are relevant to the determination of whether denial of a submarine cable application is warranted.

4. Foreign Adversary Cable Landing Presumptive Disqualifying Condition

40. To further protect U.S. communications networks from national security and law enforcement threats, we adopt a presumption that denial of an application, as specified below, is warranted where an applicant seeks to land a submarine cable in a foreign adversary country, as defined in § 1.70001(f) of our newly adopted rules, unless the applicant overcomes the adverse presumption. The Committee supports a presumption of denial on building new cable landings connecting foreign adversary countries to the United States, given the intent and capabilities of such countries to harm U.S. interests and the vulnerabilities inherent in submarine cable infrastructure. No other commenter addressed this issue. We find that adopting this presumptive disqualifying condition is consistent with the Commission's authority to withhold cable landing licenses and condition the grant of licenses to ''promote the security of the United States'' under the Cable Landing License Act and Executive Order 10530, and will protect this critical submarine cable infrastructure and ensure that it is secure from foreign adversaries and entities identified on the Commission's Covered List.

41. Specifically, we adopt a disqualifying condition that will presumptively preclude the grant of a submarine cable application filed by any applicant:

(1) That seeks to land a new submarine cable in a foreign adversary country, as defined in § 1.70001(f).

(2) That seeks to modify, renew, or extend its cable landing license to add a new landing located in a foreign adversary country, as defined in § 1.70001(f).

42. We will apply this presumptive disqualifying condition to: (1) any initial application for a cable landing license that is filed after the effective date of the *Report and Order,* and (2) an application for modification or renewal or extension of a cable landing license that is filed after the effective date of the *Report and Order* by a licensee whose initial application for a cable landing license is granted after the effective date of the *Report and Order* or by an existing licensee. An applicant can overcome this adverse presumption only by establishing through clear and convincing evidence that the applicant does not fall within the scope of the adverse presumption, as described above, or that grant of the application would not pose risks to national security or that the national security benefits of granting the application would substantially outweigh any risks. We will exercise our discretion to exclude such applications from referral to the Executive Branch agencies. We address below the process that will apply where the Commission considers whether denial of a submarine cable application is warranted. If an applicant fails to overcome any of the criteria in the presumptive disqualifying condition, we will find that denial of the application is warranted to promote the security of the United States and we will deny the application.

43. We agree with the Committee that there are substantial and serious national security and law enforcements risks associated with landing submarine cables in foreign adversary countries. Since 2017, there have been two submarine cable applications filed in part by entities with ties to foreign adversary countries and with the proposed cable landings in foreign adversary countries. The Executive Branch agencies recommended that the Commission partially deny the PLCN cable system application due to national security and law enforcement risks, stating that the proposed connection to Hong Kong, ''combined with other pending applications seeking to directly connect the United States to Hong Kong, furthers the PRC's ambitions to have access to an information hub that is directly linked to U.S. ICT infrastructure'' and ''potentially could place voluminous amounts of sensitive U.S. person data in these companies' possession at risk.'' The Committee recommended that the Commission deny the ARCOS–1 modification application due to national security and law enforcement risks, stating that ''[i]f the application is granted as proposed, U.S. persons' internet traffic, data, and communications transiting the proposed ARCOS–1 cable expansion (Segment 26) to Cuba are very likely to be compromised,'' given the ''Cuban government maintains tight control of the Cuban telecommunications networks through [Empresa de Telecomunicaciones de Cuba S.A. (ETECSA)].''

5. Prohibition on IRUs and Capacity Leases With Foreign Adversaries

44. To further protect U.S. communications networks from national security, law enforcement, and other threats, we adopt a condition that cable landing licensees are prohibited from entering into arrangements for Indefeasible Rights of Use (IRUs) or leases for capacity on submarine cable systems landing in the United States,

where such arrangement for IRUs or lease for capacity would give an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g), the ability to install, own, or manage SLTE on a submarine cable landing in the United States. While we clarify that we do not apply a strict liability standard, we expect licensees to conduct substantial due diligence to ensure compliance with FCC requirements. To the extent a licensee conducts substantial due diligence to verify all relevant information and reasonably believes the entity is not owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined herein, such licensee would not be subject to enforcement sanctions. We would consider all of the facts and circumstances raised in an individual case and take into consideration the steps a licensee took in conducting substantial due diligence to ensure compliance with the rule. We adopt this condition with respect to new and extension of existing arrangements for IRUs or leases for capacity between a cable landing licensee and any of the aforementioned entities, subject to any exception granted by the Commission. A licensee may petition the Commission for waiver of the condition. Any waiver of the condition would be granted only to the extent the licensee demonstrates by clear and convincing evidence that such new or extension of an existing arrangement or lease would serve the public interest and would present no risks to national security or that the national security benefits of granting the waiver would substantially outweigh any risks.

45. The Commission sought comment on whether it should prohibit cable landing licensees from entering into arrangements for IRUs or leases for capacity on submarine cables landing in the United States with entities associated with foreign adversaries. Specifically, the Commission sought comment on applying this prohibition to any entity that is directly and/or indirectly owned or controlled by, or subject to the influence of, (1) a government organization of a foreign adversary country, and/or (2) any individual or entity that has a citizenship(s) or place(s) of organization in a ''foreign adversary'' country, as defined under 15 CFR 791.4. For the reasons discussed above, we instead adopt the narrower, more precise, and previously-used formulation ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.''

46. We are persuaded by the record support for our action today. NASCA argues that the proposal ''to ban certain commercial transactions is not supported by specific findings that the transactions pose a national security or law enforcement risk, given that the customers in such transactions typically do not have the ability to exert influence or control over the cable.'' Other commenters, however, address national security risks associated with submarine cables in the current threat environment. FDD states that ''Beijing has also repeatedly demonstrated its willingness to use security gaps within U.S. critical infrastructure'' and ''[t]hese risks are heightened by private firms' use of remote network management systems, particularly those connected directly to the [I]nternet, to control submarine cable systems.'' The Committee states that ''the United States and its networks are under constant threat from various foreign adversaries, particularly China'' and recent compromise of U.S. telecommunications infrastructure ''reflects the increasing capability of China to target critical American infrastructure and systems.'' The Committee states that prohibiting cable landing licensees from entering into dark fiber IRU agreements with foreign adversary-affiliated entities would reduce risks posed by such entities owning or operating SLTE on submarine cables landing in the United States ''pursuant to an IRU or similar or similar legal instrument,'' and also provide ''a bright line rule'' requested by commenters. The Committee emphasizes the national security risks presented by foreign adversary entities with this type of access, including serious counterintelligence risks where an adversary could intercept or misroute U.S. persons' communications and sensitive data transiting the submarine cable.

47. We find there are serious national security and law enforcement risks associated with access, ownership, and control of communications fiber and principal equipment on this critical U.S. infrastructure by entities that are owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Capacity may be held on submarine cables through ownership, leasing, purchasing, selling, buying, or swapping of capacity, spectrum, or fiber (partial fiber pair or a full fiber pair) for transmission of voice, data, and internet over the submarine cable system to interconnect with a U.S. terrestrial network. Significant national security and law enforcement risks are raised where an untrustworthy actor has access to U.S.-based infrastructure and sensitive information that traverses such infrastructure. In the *China Telecom Americas Order on Revocation and Termination,* for example, the Commission discussed that ''the opportunities for harmful conduct associated with [China Telecom (Americas) Corporation's (CTA)] ability, as a service provider, to carry U.S. communications traffic present risks of unauthorized access to U.S. customer data and/or metadata.'' Moreover, there are serious national security and law enforcement risks where an untrustworthy actor with access, ownership, and control of submarine cable communications fiber and principal equipment, has physical presence within U.S. communications networks and ''can potentially access and/or manipulate data where it is on the preferred path for U.S. customer traffic.'' Our action today further protects the submarine cable infrastructure from threats and ensures foreign adversaries are precluded from exploiting the domestic supply chain.

*B. Cable Landing License Processes To Withhold or Revoke and/or Terminate a License*

1. Process To Withhold or Revoke and/or Terminate a License

48. We adopt the Commission's proposal to apply an informal written process in cases involving withholding or revocation and/or termination of a cable landing license. Below, we describe the procedures we will use for revocations and denials, respectively. We find that these procedures are consistent with due process and procedural requirements under the Cable Landing License Act, the Communications Act, and the Administrative Procedure Act (APA).

49. The Cable Landing License Act states that the President may ''withhold or revoke such [cable landing] license . . . after due notice and hearing,'' but does not identify particular procedures that must be followed. Where a statute does not expressly require an ''on the record'' hearing and instead calls simply for a ''hearing,'' a ''full hearing,'' or uses similar terminology, the statute does not trigger the APA's formal adjudication procedures absent clear evidence of congressional intent to do so. Agencies must adhere to the formal hearing procedures in sections 554, 556, and 557 of the APA only in cases of ''adjudication required by statute to be determined on the record after opportunity for an agency hearing.'' In addition to the Cable Landing License

Act, neither the Communications Act, the Commission's rules, nor the APA requires the Commission to use trial-type hearing procedures when it withholds or revokes a cable landing license. Congress has granted the Commission broad authority to ''conduct its proceedings in such manner as will best conduce to the proper dispatch of business and to the ends of justice.'' The Commission has broad discretion to craft its own rules ''of procedure and to pursue methods of inquiry capable of permitting them to discharge their multitudinous duties.'' Furthermore, the Communications Act gives the Commission the power of ruling on facts and policies in the first instance. In exercising that power, the Commission may resolve disputes of fact in an informal hearing proceeding on a written record. Below, we explain how we will conduct application and revocation proceedings.

50. *Revocation Informal Written Process.* We adopt an informal written process for revocations that will allow for the presentation and exchange of full written submissions before the Commission or OIA. The informal written process will provide cable landing licensees with timely and adequate notice of the reasons for any revocation action, and opportunity to cure noncompliance to the extent such an opportunity is required by the APA, and to respond to allegations and evidence in the record and to make any factual, legal, or policy arguments through the presentation and exchange of full written submissions. To the extent required by the APA, licensees will also be afforded the opportunity to cure any noncompliance before the institution of a revocation proceeding. *See* 5 U.S.C. 558(c) (''Except in cases of willfulness or those in which public health, interest, or safety requires otherwise, the withdrawal, suspension, revocation, or annulment of a license is lawful only if, before the institution of agency proceedings therefor, the licensee has been given—(1) notice by the agency in writing of the facts or conduct which may warrant the action; and (2) opportunity to demonstrate or achieve compliance with all lawful requirements.''). We adopt the proposal that the Commission may commence a revocation proceeding either on its own initiative or upon the filing of a recommendation by the Executive Branch agencies, including the Committee, to revoke the license of a cable landing licensee. A few commenters state that the Commission cannot revoke a cable landing license ''without prior coordination and approval from the State Department.'' We note that the Commission and the State Department have existing procedures by which the State Department approves the Commission's grant of a cable landing license application or revocation of a cable landing license, as required by Executive Order 10530, and these procedures would continue to apply to any revocation of a cable landing license.

51. While we believe that oral hearing procedures are not warranted in all cases involving revocation of cable landing licenses, we delegate authority to OIA to determine appropriate procedures on a case by case basis, including addressing requests for oral hearing procedures, providing an opportunity for oral hearing procedures where warranted by the facts and circumstance, and designating an Administrative Law Judge (ALJ) as the presiding officer if the hearing includes oral procedures, if OIA determines that doing so would be appropriate based on the ALJ's expertise or for other reasons. Courts have held that the question of whether to hold an evidentiary hearing is ''within [the agency's] discretion, and it may 'properly deny an evidentiary hearing if the issues, even disputed issues, may be adequately resolved on the written record, at least where there is no issue of motive, intent or credibility.''' As stated in the *2024 Cable NPRM,* we do not believe it would be appropriate to require live hearing procedures involving testimony and cross-examination in all proceedings to revoke cable landing licenses, particularly in cases involving national security issues, where the Commission has previously concluded that the burdens on the Government of implementing such procedures outweighed the private interest and the probable value of additional procedures. We also believe that live hearing procedures could entail significant administrative burdens on the Commission even in cases involving other issues that do not involve the Executive Branch agencies, such as character concerns, or other Commission rule violations. The informal written process we will apply is also distinct from the Commission's subpart B hearing rules, including the written hearing rules codified in §§ 1.371 through 1.377. No commenter addressed these proposals or argued that we should require oral hearing procedures in cases involving revocation of cable landing licenses.

52. While no commenter opposed an informal written hearing process, a few commenters state that revocation procedures should provide licensees with notice and an opportunity to resolve or cure concerns. A few commenters state generally that revocation will have an impact on investments, or that the Commission should ''provide licensees with a clearly established process to revoke a license,'' but they do not claim that the informal written process itself would provide insufficient process or fail to provide adequate opportunities for affected licensees to address the Commission's concerns. However, a few commenters propose mitigation as an additional procedural safeguard to resolve concerns or as a substitute for any revocation action. For example, INCOMPAS states that, ''[b]efore the Commission resorts to revocation, it first should engage with licensees'' to provide an opportunity to work with the Commission and Executive Branch agencies to identify national security concerns and develop mitigation measures. U.S. Chamber of Commerce states that licensees should be provided ''a meaningful opportunity'' to respond to allegations of misconduct and to cure or to mitigate concerns. As discussed below, we delegate authority to OIA to implement procedures on a case by case basis in accordance with section 558(c) of the APA, including providing notice and opportunity, where appropriate, to achieve compliance unless the facts and circumstances indicate willfulness or that the public interest or safety requires otherwise (including harm to national security). The Commission may determine, for example, in light of the relevant facts and circumstances that national security and law enforcement risks presented in a particular case cannot be addressed through mitigation with the Executive Branch agencies. Moreover, Executive Order 10530 requires the Commission to obtain the approval of the State Department, and, ''as the Commission may deem necessary,'' to seek advice from other Executive Branch agencies, before granting or revoking or terminating a cable landing license. The Commission has sought the expertise of the relevant Executive Branch agencies in identifying and evaluating issues of concern that may arise from an applicant's or licensee's foreign ownership, while also emphasizing that it will make an independent decision and will evaluate concerns raised by the Executive Branch agencies in light of all the issues raised. Further, revocation cases may involve other issues that do not involve the Executive Branch agencies, such as character concerns, or other Commission rule violations. To

the extent any revocation proceeding is commenced either on the Commission's own initiative or upon the filing of a recommendation by the Executive Branch agencies, we find that our informal written process will ensure the development of an adequate administrative record and appropriate procedural safeguards to ensure due process, including procedures for participation by affected licensees, the Executive Branch agencies, and other interested parties.

53. We disagree with proposals to curtail the Commission's authority to revoke and/or terminate a cable landing license under the Cable Landing License Act, Executive Order 10530, and the Commission's rules. Commenters suggest, for example, that the Commission should only revoke the license of a cable landing licensee on national security and economic security grounds or solely based on a history of noncompliance, or otherwise provide a clear standard such as specific national security threats posed by changed circumstances or noncompliance with the terms of a license or Commission rules. We cannot effectively discharge our duty to protect national security by limiting our revocation and termination process to a prescribed list of circumstances, as we cannot predict with certainty what circumstances might threaten national security in the future. However, in general, we will consider the possibility of initiating revocation proceedings, for example, where a licensee's actions or failure to act, or other circumstances, raise concerns about our ability to trust the licensee to comply with the Cable Landing License Act, our submarine cable rules, and/or national security commitments, or to otherwise protect national security interests. Further, a licensee's violation of other statutory or regulatory requirements, as well as serious non-FCC misconduct, may call into question our ability to trust a licensee in this regard. We will consider the possibility of initiating termination proceedings where a licensee fails to comply with any condition of its license. Separate and apart from revocation, the Commission uses the term ''termination'' where a license or authorization is terminated based on the licensee's or authorization holder's failure to comply with a condition of the license or authorization, and has determined that the informal written procedures applicable to termination need not mirror the procedures used for revocation of licenses or authorizations. To the extent any revocation and/or termination proceeding is commenced, we find that our informal written hearing process will ensure the Commission obtains the approval of the State Department, and will seek advice from other Executive Branch agencies, ''as the Commission may deem necessary,'' before revoking or terminating a cable landing license. As discussed below, we delegate authority to OIA to determine appropriate procedures on a case by case basis for revocation and/or termination of a cable landing license, as required by due process and applicable law and in light of the relevant facts and circumstances.

54. *Application Proceedings.* As stated in the *2024 Cable NPRM,* we believe that the statutory language ''withhold . . . such license'' authorizes the denial of an application, including an initial application for a cable landing license and an application to modify, assign, transfer control of, or renew or extend a cable landing license. The *2024 Cable NPRM* sought comment on the extent to which the Commission's existing procedures for denial of applications should be modified in any respect. The Commission also sought comment on whether its procedures for denial of an application to modify, assign, or transfer control of a license, or for renewal and extension applications should mirror its procedures for denial of an initial application. One commenter addressed the procedural framework applicable to denial. We conclude that additional informal written procedures beyond our existing procedures are not warranted for denial of applications, but as proposed we delegate authority to OIA to adopt additional procedures on a case-by-case basis as circumstances warrant, and consistent with due process.

55. Consistent with Executive Order 10530, we also adopt the proposal to amend § 1.767(b) of the rules so that it does not state that denial of an application requires approval by the Secretary of State. No commenter addressed this proposal. Executive Order 10530 does not require the State Department's approval of a denial action and expressly states that ''no such license shall be *granted or revoked* by the Commission except after obtaining approval of the Secretary of State . . . .'' Section 1.767(b) of the current rules, however, is inconsistent with the language in Executive Order 10530, as it states that submarine cable applications are ''acted upon by the Commission after obtaining the approval of the Secretary of State.'' The term ''acted upon'' would appear to include denial of an application. Therefore, we remove the language ''[t]hese applications are acted upon'' in the rule and state instead, ''[c]able landing licenses shall be granted or revoked by the Commission after obtaining the approval of the Secretary of State . . . .''

56. *Delegation of Authority to OIA to Implement Procedures.* Further, we adopt the Commission's proposal to modify OIA's existing delegated authority to permit OIA to deny an application and to revoke and/or terminate a cable landing license under the Cable Landing License Act and Executive Order 10530. While no commenter opposes this proposal, INCOMPAS asserts that any codification of the revocation procedures should state that any reservation of the Commission's authority to modify its approach as circumstances warrant ''is limited by the requirements of due process.'' The rule we adopt sets forth, among other things, that OIA shall determine appropriate procedures, initiate revocation and/or termination proceedings, and revoke and/or terminate a cable landing license, ''as required by due process and applicable law.'' Specifically, we delegate authority to OIA to determine appropriate procedures on a case by case basis for grant or denial of an application or revocation and/or termination of a cable landing license, to initiate and conduct application, revocation and/or termination proceedings, and to grant or deny an application and revoke and/or terminate a cable landing license, as required by due process and applicable law and in light of the relevant facts and circumstances, including providing the applicant or licensee with notice and opportunity to cure noncompliance to the extent such an opportunity is required by the APA, and to respond to allegations and evidence in the record.

2. Process To Revoke Licenses of Licensees That Are Insolvent or No Longer Exist

57. We adopt a process to revoke the cable landing licenses of licensees that are insolvent or no longer exist. Section 1.767(m)(2) of the rules requires that ''[a]ny licensee that seeks to relinquish its interest in a cable landing license shall file an application to modify the license.'' The Commission's records in the International Communications Filing System (ICFS) and other records, indicate that some submarine cables licensed by the Commission may not have commenced service and/or some cable landing licensees of record may be insolvent or no longer in operation. Furthermore, some licensees that may be insolvent or no longer exist did not file a modification application to

relinquish their interest in the cable landing license or otherwise notify the Commission. In the *2024 Cable NPRM,* the Commission sought comment on what processes it should adopt when submarine cables and/or licensees are insolvent or no longer exist. No commenter addressed this issue. Given we are conducting a one-time collection below, we will require all licensees to provide updated information so that the Commission can ensure it has accurate information regarding submarine cables and licensees subject to its oversight and begin a process to revoke licenses for insolvent cables and/or held by insolvent licensees.

58. If a licensee fails to timely respond to the information collection required in the *Report and Order* adopted herein and subsequently fails to achieve compliance after notice of the failure, we will apply our revocation process to revoke its license or remove the licensee from a license held by multiple licensees. We would deem the failure to respond to this *Report and Order* as presumptive evidence that the licensee is no longer in operation. We will publish in the **Federal Register** a list of non-responsive licensees and non-operating licensees identified by responding licensees and provide an additional thirty (30) days from that publication for those licensees to respond to the information collection requirement or file a notification to relinquish their interests in the license.

59. In situations where a licensee has gone out of business and is no longer able to make the filing on its own behalf, other licensees that jointly hold the license, if any, may appoint one licensee to make a filing that demonstrates and certifies that the licensee has ceased to exist and that the remaining licensee(s) will retain collectively *de jure* and *de facto* control of the U.S. portion of the cable system. If the licensee has not responded within thirty (30) days of the publication of the notice in the **Federal Register**, we will institute a proceeding to revoke the license or the licensee's rights under a license held by multiple licensees. We note that licensees that fail to comply fully and timely with the information collection required in this *Report and Order* are subject to enforcement action, including forfeitures, revocation, or termination. We find this process is reasonable and necessary to ensure the accuracy of the Commission's records regarding cable landing licensees.

60. Any licensee whose cable landing license is revoked for failure to respond following the institution of a proceeding may file a petition for reinstatement *nunc pro tunc* of the license or its rights under a license held by multiple licensees. A petition for reinstatement will be considered: (1) if it is filed within six months after publication of the **Federal Register** notice; (2) if the petition demonstrates that the licensee is currently in operation, including operation of the submarine cable; and (3) if the petition demonstrates good cause for the failure to timely respond. A licensee whose cable landing license or whose rights under a license held by multiple licensees is cancelled under these procedures would be able to file a new application to become a licensee in accordance with the Commission's rules, which would be subject to full review.

### *C. Cable Landing License General Requirements*

#### 1. FCC Licensing Authority Under the Cable Landing License Act

61. In the *2024 Cable NPRM,* the Commission proposed to codify its longstanding practice of applying the licensing requirement to submarine cables that lie partially outside of U.S. territorial waters. The Commission sought to bring additional clarity to the application process as well as regulatory certainty to submarine cable owners and operators. Based on the comments, we codify the proposal with one nomenclature change. That is, to clarify the application of the rule, we replace the originally proposed term ''international waters'' with the phrase ''areas beyond the U.S. territorial waters, which extend 12 nautical miles seaward from the coastline.''

62. Accordingly, we agree with the suggestion of NTIA and the State Department that we refrain from using the term ''international waters'' because the term is not used in the United Nations Convention on the Law of the Sea (UNCLOS) and to instead use ''areas beyond the limits of national jurisdiction'' or similar phrasing. Although the United States has neither signed nor ratified UNCLOS, the United States considers provisions of UNCLOS concerning traditional uses of the ocean as generally reflective of customary international law binding on all States. One provision of UNCLOS that the United States abides by is that: ''[t]he territorial sea is a belt of ocean established by a coastal State extending seaward up to 12 nautical miles from the baseline of that State and subject to its sovereignty.'' Our practice has been to require a cable landing license for a cable that connects points within the continental United States, Alaska, Hawaii, or a territory or possession if part of that cable is laid in an area beyond 12 nautical miles from the U.S. coastline, which is consistent with UNCLOS. Therefore, we adopt this modification to the proposed rule to ensure that the industry clearly understands when a cable landing license is required, which will benefit applicants and promote efficiency for the Commission. Our clarification is consistent with the Act's definition of ''United States'' to mean territory ''subject to the jurisdiction of'' the United States.

63. We therefore adopt the proposed rule with clarification as follows:

A cable landing license must be obtained prior to landing a submarine cable that connects:

(1) The continental United States with any foreign country;

(2) Alaska, Hawaii, or the U.S. territories or possessions with:

(i) a foreign country,

(ii) the continental United States, or

(iii) with each other; or

(3) Points within the continental United States, Alaska, Hawaii, or a territory or possession in which the cable is laid in areas beyond U.S. territorial waters, which extend 12 nautical miles seaward from the coastline.

64. *One Portion of the United States.* We disagree with Lumen and USTelecom that the Commission's rule is overbroad based on their view that the term ''portion'' as used in the Cable Landing License Act is intended to mean state, territory, or possession and that the Act does not require a license if a cable connects two points within one ''portion.'' Based on this interpretation, these commenters claim that the Act does not require a license if a cable connects two points within a single state, territory, or possession, because the statute only requires a license when a submarine cable connects ''one portion of the United States with any *other* portion,'' *i.e.,* one state with any *other* state. We reject this interpretation. Rather, we believe the best reading of the statute is that the phrase ''connecting one portion of the United States with any other portion thereof'' was intentionally broad and refers to cables connecting any parts of the United States. The Cable Landing License Act does not define the term ''portion.'' Had Congress meant for the term ''portion'' to mean state, territory, or possession, it could have used those terms instead, or it could have included such a definition as it did when it defined the term ''United States.'' Likewise, if Congress intended for this term to be limited in scope, it could have included an exception to the licensing requirement just as it did in

the second sentence of the same statutory section. Instead, Congress included no such limiting language. To help shed light on the requirement's intended scope, we thus look to the term's ''ordinary, contemporary, common meaning'' when that term was adopted by Congress in 1921. At that time, the ''ordinary, contemporary, common meaning'' of the term ''portion'' was ''a part of any whole.'' And a cable connecting two landing points—even if they lie within a single state, territory, or possession—connects parts of the whole of the United States. Accordingly, our interpretation best satisfies the statutory language chosen by Congress. Lumen further argues that there is ''no textual basis in the statute'' for treating differently cables connecting two points in a single state based on whether the cable is laid in international waters, as proposed in the NPRM. Lumen thus suggests that under the Commission's proffered reading of the statute, a license would be required under such circumstances unless the statutory exception relating to cables lying ''wholly within the continental United States'' applies—an exception that would not apply in the case of Hawaii, whether or not the cable is laid in international waters. Nonetheless, consistent with longstanding practice and to avoid any possible impingement of intrastate matters with respect to such cables, we codify our existing practice of not requiring a cable landing license for wholly local cables that remain within the territorial waters of the United States. For example, a submarine cable that connects one point in Hawaii to another point in Hawaii, if laid within U.S. territorial waters, would not require a cable landing license.

65. *Alaska and Continental United States.* ATA argues that ''cables solely connecting points within the state of Alaska, or connecting Alaska to the lower 48 states, are outside the scope of the licensing requirement [the Cable Landing License Act].'' We disagree with ATA's arguments and will address them in turn.

66. First, we disagree that the licensing requirement in the Cable Landing License Act is not intended to apply to cables connecting Alaska to other parts of the United States. Congress limited the application of the Cable Landing License Act by adding the following language that is now codified at section 34 of title 47 of the U.S. Code: ''The conditions of sections 34 to 39 of this title shall not apply to cables, all of which, including both terminals, lie wholly within the continental United States.'' Even if Alaska was a part of the continental United States as ATA would argue is a proper interpretation, a cable landing license would nonetheless be required for a submarine cable connecting Alaska to the United States because the submarine cable would in no way meet the statutory exception that the ''cable[ ], all of which, including both terminals, lie[s] wholly within the continental United States.'' The plain language of the statute does not state that *only* the terminals of the submarine cable must lie within the continental United States, instead, it says that *all* of the cable, which includes the terminals, must lie within the continental United States. There is no basis in the plain text of the statute to read ''all of which, including both terminals,'' to exclude the ''wet segment'' of the cable, and ATA's reliance on legislative history does not support its reading. Moreover, construing the language in this way would conflict with the Commission's longstanding interpretation, which reflects the best reading of the statute. Thus, in order for a cable connecting Alaska to other states to be exempt from the licensing requirement, *i.e.,* wholly within the continental United States, the entire submarine cable system would need to remain within U.S. territorial waters up to 12 nautical miles seaward from the coastline, which we know geographically would be impossible for a cable laid from Alaska to the continental United States. Therefore, even if Alaska was a part of the continental United States, a cable connecting Alaska to another state would not meet the exception under the Act. Second, our rule will not require a cable landing license when a submarine cable connects points within Alaska if the cable remains within U.S. territorial waters. Thus, cables connecting two points in Alaska are subject to the same licensing requirement as cables connecting any other two points within the United States.

67. ATA makes two additional claims. First, ATA claims that ''submarine cables connecting solely domestic points—even those laid in international or foreign waters—do not implicate any of the evolving national security risks that the NPRM seeks to address.'' ATA's argument is based on the mistaken premise that domestic cables are only owned or operated by domestic entities, such as U.S. carriers. This is an inaccurate assessment of the submarine cable industry in the United States as foreign entities are often cable landing licensees subject to Commission rules or there may be other foreign components of submarine cables, domestic or international. Further, domestic cables connect the United States to faraway U.S. territories such as Guam, where U.S. military bases are strategically located. It is inaccurate to indicate that there are no such concerns regarding national security or law enforcement with regard to domestic submarine cables. The Commission has long stated that foreign participation in submarine cables licensed by the Commission may pose risks to national security, law enforcement, foreign policy, and trade policy for which Executive Branch agencies' expertise is needed to assist the Commission with its public interest determination. Therefore, we reject ATA's claim that cables connecting solely domestic points do not implicate national security risks. Second, ATA states that ''[i]f the Commission finds that any category of purely domestic submarine cables is subject to the Cable Act's licensing mandate, it should streamline that requirement by granting blanket license authority by rule to land such fully domestic cables, whether or not they traverse international waters.'' We address this request in the *Further Notice of Proposed Rulemaking.*

2. Submarine Cable System Definition

68. We adopt a submarine cable system definition that will provide regulatory certainty to submarine cable owners and operators and ensure administrative efficiency for the Commission. The *2024 Cable NPRM* sought comment generally on whether it is necessary to adopt a definition of a submarine cable system for purposes of licensing a submarine cable system and whether we should codify a submarine cable definition in our rules. As the record overwhelmingly demonstrates, commenters support the proposal to define a submarine cable system and to codify a definition of a submarine cable system in the Commission's rules, stating that it will add clarity to the Commission's rules and licensing regime.

69. We adopt a definition that is consistent with the Committee's proposed definition as well as the Commission's definition in its outage reporting rules. Importantly, our definition ensures that a submarine cable system extends to and includes the SLTE, whether it is located in a cable landing station near the initial beach landing or further in-land within data centers. We believe this definition captures what a submarine cable system is under the Cable Landing License Act and clearly identifies the demarcation point of where the submarine cable system ends and the terrestrial system begins. Based on the record, we adopt the following definition:

A submarine cable system carries bidirectional data and voice telecommunications traffic consisting of one or more submarine cable(s) laid beneath the water, and all associated components that support the operation of the submarine cable system end-to-end, including the segments up to the system's terrestrial terminations at one or more SLTEs as well as the transponders that convert optical signals to electrical signals and vice versa.

70. Where the submarine cable system ends and the terrestrial system begins has changed over time and our definition establishes that the cable extends to and includes the SLTE, whether it is located in a cable landing station near the initial beach landing or further in-land within data centers. In older architectural deployments prior to the advent of open cable systems, the SLTE was placed at the cable landing stations. Some subsequent architectural deployments place an Optical Add-Drop Multiplexer (OADM), or a Reconfigurable Optical Add/Drop Multiplexer (ROADM) in the cable landing station, with the SLTEs distributed further inland. ROADMs facilitate adding and dropping optical signals used in a fiber cable, and ROADMs add additional flexibility by allowing the operator to reconfigure the device. Both of these components add efficiency and flexibility to the optical network by inserting or removing channels. Remote management of the SLTE and all other submarine cable system equipment is also a necessity of modern systems. Remote management includes configuration, performance and fault management and testing, which emphasizes the need to have trusted management systems and personnel who can access the cable system and all associated components and facilities, including the SLTE.

71. The Committee stated that it has historically viewed a submarine cable system as including SLTE, adding that the Committee shares the Commission's view on the importance of the SLTE and the access and control it offers its owners and users. NASCA, a trade association whose members include over 25 submarine cable owners and submarine cable maintenance authorities for cable systems operating in North America, supports codification of a submarine cable definition, stating that such is ''clear and consistent with licensees' current reporting requirements to the Team Telecom agencies.'' Microsoft also maintains that the proposed definition—cable system SLTE to cable system SLTE—is consistent with the Committee's current mitigation instrument conditions imposed on many licensees.

72. Some commenters disagreed with the proposed definition, and argued that the Commission should define a submarine cable system in terms of its components that would not include SLTE. NASCA does not specifically address or take a position on inclusion of SLTE in the Commission's proposed definition, but does propose that the Commission could define a submarine cable to include only the components up to and including the optical distribution frame (ODF),'' contending that the ODF is the ''demarcation point at which the submarine cable terminates and interconnects to terrestrial fiber.'' NASCA maintains that because the ''SLTE also converts terrestrial signals to submarine signal,'' the SLTE is ''just as much a terrestrial network element as a submarine network element.'' Microsoft also takes the position that the SLTE is a terrestrial component used to ''convert terrestrial signals to submarine signals,'' and states that the ''Commission equally could modify the NPRM's proposed definition to delimit the end points of a submarine cable at the ODF,'' claiming this is the demarcation point at which a submarine cable terminates and interconnects to SLTE. ICC disagrees with inclusion of SLTE as the end point of the submarine cable system, arguing that the definition is somewhat outdated and that modern submarine cable systems typically terminate at an ODF, Open Cable Interface (OCI), ROAD–M, or similar device—which serves as a given system's interface with a particular user's optical network.

73. While we adopt ICC's recommendation to clarify in our definition that the components relate to the ''operation of'' the submarine cable system, we decline to accept commenters recommendations concerning SLTEs or comments that would limit the definition. For example, ICC recommends that we limit the definition to cover only transponders that are solely located within the SLTEs. We find that doing so would incorrectly limit the definition because transponders that support the operation of submarine cable systems can be located elsewhere. We also decline to accept NCTA's recommendation to exclude fully domestic SLTE operators and lessees as some SLTE operators and lessees do not have foreign ownership and may not pose a meaningful risk to U.S. national security. Contrary to NCTA's argument, the definition is meant to encapsulate the scope of what constitutes a submarine cable system, not whether particular components of the system pose risks.

74. Finally, we do not accept commenters' suggestion that ODF, OCI, ROADM, and similar devices should be considered as the end point of a submarine cable system. We recognize that the Commission's proposed definition of a submarine cable reflects traditional/legacy architecture when the terminal cable landing station was located near the shore and cable operators were not, as is the case today, purchasing SLTE(s) from independent equipment vendors that can be remotely managed. We also understand that cable operators today require multiplexing and other equipment to manage their fiber in cable landing stations, and that SLTE equipment allows for routing of fiber from one cable landing station to another cable landing station, or a data center located further inland and beyond the initial cable landing station. We find it necessary to include SLTE as a component in our definition because it is the SLTE that converts between submarine cable signals and terrestrial signals. While the reverse is also true, as was raised by commenters, only the SLTE converts cable signals to terrestrial signals. Therefore, whether this conversion occurs at the first, or initial, cable landing station, or occurs inland at a cable landing station or data center, we include the SLTE as the end point component of the submarine cable in our definition of a submarine cable under the Cable Landing License Act. Several commenters, noting that the Commission's proposed definition of a submarine cable system aligns with that used by the Committee in its mitigation agreements (SLTE to SLTE), support continued engagement by the Commission with other governmental entities to address risks to submarine cable infrastructure and to limit regulatory compliance burdens by avoiding unnecessary duplication on licensees' parallel Committee obligations.

3. Twenty-Five Year License Term

75. Based on the comments in the record, we retain the 25-year term for cable landing licenses. In the *2024 Cable NPRM,* the Commission sought comment, as an alternative to the proposed periodic reporting, on whether shortening the current 25-year submarine cable license term or adopting a shorter license term in combination with periodic reporting would similarly account for evolving national security, law enforcement, and other risks. We agree with the commenters that shortening the 25-year license term could have outsized negative impacts on the deployment and resilience of submarine cable systems

without providing a corresponding benefit to national security, and we therefore do not adopt a shortened license term. Instead, we retain the routine condition that a cable landing license shall expire twenty-five (25) years from the in-service date, unless renewed or extended.

*D. Submarine Cable Applicant/Licensee Requirements*

1. Licensee Requirements

76. In this *Report and Order,* we largely retain the current requirements for who must be an applicant/licensee for a cable landing license. We retain the licensing requirements for those entities that own or control a 5% or greater interest in the cable system and use the U.S. points of the cable system and those entities that control a cable landing station, but we exclude those entities that merely own, but do not control, a cable landing station from becoming an applicant/licensee for a cable landing license. At this time, we decline to adopt a licensing requirement for SLTE owners and operators. Instead, based on the comments in the record, we seek to further develop the record with a one-time information collection. The one-time information collection will assist the Commission to better understand the scope of SLTE owners and operators. In the *Further Notice of Proposed Rulemaking,* the results from the one-time information collection will assist us in adopting a more targeted SLTE regulatory framework.

a. Five Percent Ownership Threshold and Use of U.S. Points

77. We retain the requirement that an entity owning or controlling a 5% or greater interest in the cable system and using the U.S. points of the cable system must submit an application to become a licensee. We decline to adopt other proposals at this time. In the *2024 Cable NPRM,* the Commission sought comment on whether to retain the requirement that an entity that owns or controls a 5% or greater interest in the cable and uses the U.S. points of the cable system shall be an applicant for and licensee on a cable landing license. The Commission also sought comment on whether to require any entity that owns the submarine cable system or any entity that has capacity on the submarine cable system to become a licensee. The Commission additionally sought comment on whether it should require entities that own or control a U.S. landing station or submarine line terminal equipment (SLTE) to become licensees.

78. Commenters generally support the Commission's retention of the current requirement with its 5% interest threshold and use of the U.S. points of the cable system, and oppose other options. Commenters argue that the rule continues to serve a good purpose. The Coalition, for example, asserts that there is no need to change the 5% threshold because it is still an efficient method to remove regulatory burden for small carriers or investors that do not have any ability to control the submarine cable system. NASCA and INCOMPAS echo this point and state that ''imposing licensing burdens on [cable] owners [with no interest in the U.S. territory portion of a submarine cable system] would harm the market by making it less attractive for systems with multiple non-U.S. landing points to partner with investors who have no interest in the U.S. endpoint.'' Many commenters, including Microsoft, ICC, INCOMPAS, AP&T, ITI, CTIA, USTelecom, and the Coalition disagree that capacity holders should be licensees because they assert that there is no basis under the Cable Landing License Act to require such entities to become licensees, as capacity holders do not land or operate the cable system.

79. We agree with commenters that there is not a sufficient reason to disturb the requirement that any entity owning or controlling a 5% or greater interest in the cable system and using the U.S. points of the cable system must become an applicant/licensee. Additionally, requiring entities that merely own capacity on the cable system, without meeting the requisite licensing requirements of ownership of 5% or greater interest and using the U.S. points of the cable system, to become applicants/licensees would greatly increase the number of entities that must comply with our regulatory framework. At this time, pure capacity holdings, without ownership of infrastructure or deployment of certain equipment, have a negligible impact or harm on national security and do not rise to the level of requiring a license. Instead, we tailor the licensing requirements to identify those entities that can exercise ownership or control over the submarine cable system, as discussed below and in the *Further Notice of Proposed Rulemaking.* This approach, as raised by commenters, maintains our ability to know about potential foreign adversaries without harming the market and investment in and deployment of submarine cable systems connecting to the United States.

b. Control of Cable Landing Station

80. In this *Report and Order,* we revise our license requirement with respect to cable landing stations and require entities that control cable landing stations to be licensees. Entities that merely own a cable landing station are no longer required to become licensees. In the *2024 Cable NPRM,* the Commission sought comment on an appropriate rule that would capture which entities should be an applicant/licensee on a cable landing license under the Cable Landing License Act to ensure the Commission meets its public interest responsibilities. The Commission sought additional comment on the applicability of the Commission's rules to entities that own the real property/facility in which the cable landing station is located, but do not have any ability to significantly affect the cable system's operation, such as data center owners, who often request waivers from the Commission because they do not seek to be an applicant or a licensee. Moreover, the Commission sought comment on the applicability of its rules to data center owners, ''including the access they have over submarine cables and the site operations, such as physical security, power, backup power, HVAC, and other environmental support essential to proper operations of cable landing systems housed in their facilities.''

81. We agree with commenters that licensing requirements should not apply to entities that may own the cable landing station but are not directly involved in cable operations and do not control the operations of the cable system. Commenters were generally supportive of the proposal to reduce the licensing requirement. INCOMPAS does not support licensing for data center owners, claiming it would be a shift beyond the Commission's legal authorities and would not yield useful information for advancing the Commission's national security goals because ''data center owners often lack visibility into or control over cable operations'' unlike licensed cable operators. The Commission's standard practice has been to grant requests for waiver of the licensing requirements filed by entities that own the real property or facility in which the cable landing station is located but that do not have the ability to significantly affect the cable system's operation. Instead of continuing to process waivers on a case-by-case basis, we now revise our licensing requirement to require a license for ''[a]ny entity that controls a cable landing station in the United States'' and to require the applicant to

provide specific information in an application regarding ownership of the cable landing station. We find that adoption of this rule will streamline and clarify our licensing process and will reduce burdens by narrowing the scope of the licensing requirement and making it unnecessary for non-controlling property or facility owners to file waiver requests.

c. Submarine Line Terminal Equipment (SLTE) Owners and Operators

82. While we include SLTE within the definition of a submarine cable system, we decline to adopt a licensing requirement for owners and operators of SLTE at this time. A SLTE owner would need to be a licensee if it otherwise meets the Commission's requirements to be a licensee (*i.e.,* 5% or greater ownership in the cable system or controls a cable landing station). For purposes of this section, SLTE refers to technology that converts optical signals that traverse the submarine cable system into electrical signals that transmit across terrestrial networks and vice versa. We agree with commenters that we should seek comment in the *Further Notice of Proposed Rulemaking* as to how the Commission can best incorporate such entities into its regulatory framework. We recognize that we need further information on the number of SLTE owners and operators. We understand that at least one SLTE is needed per fiber, but due to dark fiber IRU or lease agreements where entities light their own fiber that could then be subject to further resale through separate IRU or lease agreements for fiber, capacity, or spectrum, there may be numerous SLTEs deployed on one fiber alone. We adopt below a one-time information collection to assist the Commission in obtaining comprehensive and current information on SLTEs so that the Commission may consider appropriate rules for purposes of ensuring the safety and security of submarine cable infrastructure. As the Commission stated in the *2024 Cable NPRM,* we need to know which entities own or control SLTE so that we can protect national security and law enforcement interests in carrying out our licensing duties. As the Committee noted, ''[a] foreign adversary-controlled non-licensee entity that owns, controls, or operates its own SLTE, or equivalent equipment, on a submarine cable landing in the United States may have connectivity comparable to operating their own communications cable to the United States without a license, or any regulatory review, mitigation, or monitoring for national security or law enforcement risk.'' Through the *Further Notice of Proposed Rulemaking,* we anticipate developing a record to take the best approach balancing our focus on supporting industry's ability to deploy submarine cable systems and our obligations to protect national security.

2. Application Requirements

83. Today, we adopt new application requirements that will ensure the Commission has targeted and granular information about the submarine cable system and third-party foreign adversary service providers, which is critical to improve the Commission's assessment of national security risks. We also adopt new certification requirements that will require applicants and licensees to certify whether or not they meet any of the Commission's presumptive disqualifying conditions; that they have created, updated, and implemented a cybersecurity and physical security risk management plan; and that they comply with Covered List requirements. For purposes of the information requirements, unless otherwise indicated, we use the terms ''applicant'' or ''applicants'' to refer to an applicant or licensee that currently files the following applications or notifications: (1) applicants that file an initial application for a cable landing license or an application for modification, substantial assignment, substantial transfer of control, or renewal or extension of a cable landing license; (2) cable landing licensees that file a notification of pro forma assignment or transfer of control of a cable landing license; and/or (3) applicants that file a request for special temporary authority (STA) related to the operation of a submarine cable. *See* 47 CFR 1.767(a), (g)(6)–(7); 63.24(e) (referring to ''substantial'' transactions); 63.24(d) (defining ''Pro forma assignments and transfers of control''). Unless otherwise indicated, we use the term ''application'' or ''submarine cable application'' to refer to an initial application for a cable landing license; an application for modification, substantial assignment, substantial transfer of control, or renewal or extension of a cable landing license; and a pro forma assignment or transfer of control notification. These requirements will apply to all applications for a cable landing license and modification, assignment, transfer of control, renewal or extension of a cable landing license. We will retain the current requirement for applicants to identify their 10% or greater direct and indirect equity and/or voting interests.

a. Public Interest Statement

84. Consistent with longstanding practice, we adopt the proposed requirement that ''an applicant seeking a submarine cable landing license or modification, assignment, transfer of control, or renewal or extension of a submarine cable landing license shall include in the application a statement demonstrating how the grant of the application will serve the public interest.'' The Commission has long found that national security, law enforcement, foreign policy, and trade policy concerns are important to its public interest analysis of submarine cable applications, and these concerns warrant continued consideration in view of evolving and heightened threats to the nation's communications infrastructure.

85. We agree with NASCA that the requirements of the public interest standard should be clarified so they are ''targeted, objective, and express.'' Accordingly, our final rule clarifies the scope of this obligation. Specifically, and consistent with the express statutory objectives, the public interest statement must explain how the application will ''assist in securing rights for the landing or operation of cables in foreign countries, or in maintaining the rights or interests of the United States or of its citizens in foreign countries, or will promote the security of the United States,'' provide ''just and reasonable rates and service,'' and prohibit ''exclusive rights of landing or of operation in the United States.''

86. NASCA acknowledges that a reasonably tailored public interest standard ''would not be overly burdensome,'' observing that ''applicants already routinely include information relevant to the public interest in their applications.'' However, NASCA argues that ''the Commission must have an identifiable legal basis'' for imposing such requirements, which it claims the *2024 Cable NPRM* fails to do. We disagree. As articulated in the *2024 Cable NPRM,* the Commission has ''long found that national security, law enforcement, foreign policy, and trade policy concerns are important to its public interest analysis of submarine cable applications, and these concerns warrant continued consideration in view of evolving and heightened threats to the nation's communications infrastructure.'' The legal basis to require applicants to provide this public interest statement is grounded on our authority to grant, withhold, revoke, or condition a license and the statutory criteria for doing so. *First,* the Commission can withhold the grant of

a license to protect the interests of the public as expressed in the statutory licensing criteria. The determination of whether to grant a license rests on the same statutory criteria, including consideration of how grant of the application will ensure the security of the United States. *Second,* the Cable Landing License Act authorizes the Commission to impose terms upon grant of a license that are ''necessary to assure just and reasonable rates and service,'' and to prohibit ''exclusive rights of landing or of operation in the United States.'' Accordingly, the legal basis for the public interest standard we adopt today is derived from Congress' directive as reflected in the statutory language.

b. Ten Percent Threshold for Reportable Interests

87. We retain our current requirement for applicants to identify the 10% or greater direct and indirect equity and/or voting interests held in the submarine cable applicants. In the *2024 Cable NPRM,* the Commission sought comment on whether to lower the current 10% ownership reporting threshold to five percent (5%) or greater direct or indirect equity and/or voting interests in the applicant(s) and licensee(s). Some commenters raised concerns about cost burden of compliance, impact on investment, privacy for smaller investors, and raised doubts that owners of smaller interests could wield significant influence over the cable, while others urged we go further and consider requiring the reporting of any known foreign adversary interest in cable landing license applicants and licensees instead of adopting the 5% reportable ownership threshold. At this time, we will not modify the 10% ownership threshold for disclosing reportable interest holders, because we assess that national security risks are best addressed through the certifications regarding whether the applicant is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.

c. Submarine Cable System Information

88. Below, we adopt rules to provide the Commission with important and relevant information concerning the submarine cable system. As discussed, we find that collection of this information is critical to our review of submarine cable applications and cable landing licensees for national security purposes and will advance our efforts to protect the security, integrity, and resilience of this critical U.S. infrastructure.

89. We adopt the Commission's proposal to require applicants seeking a cable landing license or modification, assignment, transfer of control, or renewal or extension of a license, and licensees submitting a Foreign Adversary Annual Report, to provide additional detailed information concerning the submarine cable system. Specifically, we adopt the proposal to require applicants and licensees to submit with these applications and/or Foreign Adversary Annual Reports the following detailed information regarding the submarine cable system:

(1) the states, territories, or possessions in the United States and the foreign countries where the submarine cable system will land;

(2) the number of segments in the submarine cable system and the designation of each (*e.g.,* Segment A, Main Trunk, A–B segment);

(3) the length of the submarine cable system by segment and in total;

(4) the location, by segment, of any branching units;

(5) the number of optical fiber pairs, by segment, of the submarine cable system;

(6) the design capacity, by segment, of the submarine cable system;

(7) specific geographic location information (geographic coordinates, street address, county or county equivalent, as applicable), or if not available, a general geographic description and specific geographic location information to be filed no later than ninety (90) days prior to construction regarding:

(i) each U.S. and non-U.S. cable landing station and beach manhole;

(ii) each network operations center (NOC) and backup NOC and, if distinct from the NOC, each security operations center (SOC) and backup SOC, or else a statement that the SOC and backup SOC are not distinct from the NOC and/or backup NOC;

(iii) where each Power Feed Equipment (PFE) and each Submarine Line Terminal Equipment (SLTE) is connected with the terrestrial land based system(s) and from where each is operated; and

(iv) the route position list including the wet segment of the submarine cable system; and

(8) Anticipated time frame when the applicant(s) intends to place the submarine cable system into service.

90. In addition, we adopt the proposal to modify the rules by requiring applicants to provide a specific description of the submarine cable system, including a map and geographic data in generally accepted GIS formats or other formats. We adopt the proposal to delegate authority to OIA, in coordination with the Office of Economics and Analytics (OEA), to determine the file formats and specific data fields in which data will ultimately be collected. We will allow applicants for a cable landing license to initially file a general geographic description of the geographic location information described in our newly adopted rule at § 1.70005(e)(7) concerning the submarine cable, but grant of the application will be conditioned on the Commission's final approval of specific geographic location information, consistent with the new requirements, to be filed by the applicant no later than ninety (90) days prior to construction.

91. With respect to route position lists, cable landing licensees with a license granted prior to the effective date of the new rules must submit a route position list consistent with the requirement under § 1.70005(e)(7)(iv) under the relevant license file number in the Commission's International Communications Filing System (ICFS), or any successor system, no later than sixty (60) days after the effective date of the new rules. Existing licensees may petition the Commission for waiver of the requirement, which may be granted only to the extent the licensee demonstrates that the required information is unavailable by the submission deadline.

92. We disagree with commenters' suggestions that requiring applicants and licensees to provide this information does not serve a regulatory purpose. We find that requiring specific information about the submarine cable system, including a map and route list data, is essential for ensuring the Commission can properly evaluate applications for cable landing licenses for their national security implications, determining if the application is in the public interest, and ensuring the Commission has fundamental and accurate knowledge about the security and resilience of submarine cable systems. The Coalition, for example, is generally supportive of requiring the specific location of each beach manhole, cable landing station (including locations of each PFE and each SLTE), NOC, and route position lists, provided the Commission ensures it does not involve disclosure of material non-public technical information and does not delay the review of the Commission or the Committee. We find the concerns about application delay are addressed by our adopted rules, permitting a general description at the application stage supplemented by landing points notifications. We find that concerns regarding confidentiality are addressed

below by our adoption of the Commission's proposal to provide confidential treatment. We are unpersuaded by the Coalition's suggestion that the Commission should require route position lists only for the portion of the wet segment that is in U.S. territorial waters because the Commission's jurisdiction does not extend beyond U.S. territory. We agree with the Committee that route position lists would enhance the ability of the Commission and Committee to ensure the protection of this critical infrastructure.

93. NASCA requests that the Commission allow applicants to file this information at a time closer to the in-service date. While we decline to adopt the in-service date, we recognize that the final specific geographic location information may not be available at the time an application for a cable landing license is filed. In those cases, the Commission will accept a general geographic description, provided the Commission is notified of the specific geographic location no later than ninety (90) days prior to commencing construction as a condition of any grant of such application. NASCA also requests that the Commission accept a route position list that is limited to the geocoordinate data in a full route position list. We believe our clarification to § 1.70005(e)(7) of our adopted rules shows that the Commission will require geographic location information and not other potentially competitively-sensitive information about system design as raised by NASCA. NASCA asserts that the Committee does not currently require NOC information and recommends that the Commission instead require a certification that a NOC is not located in a ''high-risk jurisdiction.'' We find that the location information of NOCs is critical for the Commission's knowledge and assessment of from where a submarine cable is or will be accessed and controlled, including by third parties, through network management, monitoring, maintenance, performance measurement, or other operational functions, and any risks presented by such access and control.

94. *Confidential Treatment.* Based on our review of the record, we adopt the Commission's proposal to provide confidential treatment for the exact addresses and specific geographic coordinates required by the newly adopted rule at § 1.70005(e)(7). We adopt the proposal to withhold the exact location information from public inspection where it concerns the wet segment as it approaches the shore, the submarine cable as it reaches the beach manhole, and the dry segment including the cable landing station(s), such as where the SLTE is located and/or from where it is operated. The record supports adoption of these proposals. Commenters explain that such location information is competitively sensitive and that public disclosure would harm the security of the submarine cable. We will release publicly more general location information, such as the city or locality, state/province/department, and country in which the submarine cable system will land.

95. *Sharing with Federal Agencies.* We adopt a rule to allow the Commission to share with the Committee information about the submarine cable system—including the location information of cable landing stations, beach manholes, PFE, SLTE, NOCs and backup NOCs, SOCs and backup SOCs, and route position lists—that is filed on a confidential basis without the pre-notification procedures of § 0.442(d) of the Commission's rules. The Commission may share information that has been submitted to it in confidence with other federal agencies when they have a legitimate need for the information and the public interest will be served by sharing the information. In the *2024 Cable NPRM,* the Commission sought comment on whether to adopt a rule that would allow the Commission to share submarine cable landing geographic coordinates, route position lists, and other information with relevant federal agencies, including information for which confidential treatment is requested, without the pre-notification procedures of § 0.442(d). No commenters oppose the sharing of the information with federal agencies. The Committee supports adoption of this rule and recommends that the Commission include all of the Committee members in any effort to share relevant submarine cable infrastructure information.

d. Third-Party Foreign Adversary Service Provider or Access From Foreign Adversary Information

96. We adopt a modified, narrower version of the Commission's proposals to require applicants to report whether or not they use and/or will use third-party foreign adversary service providers in the operation of the submarine cable. Specifically, we will require applicants to report whether or not they use and/or will use the following third-party service providers in the operation of the submarine cable system:

(1) any entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g);

(2) any entity identified on the Covered List that the Commission maintains pursuant to the Secure Networks Act, 47 U.S.C. 1601–1609; and/or

(3) any entity that can access the submarine cable from a foreign adversary country, as defined in § 1.70001(f), and to identify any such foreign adversary country.

97. This targeted approach sufficiently addresses the national security and law enforcement risks from foreign adversaries. In the *2024 Cable NPRM,* the Commission used the term ''managed network service provider'' (MNSP) to refer to the kinds of service providers licensees should disclose. The Commission proposed to define an ''MNSP'' as ''any entity other than the applicant(s) or licensee(s) (*i.e.,* third-party entity) with whom the applicant(s) or licensee(s) contracts to provide, supplement, or replace certain functions for the U.S. portion of the submarine cable system (including any cable landing station and SLTE located in the United States) that require or may require access to the network, systems, or records of the applicant(s) or licensee(s).'' We agree with the Committee that we should refer more generally to ''service providers'' to avoid confusion about which service providers are involved in managing networks as compared to other tasks that involve access to and control of the cable system. We also clearly define ''third-party service provider'' as an entity that is involved in providing, hosting, analyzing, repairing, and maintaining the equipment of a submarine cable system, including third-party owners and operators of NOCs. We find that our approach provides requested clarity in response to commenters that claim the Commission's proposed definition of MNSP is too vague.

98. We find that obtaining information about the third-party service providers is important and relevant to the Commission's consideration of national security, law enforcement, and other risks associated with a submarine cable application. We therefore disagree with INCOMPAS' suggestion that information about providers of ''supporting services'' exceeds the scope of the Cable Landing License Act. While NASCA and Microsoft argue that the most effective way to address risks of third-party access involves implementing ''rigorous'' or ''robust'' access controls, we find that requiring disclosure as to whether untrustworthy third-party

actors have access to this critical U.S. communications infrastructure will ensure that the Commission and applicants and licensees consistently identify and address such threats. The Committee supports prohibiting licensees from using vendors for equipment or services that are owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. While we do not go so far as to *prohibit* use of such third-party service providers, because the Commission did not seek comment on it in the *2024 Cable NPRM,* we do seek comment on whether to prohibit the use of such third-party service providers.

99. A few commenters recommend requiring such information only to the extent it is available at the time an application is filed given third-party service arrangements may not be known until a later time. Based on this, if an applicant is unable to confirm this information at the time of filing, we will require such applicants to file a request for waiver with status updates every thirty (30) days until they provide the information. We also find that our tailored approach addresses concerns that the information requirements we adopt relating to third-party service providers would duplicate information that is currently submitted to the Committee. Finally, as discussed below, as an initial step, we adopt a one-time collection that requires licensees to disclose whether they use certain third-party service providers.

3. Required Certifications for Applicants and Licensees

100. Below, we adopt rules requiring applicants to certify whether or not they exhibit any of the criteria set out in the presumptive disqualifying conditions adopted herein; that they have created and will implement and update a cybersecurity and physical security risk management plan; and that they comply with Covered List requirements. We will require licensees to inform the Commission of any Covered List equipment/services in a one-time collection. We also hold applicants and licensees responsible for the acts, omissions, or failures of third-parties with whom the applicant or licensee has a contractual relationship that impact the cybersecurity of the applicant's or licensee's systems and services.

a. Certification of Presumptive Disqualifications

101. We adopt new certification requirements consistent with the presumptive disqualifying conditions adopted herein. Specifically, we will require an applicant seeking a cable landing license or modification, assignment, transfer of control, or renewal or extension of a cable landing license to certify whether or not it exhibits any of the criteria set out in the foreign adversary and character presumptive disqualifying conditions. We will require an applicant seeking a cable landing license or modification, or renewal or extension of a cable landing license to certify whether or not it exhibits any of the criteria set out in the foreign adversary cable landing presumptive disqualifying condition. We delegate authority to OIA to develop the questions and certifications for the applications.

102. As discussed above, we will apply the foreign adversary and character presumptive disqualifying conditions to: (1) any initial application for a cable landing license that is filed after the effective date of the *Report and Order,* and (2) all other types of submarine cable applications—including an application for modification, assignment, transfer of control, or renewal or extension of a cable landing license—filed by a licensee whose initial application for a cable landing license is granted after the effective date of the *Report and Order* or an existing licensee that currently does not exhibit (prior to the effective date of the *Report and Order*) any of the criteria set out in the disqualifying condition. We will apply the foreign adversary cable landing disqualifying condition to: (1) any initial application for a cable landing license that is filed after the effective date of the *Report and Order,* and (2) an application for modification or renewal or extension of a cable landing license that is filed after the effective date of the *Report and Order* by a licensee whose initial application for a cable landing license is granted after the effective date of the *Report and Order* or by an existing licensee.

b. Cybersecurity and Physical Security Risk Management Plan Certifications

103. To protect submarine cable infrastructure from cybersecurity and physical security threats, we require all applicants for an initial cable landing license to certify that they have created and will implement and update a cybersecurity and physical security risk management plan and will take reasonable measures to protect their systems and services from these threats that could affect their provision of communications services through the submarine cable system, as supported by the record. We require all licensees seeking a modification, assignment, transfer of control, or renewal or extension of a cable landing license to certify in the application that they have created, updated, and implemented a cybersecurity and physical security risk management plan and will take reasonable measures to protect their systems and services from cybersecurity and physical security risks that could affect their provision of communications services through the submarine cable system. We also require existing licensees to implement a cybersecurity and physical security risk management plan within one year of the effective date of the new rules to also protect against these threats that could affect the provision of communications services through the submarine cable system. As discussed below, we do not require that these plans use any particular framework, in line with commenters who supported a flexible approach. Cybersecurity and physical security risk management plan certification is also supported by the Committee, as it will ''bring all licensees up to the minimum standards . . . needed to protect our critical infrastructure from foreign adversary threats.''

104. All applicants and licensees must certify that the cybersecurity and physical security risk management plan meets the following three requirements:

- The plan describes how the applicant or licensee takes or will take reasonable measures to employ its organizational resources and processes to ensure the confidentiality, integrity, and availability of its systems and services that could affect their provision of communications services through the submarine cable system;
- The plan identifies the cyber risks they face, the controls they use or plan to use to mitigate those risks, and how they ensure that these controls are applied or will be applied effectively to their operations; and
- The plan addresses both logical and physical access risks, as well as supply chain risks.

105. Although the *2024 Cable NPRM* proposal focused on cybersecurity, rather than physical security, the Commission sought comment on ''whether to require applicants' and licensees' cybersecurity risk management plans to include provisions for identifying, assessing, and mitigating supply chain cybersecurity threats'' and proposed to require that plans cover all ''systems and services that could affect [applicants'/licensees'] provision of communications services.'' The *2024 Cable NPRM* also sought comment on whether the Commission should require the implementation of other ''common security controls to protect applicants' and licensees' systems and services.''

Additionally, several commenters urged the Commission to address physical risks. Most notably, the Committee ''additionally propose[d] applicants to certify that they have created, updated, and implemented comprehensive security risk management plans, consistent with industry best practices, for the cable systems that would also include supply chain risk management and physical security.'' Therefore, we require the risk management plans have measures to address physical security risks as well.

106. Beyond those baseline requirements, applicants and licensees will retain flexibility to tailor their cybersecurity and physical security risk management plans to the risks they face that could affect their provision of communications services through the submarine cable system and their organizational needs. Applicants and licensees will have flexibility to determine, for example, how to best mitigate the risks of compromised access controls by, at a minimum, using multifactor authentication or other suitable measures to protect their systems and services. Although we do not require applicants and licensees to follow any particular frameworks in creating their plans, we further find a plan will presumptively satisfy our requirements if it is structured according to an established risk management framework, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and incorporates best practices, such as the standards and controls set forth in the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Cross-Sector Performance Goals and Objectives (CISA CPGs), or the Center for internet Security's Critical Security Controls (CIS Controls). The plan should address both cybersecurity and physical security risks.

107. This approach is consistent with views of commenters that support a flexible approach to cybersecurity grounded in the NIST CSF. Given our approach and to reflect the evolving nature of cybersecurity risks, we decline to require that all plans include the six additional security controls identified in the *2024 Cable NPRM* or some other subset of common security controls. However, we still expect applicants and licensees to consider these types of controls, or reasonable alternatives, as may be necessary to mitigate the risks that they face or will face that could affect their provision of communications services through the submarine cable system. Importantly, the Committee emphasized in its reply comment, that the CISA CPGs and CIS Controls represent a ''baseline'' of cybersecurity measures ''that all licensees can and should surpass''—in other words, they are ''a floor, not a ceiling, when it comes to cybersecurity.'' Thus, allowing licensees and applicants to satisfy their duty under our rules by adopting a cybersecurity and physical security risk management plan that adheres to these well-established best practices ensures that submarine cable networks will be operated with a baseline of key security controls.

108. The rules promote the harmonization of cybersecurity certification requirements for licensees and applicants, as many commenters requested. CTIA and USTelecom suggest that the Commission should align its rules for submarine cable licensees with its rules for 5G Fund recipients. Submarine cable applicants and licensees that satisfy the requirements adopted in the *5G Fund Order* will necessarily also satisfy the requirements we impose today. Those rules require 5G Fund recipients to implement operational cybersecurity and supply chain risk management plans that ''must reflect'' the NIST CSF as well as ''established cybersecurity best practices that address each of the Core Functions described in the NIST CSF, such as the standards and controls set forth in'' the CISA CPGs or the CIS Controls. The same is true of the Commission's other rules governing the receipt of Universal Service Funds, which similarly require recipients' plans to reflect those sources. SCCL also urges us to also conclude that certain International Organization for Standardization (ISO) standards would satisfy the Commission's rules. While we do not conclude that compliance with any particular ISO standard would necessarily satisfy the rules, we observe that ISO standards, where appropriately mapped onto the NIST CSF's Core Functions, may also be useful to applicants and licensees seeking to comply and mitigate the risks they face or will face.

109. We agree with commenters on the importance of harmonizing cybersecurity certification requirements with requirements imposed by the Committee and other Executive Branch agencies. We find that licensees that have an existing mitigation agreement or are required to enter into a new mitigation agreement with the Committee, and who implement those agreements in full, will be presumed to satisfy the cybersecurity certification requirements. We expect that the logical security measures or other measures to prevent unauthorized or unlawful access, use, or disclosure of information being carried on a licensee's cable imposed by the Committee in such agreements will be comparable to, or more demanding than, the baseline measures we require here.

110. We stress that, while this is our expectation, a mitigation agreement would not satisfy the requirements of the rules if it does not comprehensively identify the cybersecurity risks that the licensee faces (including physical and supply chain risks), the controls it uses to mitigate those risks, and how it ensures that these controls are applied effectively to its operations. This approach is consistent with the Committee's request in its reply comments that the Commission work with the Committee to harmonize cybersecurity requirements to the extent possible, while supporting the Commission's proposed certification requirement and acknowledging that ''there may be instances where the Commission needs . . . information independent of the Committee's actions.'' NCTA suggests that the rules are unnecessary in view of the Committee's imposition of logical access requirements as part of its review. We disagree as the Committee does not review all cable landing license applications, therefore, not all cable landing licenses are subject to mitigation agreements. Instead, we agree with Microsoft that ''adoption of uniform rules for cybersecurity'' is important ''to avoid unnecessary duplication or complexity,'' and we establish a baseline certification requirement here that applies to all applicants and licensees, with the conditions in a mitigation agreement presumed to satisfy these requirements, which will contribute to a more streamlined approach across the U.S. government.

111. We also reject ICC's argument that the physical resiliency of submarine cable infrastructure should be the sole focus of the Commission's security requirements, and that adopting cybersecurity requirements that also address logical access and supply chain risks would ''significantly increase regulatory burden and privacy concerns without meaningfully increasing the security of the underlying data.'' While the most common threat to submarine cables remains physical damage from fishing, shipping, or undersea weather events, intentional damage from state or non-state actors using more subtle means of infiltration is ''of greater concern.'' These threats require holistic planning, including both cybersecurity and physical security. Physical resiliency protections (*e.g.,* identity

management, authentication and access controls) should also be included in applicants' and licensees' cybersecurity and physical security risk management plans, to the extent necessary to reasonably protect the confidentiality, integrity, and availability of their communications systems and services. While more difficult, infiltrators (including foreign adversaries) could also tap into cables to ''record, copy, or steal data'' for espionage, thereby compromising its confidentiality. This could occur through backdoors inserted during the cable manufacturing process, targeting onshore landing stations and SLTEs, or by tapping cables at sea. Encryption alone is insufficient to ensure cyber protections, as encrypted data can still be disrupted or delayed, and encrypted data can be exfiltrated and stored pending technological advances that will enable decryption and exploitation of the data at a later time. Although some of these attack vectors present technical challenges using current technologies, it is critical for cable systems to be secure into the future as technology advances.

112. Submarine cable infrastructure also faces a threat of malicious cyber activities that target the broader networks of which submarine cables represent only one link. Malicious actors may take advantage of vulnerabilities in these larger networks at locations with remote access to the submarine cable infrastructure to disrupt data flows, divert traffic, or delete data transmitted through the submarine cables, with serious consequences for the operational security of this critical infrastructure and the confidentiality, availability, and integrity of the information. Accordingly, we adopt cybersecurity and physical security risk management requirements to ensure that appropriate cybersecurity protections are in place against the physical, logical, and supply chain threats to applicants' and licensees' communications systems and services that could affect their provision of communications services through the submarine cable system.

113. We adopt commenters' suggestion to limit the scope of the cybersecurity certification requirement to the submarine cable system operator and the submarine cable network management systems only. In the interests of tailoring our requirements to the specific problem of submarine cable security and to limit regulatory burdens, the risk management plans only need to explain how the applicant or licensee takes or will take reasonable measures to employ its organizational resources and processes to ensure the confidentiality, integrity, and availability of its systems and services that could affect its provision of communications services through the submarine cable system.

114. *Senior Officer Review.* We adopt the Commission's proposal that an applicant's or licensee's Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Technology Officer (CTO), or a similarly situated senior officer responsible for governance of the organization's security practices, must sign the applicant's or licensee's cybersecurity and physical security risk management plan. We affirm that a signatory with organization-wide visibility and governance authority is critical to ensuring that the plan is comprehensively, effectively, and widely implemented.

115. Commenters raise a variety of concerns regarding this requirement. CTIA recommends harmonizing the signatory requirement with the *5G Fund Order,* which does not specify who must sign a plan. Microsoft contends that requiring senior staff signoff would be impractical for large network operators and suggests allowing entities to designate another appropriate authority within the organization. USTelecom expresses similar concerns, and suggests that a Chief Information Security Officer (CISO) or equivalent technical expert would be better positioned to assess and certify the plan's content. In response to these comments, we clarify that the requirement is not intended to impose unnecessary burdens or to prescribe a one-size-fits-all governance structure. Rather, the objective is to ensure meaningful executive oversight and accountability for cybersecurity and physical security risk management. Accordingly, we expressly recognize that an applicant's or licensee's CISO, or an equivalent officer with overall responsibility for the organization's security governance, qualifies as a ''similarly situated senior officer'' under this rule. This approach maintains the integrity of the executive accountability framework while providing sufficient flexibility for applicants and licensees to designate an officer who possesses the requisite authority and subject matter expertise.

116. *Submarine Cable Applications.* Applicants for a cable landing license must certify in the application that they have created and will implement and update a cybersecurity and physical security risk management plan consistent with the requirements herein. If an application for a cable landing license is filed prior to the effective date of the new rules and remains pending on or after the effective date of the new rules, the applicant(s) must submit a certification, within thirty (30) days of the effective date of the new rules, attesting that it will create and implement a cybersecurity and physical security risk management plan as of the date the submarine cable is placed into service. All licensees seeking a modification, assignment, transfer of control, or renewal or extension of a cable landing license must certify in the application that they have created, updated, and implemented a cybersecurity and physical security risk management plan and will take reasonable measures to protect their systems and services from cybersecurity risks that could affect their provision of communications services through the submarine cable system. We delegate authority to OIA to update application forms as necessary to include applicants' certifications.

117. *Routine Conditions for Licensees.* All licensees whose cable landing license is granted after the effective date of the new rules must implement a cybersecurity and physical security risk management plan as of the date the submarine cable is placed into service. We will require licensees to submit a certification, within thirty (30) days of the date the submarine cable is placed into service, that they have created and implemented a cybersecurity and physical security risk management plan as of the in-service date. Licensees must continue to implement and update the cybersecurity and physical security risk management plan, as required based on material changes to the cybersecurity and physical security risks and vulnerabilities that the licensee faces that could affect their provision of communications services through the submarine cable system.

118. *Implementation Timeline for Existing Licensees.* Existing licensees must implement a cybersecurity and physical security risk management plan within one year of the effective date of the new rules. To the extent an existing licensee does not commence service on the submarine cable by this timeframe, the licensee must implement a cybersecurity and physical security risk management plan as of the date the submarine cable is placed into service. Existing licensees must file a certification, within thirty (30) days of the effective date of the new rules, attesting that they will implement a cybersecurity and physical security risk management plan within this timeframe. The certification shall be submitted in the license file number(s) associated with the licensee's cable landing license(s) in ICFS. We find that this phased approach appropriately

balances the urgency of enhancing cybersecurity preparedness with the need to allow for thoughtful, effective plan development and integration into existing operations.

119. *Reporting Requirements and Confidentiality.* We adopt the Commission's proposal requiring that applicants and licensees submit cybersecurity and physical security risk management plans to the Commission upon request. We delegate to OIA, in coordination with PSHSB, the authority to request, at their discretion, submission of such plans and to evaluate them for compliance with the rules adopted in this proceeding. We decline to adopt NCTA's recommendation that the Commission should only obtain the plans based on a specific need. Access to these plans will enable the Commission to confirm whether cybersecurity and physical security risk management plans are being regularly updated, to review a specific plan as needed, or to proactively review a sample of plans to ensure they identify the relevant cybersecurity risks to communications systems and services. Consistent with the Commission's proposal and with the unanimous support of commenters, we will treat cybersecurity and physical security risk management plans as presumptively confidential under our rules. We agree with commenters that this approach will best protect and cultivate their cybersecurity practices.

120. *Recordkeeping.* We also adopt a recordkeeping requirement to support Commission oversight and ensure that applicants and licensees maintain accountability for creating and implementing their cybersecurity and physical security risk management plans. Specifically, applicants and licensees must preserve data and records related to their cybersecurity and physical security risk management plans, including documentation necessary to demonstrate how those plans are or will be implemented, for a period of two years from the date the related risk management plan certification is submitted to the Commission. We agree with FDD that ensuring documentation of cybersecurity efforts is important to bolster the resilience of submarine cable infrastructure and mitigate intrusions. Accordingly, we adopt the proposed two-year record retention requirement, which aligns with industry practices and supports our ability to assess compliance when needed.

121. *Third-Party Liability.* As part of today's action, we hold applicants and licensees responsible for the acts, omissions, or failures of third parties with whom the applicant or licensee has a contractual relationship, or whose acts or omissions the applicant or licensee otherwise has the ability to control, that impact the cybersecurity of the applicant's or licensee's systems and services. For purposes of this requirement, third parties include non-licensee individuals and entities with access to U.S.-licensed submarine cable systems that are hired by the licensee to provide services in connection with the management of the cable system (including service providers) and other third-party entities with access to the cable system's NOC. In connection with the Commission's requirement that an applicant or licensee take reasonable measures to protect the confidentiality, integrity, and availability of its communications systems and services, if an applicant or licensee relies on a third party to provide equipment or services, and an unreasonable act or omission of that third party results in the applicant's or licensee's failure to protect the confidentiality, integrity, or availability of its systems and services, the applicant or licensee will be responsible for that act or omission.

122. However, we find that reliance upon a third party to manage, route, or otherwise contribute to critical system operations does not relieve licensees of their cybersecurity responsibilities. The Commission has long held that ''licensees and other regulatees are responsible for the acts and omissions of their employees and independent contractors,'' and has recognized that ''under long established principles of common law, statutory duties are nondelegable.'' The risk of systemic harm to critical infrastructure warrants a regulatory approach that ensures licensees remain ultimately accountable for the security of their systems, including those operated or maintained by third parties.

c. Covered List Certifications

123. We adopt the proposal in the *2024 Cable NPRM* with some modifications, as described in detail below. We require applicants submitting initial cable landing license applications to certify that their submarine cable system will not use covered equipment or services (*i.e.,* the equipment or services identified on the Covered List). We require existing licensees to certify that they will not add covered equipment or services to their submarine cable system under the license in two scenarios, as described below. We further require licensees to disclose information about the covered equipment or services in their submarine cable system as part of the one-time information collection adopted today. We find that such equipment and services have been deemed to pose an unacceptable risk to the national security of the United States and the security and safety of United States persons. As discussed below, there is general support in the record for the proposal to protect U.S. communications networks and the communications supply chain against national security threats. These certifications will further both the Commission's efforts and whole-of-government efforts to prevent untrusted equipment or services from entering the submarine cable communications ecosystem.

124. *Covered List Certification for Cable Landing License Applications, and for Addition of New Segment to Currently Licensed Cable.* Specifically, we adopt the proposal that, as a condition of a potential grant of an application for a cable landing license, applicants are required to certify that the submarine cable system will not use equipment or services identified on the Commission's Covered List. At this time, we decline to require such certification based on entity lists of other Federal agencies or the Department of Commerce's identification of foreign adversaries in 15 CFR 791.4, which were discussed in the *2024 Cable NPRM.* In addition, we decline to require existing licensees to file a certification on or after sixty (60) days after the date that any equipment or service is newly placed on the Covered List, and instead seek comment in the *Further Notice of Proposed Rulemaking.* Applicants must certify that the submarine cable system will not use covered equipment or services. Since the Commission's Covered List was originally created, PSHSB has added multiple entries to the Covered List, the most recent as of July 23, 2024.

125. Many commenters are generally supportive of the use of the Commission's Covered List as a tool to promote national security. Equipment or services are placed on the Covered List based on a determination made by, among others, an appropriate national security agency that the equipment and/or services pose an unacceptable risk to the national security of the United States or the security and safety of United States persons pursuant to the Secure Networks Act. NASCA explicitly supports adopting the Commission's proposal to require applicants to certify that any proposed submarine cable systems will not use covered equipment or services. NASCA supports the Commission's proposal to ''require applicants . . . to certify whether or not

they use equipment or services identified on the Commission's 'Covered List,' provided the Commission's rules limit application to the relevant submarine cable system.'' We agree with NASCA and will require that the certification apply to the submarine cable system relevant to the particular application pending before the Commission.

126. We also require, as a condition of a potential grant of an application to modify a cable landing license to add a new segment, that applicants must certify that the new submarine cable segment and landing point will not use equipment or services identified on the Commission's Covered List. For example, if a licensee files a modification application to add a new landing point, the certification would apply to the segment connecting the submarine cable to the new landing point to ensure the protection of the new segment and landing point from any national security threats.

127. We are not persuaded by CTIA's argument that we should decline to prohibit the use of covered equipment or services in submarine cable systems because it would expand the Covered List ''in ways that were not originally contemplated by pertinent statutory authorities'' and ''without Congressional direction.'' The Commission's responsibility to place equipment and services on the Covered List is set out in section 2 of the Secure Networks Act, and both that Act and the Secure Equipment Act of 2021 impose certain related duties on the Commission. However, the Commission can adopt, and has adopted, certain requirements that are not specifically required by statute but that take into consideration the fact that the Covered List represents a list of equipment and services that have been determined to pose risks to national security and public safety. In fact, the Secure Equipment Act recognizes the Commission's legal authority to take actions concerning the Covered List to fulfill the Commission's national security mission. We act here pursuant to our authority under the Cable Landing License Act and on the basis of this record to prevent new or additional insecure equipment and services from being integrated into this critical U.S. infrastructure by a cable landing licensee.

128. Finally, we received a variety of viewpoints on using other federal government lists. For example, SentinelOne supports expanding the sources used for identifying untrusted equipment, encouraging the Commission ''to align its Covered List with other federal authorities, including the Department of Defense's 1260H list, the Department of Commerce Bureau of Industry and Security Entity List, and related U.S. Government assessments.'' TIA argues that while it makes sense to rely on the Covered List to limit the participation by untrusted vendors, the Commission should also collaborate with its national security counterparts in the federal government to investigate the need for additional restrictions. We are not prepared at this time, however, to draw from the lists of those other federal agencies or apply the certification requirement to all vendors ''from'' foreign adversaries, given the uncertain nature of this latter category. Rather, in the *Further Notice of Proposed Rulemaking,* we propose instead to extend this certification requirement to communications equipment and services produced or provided by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g). In the meantime, we will continue to rely on the Commission's Covered List, which Congress has directed the Commission to maintain and which is specific to communications equipment and services.

129. *Covered List Certification for Cable Landing Licenses.* To enhance the security of submarine cable systems, we adopt the Commission's proposals in the *2024 Cable NPRM,* with some modifications. We require cable landing licensees to certify that they will *not add* to the submarine cable system under the license (or if a licensee holds multiple licenses, for each submarine cable system under each license), covered equipment or services. Licensees shall submit this certification within sixty (60) days of the effective date of the new rules. In the *2024 Cable NPRM,* the Commission proposed to require licensees to certify whether they use, for the relevant submarine cable system, equipment or services identified on the Covered List, and sought comment on a requirement to remove the covered equipment or service. Some commenters support the certification proposal, while others explain that for substantially launched or completed projects, the replacement costs for covered equipment or services may have substantial cost constraints. Others oppose the certification proposal and disfavor suggestions to replace equipment or services, explaining that the Committee's role with respect to monitoring individual submarine cables and the respective mitigation agreements with licensees address national security concerns.

130. We provide an exception to this certification requirement for existing licensees that are entities identified on the Commission's Covered List. Such entities identified on the Covered List can continue to add covered equipment or services on their submarine cable system. Based on the determinations that equipment or services produced or provided by entities on the Covered List have been found to present national security risks, the Commission believes there is little national security benefit to prohibiting their use of covered equipment or services on their submarine cable system. Rather, the risks these entities pose are best mitigated through the presumptive disqualifying conditions and the Foreign Adversary Annual Report that we adopt in this *Report and Order.*

131. We find that it is premature to establish a ''rip and replace''-like framework for current submarine cable infrastructure. We recognize that for existing licensees with covered equipment or services, there are costs associated with replacing these equipment or services, as well as other challenges, as suggested by commenters. Unlike the context of section 4 of the Secure Networks Act, where funds have been allocated to reimburse entities that are required by the federal government to remove equipment determined to present a national security risk, no such funds have been appropriated for submarine cable systems. Under these circumstances, we find that requiring licensees to replace existing covered equipment or services in their submarine cable systems would be overly burdensome and could have adverse effects, such as fewer deployment of submarine cables or related facilities.

132. In addition, given the national security risks and threats posed by covered equipment or services, and the Commission's responsibilities as a licensing agency for submarine cables, we believe that the Commission should have a greater understanding of the covered equipment or services involved with licensed submarine cables. While the Committee may have individual mitigation agreements with certain cable landing licensees, the Commission is in the position as the licensing agency for submarine cables to understand the collective U.S. submarine cable ecosystem. Therefore, we modify the proposed scope of the certification and require licensees to certify that they will not add to their submarine cable systems, covered equipment or services that are currently identified or newly identified in the future. Licensees will be required to provide this certification

in ICFS no later than sixty (60) days of the effective date of the new rules.

133. *Covered List One-Time Information Collection From Licensees.* We adopt the Commission's proposal in the *2024 Cable NPRM,* with some modifications, to require existing licensees to disclose as to whether or not their submarine cable systems use equipment or services identified on the Covered List. We require licensees to disclose this information as part of the one-time information collection adopted in this *Report and Order.* In the *2024 Cable NPRM,* the Commission proposed to require licensees to provide a certification as to whether or not they use, for the relevant submarine cable system, equipment or services identified on the Covered List within sixty (60) days of the effective date of any rule adopted in this proceeding, following approval by OMB. While commenters express support or do not otherwise object to the proposal to require licensees to certify whether or not they use covered equipment or service in their respective cables, we require this certification in the one-time information collection and require licenses to respond with information about their respective submarine cables and any use of equipment or services identified on the Commission's Covered List as of the date that OIA publishes notice of the effective date of the information collection requirement and the filing deadline in the **Federal Register**.

*E. New Routine Conditions for Cable Landing Licenses*

134. We adopt new routine conditions and modify the Commission's existing routine conditions that are attached to cable landing licenses under § 1.767(g) of the current rules. The routine conditions we adopt: (1) eliminate a distinction that applies the routine conditions only to licensees of a cable landing license granted on or after March 15, 2002, (2) ensure the protection of this critical submarine cable infrastructure through prohibitions, (3) require commencement of service within three years following the grant of a cable landing license, and (4) require important updated information regarding the submarine cable system, including contact information. These measures are necessary to ensure that licensees remain vigilant against foreign adversary threats and that the Commission has updated and accurate information about licensees and the operation of licensed submarine cable systems. The routine conditions will promote the security, integrity, and resilience of critical submarine cable infrastructure.

135. *Eliminate 2002 Distinction.* We adopt the proposal to eliminate the distinction in § 1.767(g) that applies the routine conditions only ''to each licensee of a cable landing license granted on or after March 15, 2002.'' No commenter addressed this issue. As the Commission explained in the *2024 Cable NPRM,* we believe that this distinction is no longer meaningful given that cable landing licenses granted prior to March 15, 2002 either have expired or are nearing the expiration of their 25-year term. Further, to the extent we grant applications to renew the license of a submarine cable, our current practice is to issue a new cable landing license based on the rules in effect at the time of renewal, instead of renewing the terms of the license that were in effect prior to March 15, 2002. We therefore modify § 1.767(g) by eliminating the text ''granted on or after March 15, 2002'' and apply the routine conditions, as amended in this proceeding, ''to each licensee of a cable landing license'' irrespective of the date of grant.

136. *Prohibition on IRUs and Capacity Leases with Foreign Adversaries.* As discussed above, to further protect U.S. communications networks from national security, law enforcement, and other threats, we adopt a routine condition that prohibits cable landing licensees from entering into new or an extension of existing arrangements for IRUs or leases for capacity on submarine cable systems landing in the United States, where such arrangement or lease would give an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g), the ability to install, own, or manage SLTE on a submarine cable landing in the United States. This routine condition will ensure compliance with the prohibition and ensure the security, integrity, and resilience of this critical infrastructure against foreign adversary threats.

137. *Prohibit Licensees from Adding Covered Equipment or Services.* Consistent with the actions we take in this *Report and Order,* we adopt a routine condition that a licensee whose application for a cable landing license is filed and granted after the effective date of the *Report and Order,* shall not use equipment or services identified on the Covered List on its submarine cable system subject to the license. A licensee whose modification application to add a new segment is filed and granted after the effective date of the *Report and Order,* shall not use covered equipment or services on the new segment and the new landing point. Cable landing licensees shall not add equipment or services currently identified or newly identified in the future on the Covered List to their submarine cable system(s) subject to their respective license(s), with an exception discussed above. In the *Further Notice of Proposed Rulemaking,* we propose, among other things, to adopt a routine condition that requires cable landing licensees, irrespective of when the license was granted, to certify, within sixty (60) days of a **Federal Register** publication announcing any new addition of equipment or services to the Covered List, if they use such covered equipment or services in their respective submarine cable system.

138. *Foreign Adversary Annual Report.* As discussed below under section III.G., we adopt a new routine condition requiring a cable landing licensee whose license was or is granted prior to the effective date of the new rules, to file a Foreign Adversary Annual Report if such licensee meets one or more of the criteria specified therein.

139. *Commencement of Service Requirement.* We adopt a routine condition requiring that a licensee must commence commercial service on the submarine cable under its license within three years following the grant of the license or submit a waiver request. In the *2024 Cable NPRM,* the Commission tentatively concluded that cable landing licensees should retain their license only if they construct and operate the submarine cable under that license. The Commission proposed to require a cable landing licensee to commence commercial service on the cable under its license within three years following the grant, and that if a licensee requested a waiver of the three-year time period, the licensee must identify the projected in-service date and reasons for the delay and demonstrate good cause for grant of a waiver.

140. We did not receive comment on this proposal, and we adopt it as a routine condition on all grants of a cable landing license granted after the effective date of the new rules. We find this requirement would provide the Commission with more accurate information as to which license grants were not utilized to construct and operate submarine cables and improve the administration of the Commission's rules. Failure to notify the Commission of commencement of service within three years following the grant of the license shall result in automatic termination of the license after seeking approval of the State Department, unless

the licensee submits a waiver request. If a licensee cannot commence commercial service during that time period, we require the licensee to submit a waiver request and provide an expected in-service date, explain the reasons for delay, and show why the license should not be terminated. Upon a showing of good cause, the Commission may extend the date to commence service beyond the three-year period.

141. *Notification of Name Changes of the Licensee or Submarine Cable System.* We adopt the Commission's proposal to add a new routine condition requiring licensees to notify the Commission of any changes to the name of the licensee (including the name under which it is doing business) or the name of the submarine cable system within thirty (30) days of such change. We adopt a slightly modified version of the proposal to require the lead licensee to file the notification with the Commission if there are multiple licensees of the submarine cable system. Specifically, we will require that the lead licensee file a notification of any change in the name of the submarine cable system within the 30-day timeframe. We will require each licensee to notify the Commission of any changes to its own name within the 30-day timeframe as each licensee is best situated to know and timely disclose this information. As the Commission explained in the *2024 Cable NPRM,* it is important for the Commission to maintain updated information that is critical to identifying the licensees and the licensed submarine cable system. No commenter addressed this proposal.

142. *Changes in the Points of Contact.* We adopt the proposal to add a new routine condition requiring cable landing licensees to notify the Commission of any changes to their contact information within thirty (30) days of such change. Specifically, cable landing licensees must inform the Commission of any changes to the contact information provided in their most recent submarine cable application—including the application for a new cable landing license or any modification, assignment, transfer of control, or renewal or extension of the license—and the most recent Foreign Adversary Annual Report if applicable. We did not receive comment on this. Among other things, it is essential for the Commission to maintain updated contact information for the appropriate points of contact to whom any matters concerning a licensed submarine cable may be addressed for national security, law enforcement, and emergency preparedness and response purposes, including where a cable is rendered inoperable.

*F. Other Changes to Current Requirements*

1. Existing Streamlining Process

143. In noting existing licensing delays, commenters indicate that applications that qualify for streamlining under the Commission's rules often are removed from streamlined processing. Commenters encourage the Commission to use the existing streamlining process. While the *Further Notice of Proposed Rulemaking* is pending, and to streamline the processing of submarine cable applications during this time, we will consistently implement our streamlined processing rules and not defer action on a submarine cable application unless the Committee provides specific and compelling national security, law enforcement, or other justifications to defer action. Applicants seeking streamlined processing must certify, among other things, that ''all ten percent or greater direct or indirect equity and/or voting interests, or a controlling interest, in the applicant are U.S. citizens or entities organized in the United States.'' We believe that our streamlined processing rules, combined with the strong national security measures we adopt in this *Report and Order*—including presumptive disqualifying conditions, prohibitions, and information and certification requirements—to identify and mitigate foreign adversary threats to new and existing submarine cable systems would lessen the need in many cases to refer applications that qualify for streamlined processing. We note that Executive Order 13913 continues to apply and is effective when the Commission refers an application to the Committee, or when the Committee reviews ''existing licenses'' to identify any additional or new risks to national security or law enforcement interests of the United States.

2. Renewal Applications, Extension Applications, and Streamlined Processing

144. We adopt a rule specifying the requirements for an application to renew or extend a cable landing license upon expiration of the 25-year license term. Specifically, we adopt the proposals set out in the *2024 Cable NPRM* to require applicants for renewal or extension of an existing cable license to provide the same information and certifications required in an application for a new license. Applicants for a license renewal or extension must also provide a public interest statement demonstrating how grant of the renewal application will promote and protect national security and serve other statutory objectives. NASCA states that licensees should not be required to restate information to the Commission that has not changed, noting the Commission's proposal to require periodic reports. It has been the case that there are often changes in the licensees of a cable when a cable landing license is renewed or extended. Further, since we are not adopting the proposal to file periodic reports updating information about the cable system and the licensees, except for foreign adversaries, there may have been numerous changes to the cable system and licensees that have not been reported to the Commission and the information the Commission has on the cable may be outdated.

145. *Renewal or Extension Must be Filed Six Months Prior to License Expiration.* We adopt the proposed rule to require licensees to file an application for renewal or extension of a license six months prior to its expiration. Upon the filing of a timely and complete application in accordance with our rules, a licensee may continue operating the cable system while the application is pending with the Commission. NASCA supports the Commission's proposal to allow a licensee to continue to operate the cable system while its renewal application is pending with the Commission. In cases where the renewal or extension application is not filed six months prior to the expiration and the Commission has not acted on the renewal or extension application prior to expiration of the license, the licensees will need to file a request for special temporary authority (STA) to continue to operate the cable past the expiration of the license, unless the Commission has granted a waiver of the rules to allow continued operation before then. The licensees should file the STA request at least 30 days prior to the expiration of the license to allow the Commission to process and act on the STA request prior to the expiration of the license.

146. *Renewal or Extension Streamlined Processing Procedures.* We adopt with one modification the proposals made in the *2024 Cable NPRM* regarding streamlined processing for renewal or extension applications similar to the existing 45-day streamlined process for initial applications. NASCA states that any renewal process should be streamlined, with non-streamlined processing being the exception even if there is foreign

ownership. Upon further reconsideration and in light of the comments from NASCA, we modify the criteria to allow for streamlined processing if the only reportable foreign ownership has previously been reviewed by the Commission and the Committee. In cases where the only reportable foreign ownership in a renewal or extension application has been previously reviewed by the Commission and the Committee, we will follow our current procedure and not formally refer the renewal or extension application but will send a courtesy copy of the Accepted For Filing public notice to the Executive Branch agencies.

147. We will place a renewal or extension application on streamlined Accepted for Filing public notice and take action on such application within forty-five (45) days after release of the public notice if: (1) the Commission does not refer the application to the Executive Branch agencies because (a) the applicant does not have reportable foreign ownership, as defined in § 1.40001(d), or (b) the only reportable foreign ownership is not ownership or control by a foreign adversary, as defined in § 1.70001(g), and has been previously reviewed by the Commission and the Committee and (c) the application does not raise other national security or law enforcement concerns, or other considerations warranting Executive Branch review; (2) the application does not raise other public interest considerations, including regulatory compliance; (3) the Executive Branch agencies do not separately request during the comment period that the Commission defer action and remove the application from streamlined processing; (4) no objections to the application are timely raised by an opposing party; and (5) any proposed grant of a renewal or extension application is approved by the State Department.

3. Requirements To File a Modification Application

148. We adopt the proposal in the *2024 Cable NPRM* to set out in the rules what changes to a submarine cable system require the filing of a modification application or a notification and the process for review of those filings. Based on the comments, we make changes to the proposals to minimize the burden on licensees where a change to an existing cable system does not present additional risks with the cable system, but will require that the licensee(s) notify the Commission about those changes. Specifically, we will require licensees to file modification applications and receive prior approval from the Commission before adding a new landing point or a new licensee to a cable system. For other changes to the cable system, the licensees will be required to file a notification of the change in the cable with the Commission. The removal of a landing point or a licensee or a change in a national security condition on a cable landing license will require a post-action notification which must be filed within 30 days after the change occurs. In situations where two Commission-licensed cable systems will interconnect in waters beyond the U.S. territorial waters or a new segment and landing point will be added to connect two (or more) foreign points and the connection cannot be used to connect directly or indirectly with the United States, the licensee(s) must notify the Commission 90 days prior to the change taking effect.

a. New Landing Point or New Licensee

149. As was discussed in the *2024 Cable NPRM,* the addition of a new landing point or a new licensee is a major change to a cable landing license that requires an application and Commission approval before the change takes place. ICC and NASCA agree that these are major changes to a cable. As proposed in the *2024 Cable NPRM,* we will continue our current practice and require a full application for these types of changes to a cable system. Applications for a new landing point must describe the proposed new landing point including the exact location, how the new landing point will be connected to the cable, and the ownership and control of any new U.S. landing point and the segment connecting the cable to the new landing point. In situations where a landing point is being moved within the same town/city/county as approved in the cable landing license, the licensee(s) need only file a letter informing the Commission of the new location of the landing within 30 days of the change of location. An application to add a new licensee must provide the contact information for the proposed licensee, its ownership and the specific ownership interest it will have in the cable system, and how the ownership interests of the other licensees will change with the new licensee. If the proposed new owner has reportable foreign ownership or the licensees on a cable proposing a new cable landing point have reportable foreign ownership, the application will be subject to our rules and policies regarding coordination of submarine cable applications with the Executive Branch.

b. Removal of a Licensee or Landing Point, or Change in a National Security Mitigation Condition

150. We find that removal of a previously approved landing point, licensee, or condition to comply with a national security mitigation condition does not raise concerns that would normally require a full application. Based on the record in the proceeding, we agree with ICC and NASCA that certain types of changes to a submarine cable system, such as the removal of a licensee or a cable landing point or a minor change in the location of an existing landing point can be handled through a notification to the Commission. Consequently, we will not adopt the proposal in the *2024 Cable NPRM.* Instead, we will require the licensee(s) to file a notification with the Commission within 30 days of the change. Similar to a *pro forma* transaction notification, the Commission will place the notification of the change to the cable landing license on public notice. In cases where the proposed change involves adding or modifying a condition requiring compliance with a mitigation agreement with the Committee regarding national security and law enforcement concerns, the modification will be effective upon public notice.

151. *Relinquishment by a Licensee.* Notifications filed by a licensee that relinquished an interest in the submarine cable must contain the following information: (1) the name of the licensee relinquishing its interests in the cable; (2) the ownership interests held by that licensee prior to the relinquishment; (3) whether the licensee relinquished all its interests or whether it is seeking to be removed as a licensee because its interests decreased to a point where it is no longer required to be a licensee (in which case, the remaining interest must be identified); (4) an explanation of what happened to the interests that were relinquished (*i.e.,* were the interests re-distributed pro rata amongst the remaining licensees or otherwise re-distributed); and (5) a certification that the remaining licensees retain collectively *de jure* and *de facto* control of the U.S. portion of submarine cable system sufficient to comply with the requirements of the Commission's rules and any specific conditions of the license. The filer must also certify that the notification has been served on all the other licensees of the cable. This requirement will also apply to joint licensees of a submarine cable that collectively relinquish the license.

152. *Removal of a Licensee by the Other Licensee(s) on the Cable Landing License.* We adopt a rule based on the *2024 Cable NPRM* by which joint licensee(s) of a consortium submarine cable may collectively request the removal of a licensee that no longer exists from the cable landing license. Under this rule, if any joint licensee(s) of a submarine cable no longer exists and is unable to file a notification to modify the license to relinquish its interest in the license, the remaining joint licensee(s) of the cable, if any, may collectively file a notification to remove the licensee from the license by demonstrating and certifying that (1) the licensee no longer exists as a legal entity, and (2) the remaining joint licensee(s) retain collectively *de jure* and *de facto* control of the U.S. portion of the submarine cable system sufficient to comply with the requirements of the Commission's rules and any specific conditions of the license. Any notification submitted under this rule shall be certified and signed by each remaining joint licensee(s) of the submarine cable, respectively. Joint licensees may appoint one party to act as proxy for purposes of complying with this requirement.

153. *Removal of a Landing Point.* Notifications regarding the removal of a landing point must contain the following information: (1) specific identification of the landing point that was removed from the submarine cable and the segment connecting the cable to that landing point; (2) an explanation of what happened with the physical facilities of the landing point and the connecting segment upon removal from the cable; (3) an explanation of how the removal affected the ownership of the remaining portions of the cable; and (4) updated information on the cable with the removal of the landing station and connecting segment.

154. *Changes to National Security Condition.* Notifications regarding changes to a condition requiring compliance with a national security mitigation agreement—typically either a letter of agreement (LOA) or a national security agreement (NSA)—must explain the change that has occurred. The notification must explain whether the condition is being removed or if the mitigation agreement is being replaced. If an existing mitigation agreement is being replaced with a new agreement, a copy of the new mitigation agreement must be included in the filing. The removal of the condition or the replacement of the condition will be effective upon release of the public notice.

c. Adding an Interconnection Between Two Commission-Licensed Cables

155. We adopt a pre-action notification requirement when two Commission-licensed cables propose to interconnect. In the *2024 Cable NPRM,* the Commission proposed to require that a modification application be filed when two licensed cables interconnect in the water. Both the Coalition and NASCA object to this proposal, arguing that because there are no new landing points and no change in ownership of the two cables, such an interconnection does not require Commission approval or filing of a modification application. Although the Coalition argues that the Commission has no jurisdiction over interconnections in international waters, NASCA acknowledges that the Commission can require notification of an interconnection. We have jurisdiction as these interconnections allow for direct connections to the United States from these cables to new landing points that were not set out or approved in their respective cable landing licenses. We do acknowledge, however, that these landings have been approved for the pre-interconnecting cable configuration and thus these interconnections present a lower risk than the addition of new landing points never previously approved.

156. Although such a change may not raise concerns, there may be instances where an interconnection—whether it be in U.S. territorial waters or outside of U.S. territorial waters—may raise national security concerns and the Commission should be notified about such a change in advance. Accordingly, we adopt procedures for such changes similar to the process used for landing point notifications. Licensees will be required to file a notification about a proposed interconnection at least 90 days prior to the construction of the proposed interconnection. The Commission will give public notice of the notification of modification. The modification will be considered granted, without further Commission action, unless the Commission notifies the licensees otherwise in writing no later than 60 days after the submission of the notification. If, upon review of the notification, the Commission finds that such an interconnection presents a risk to national security, law enforcement, foreign policy and/or trade policy or raises other concerns, it may require the licensee(s) to file a complete modification application to seek Commission approval for the interconnection. We find that this notification process will be less burdensome on licensees than the full modification process proposed in the *2024 Cable NPRM.*

157. The notification about a proposed interconnection must be filed 90 days prior to construction of the proposed connection. The filing must include information on: (1) the cable systems being interconnected, including the names and file numbers for the cables and (2) a general description of where the interconnection will take place and the terms of the interconnection agreement.

d. New Connection Between a Branching Unit of a Licensed Submarine Cable System and a Foreign Landing Point

158. We agree with the Coalition and NASCA that if a new segment and landing point only connects two (or more) foreign points and the connection cannot be used to connect directly with the United States, the segment does not need to be licensed by the Commission. In the *2024 Cable NPRM,* the Commission proposed to require a modification application be filed when a new segment from a foreign country is connected to a branching unit of the licensed submarine cable system to allow connection to another foreign country. The Coalition and NASCA both oppose this proposal arguing that such connections are outside of Commission jurisdiction. Such a new connection using a U.S.-licensed cable does affect the cable, however, and the Commission should be aware of the proposed connection. We find that the Commission should have an opportunity to review the proposed connection before it is constructed to determine if the Commission agrees that there will not be a direct connection to the United States and thus the connection requires the filing of a modification application. Therefore, we will require the licensee(s) to file a notification with the Commission at least 90 days before construction of the proposed connection. The modification will be considered granted, without further Commission action, unless the Commission notifies the licensees otherwise in writing no later than 60 days after the submission of the notification. If, upon review of the notification, the Commission finds that such a connection presents a risk to national security, law enforcement, foreign policy or trade policy and/or raises other concerns, it may require the licensee(s) to file a complete modification application to seek Commission approval for the connection.

159. The filing must include: (1) the name and file number of the U.S.

licensed cable whose branching unit will be used to make the proposed connection between two (or more) foreign points; (2) a description of the proposed connection, including which foreign points would be connected; (3) the relationship between the owner of the proposed connection and the licensees; and (4) an explanation of how the proposed connection would not allow for direct connection from the new foreign point(s) to the United States. This will allow the Commission to determine if this new connection would allow direct connection to the United States and require a full application for prior Commission approval.

4. New Requirements for Assignments and Transfer of Control Applications

160. We adopt the proposal to require that an applicant seeking to assign or transfer control of a cable landing license must include the percentage of voting and ownership interests being assigned or transferred, including in the U.S. portion of the cable system, which includes all U.S. cable landing station(s). The applicant must also demonstrate that grant of the transaction will serve the public interest. In addition, the rule regarding assignments and transfer of control applications is amended to incorporate the changes adopted herein for all applications, including the required certifications. No commenter addressed these proposals.

5. Pro Forma Assignment and Transfer of Control Post-Transaction Notifications

161. We adopt the proposal to have a separate rule section regarding notification of *pro forma* assignments and transfers of control. By creating a specific section for *pro forma* assignments and transfers of control, we provide clarity on the requirements for such notifications. Section 1.70013 of our newly adopted rules also provides information on what constitutes a *pro forma* transaction. We decline to adopt the Commission's earlier proposal that a *pro forma* notification contain substantially the same information as required for a substantive transaction, and instead, streamline the requirements. NASCA argues that there is no need for a *pro forma* notification to mirror a substantive transaction application, stating that with the significant reporting updates proposed in the *2024 Cable NPRM,* a licensee would be providing the same information repeatedly. ICC argues that *pro forma* notifications should be streamlined and requiring the inclusion of the same information as substantive transactions would undermine the simplicity of the notifications.

162. Under the rules we adopt, a licensee will continue to be required to file a *pro forma* notification no later than thirty (30) days after the assignment or transfer of control is consummated. In response to NASCA and ICC, we will not mirror the requirements of applications for substantive transactions but instead adopt streamlined *pro forma* notification rules. Consistent with our practice, the notification must include information about the transaction, including (1) the contact information and place of organization of the assignor/transferor and the assignee/transferee, (2) the name of the submarine cable system, (3) a narrative describing the means by which the *pro forma* assignment or transfer of control occurred, (4) ownership information as required in § 63.18(h), including both the pre-transaction and post-transaction ownership diagram of the licensee, (5) specification, on a segment specific basis, of the percentage of voting and ownership interests that were assigned or transferred in the cable system, including in the U.S. portion of the cable system (which includes all U.S. cable landing station(s)), (6) a certification that the assignment or transfer of control was *pro forma,* as defined in § 1.70013(b), and, together with all previous *pro forma* transactions, does not result in a change of the licensee's ultimate control, and (7) a certification that the assignee or the transferee and the licensee that is the subject of the transfer of control accepts and will abide by the routine conditions of the cable landing license as specified in § 1.70007. The notification must include the foreign carrier affiliation information and certifications currently required in § 1.767(a)(8)(ii) through (iv), and the certifications required in § 63.18 (o) and (q) for the assignee or the transferee and the licensee that is the subject of the transfer of control.

163. Additionally, to ensure the Commission has up-to-date information on national security or compliance matters affecting a cable landing license, we will require that notifications of *pro forma* transactions contain the same certifications as applications for substantive transactions as to whether or not the licensee, assignor/transferor, or assignee/transferee exhibit any of the criteria set out in the foreign adversary and character presumptive disqualifying conditions that will apply to certain applications as discussed above.

6. Requests for Special Temporary Authority (STA)

164. We adopt the proposal to create a rule specific to requests for an STA for submarine cables rather than continuing to rely on the STA rule in Part 63 for temporary or emergency service by international carriers. Generally, the Commission will consider requests for an STA: (1) seeking to commence construction of or commercial service on a cable system while the cable landing license or modification application is pending Commission approval; (2) seeking to continue operating a cable system following the expiration of a license and pending the filing of an application to renew or extend the cable landing license when the renewal or extension application is not filed in a timely or complete manner; (3) where the cable system is being operated without first obtaining a license; (4) where a transaction was consummated without prior Commission consent; or (5) seeking to provide emergency service arising from a need occasioned by conditions unforeseen by, and beyond the control of, the licensee(s), among other examples. ICC is generally supportive of the proposals related to STAs.

165. An application for an STA must include the following information: (1) the name(s), contact(s), and citizenship(s) or place(s) of organization of each applicant requesting an STA with respect to the submarine cable, including the licensees that jointly hold a cable landing license; (2) the name of the cable system for which applicant(s) request an STA; (3) a description of the request for an STA: (a) the reason why the applicants seek an STA, (b) whether it is a new request for an STA, a request to extend or renew an STA, or other type, and (c) the justification for such request, including why grant is warranted; (4) the date by which applicants seek grant of the STA; and (5) the duration for which applicants seek an STA (up to 180 days). Applicants must acknowledge that any grant of an STA (1) does not prejudice action by the Commission on any underlying application(s); (2) is subject to revocation/cancellation or modification by the Commission on its own motion without a hearing; (3) will expire automatically upon the termination date unless the applicant has made a timely and complete application for extension of the STA; and (4) does not preclude enforcement action for non-compliance with the Cable Landing License Act, the Communications Act, or the Commission's rules for action or failure

to act at any time before or after grant of the STA.

166. If the STA application relates to a licensed cable or a cable whose license expired, the applicant(s) must provide the license file number(s) of the cable landing license. If the request for an STA is associated with an application(s) pending with the Commission (*e.g.,* application for a new license, or modification of an existing license), the applicants must provide the file number(s) of the application(s). If the STA application relates to unauthorized operation of a cable system, including unauthorized operation of a segment/branch of a licensed system or operating a submarine cable system after the expiration of its license, and an application seeking authority for such operation has not yet been filed (*e.g.,* application for a new license or modification or renewal or extension of an existing license), the STA applicant(s) must include information on when the application seeking authority to operate will be filed.

167. All STA applications require a certification that none of the applicant(s) are subject to a denial of Federal benefits pursuant to of the Anti-Drug Abuse Act of 1988. If the STA application is for operation of the cable system, the applicant(s) must include the certifications required in an application for a new cable landing license, with the exception of § 1.70006(d).

168. We will continue to follow our current practice related to STA applications. Once an STA application is found to be Acceptable For Filing, we will place it on public notice for comment. While we will not formally refer the STA application to the Executive Branch agencies, we will send a courtesy copy of the public notice to the Executive Branch agencies if any of the applicants have reportable foreign ownership. The Commission may consult with the Committee on a particular request for an STA, where appropriate, prior to releasing the public notice. Any grant of an STA does not prejudice action by the Commission on any underlying application, including enforcement action.

7. Foreign Carrier Affiliation Notifications

169. We adopt the Commission's proposal to amend § 1.768(e)(4) of the rules to require that licensees must include voting interests in a notification of a foreign carrier affiliation, in addition to the equity interests, and a diagram of individuals or entities with a 10% or greater direct or indirect ownership in the licensee. Currently, a licensee is required to include, among other things, in a foreign carrier affiliation notification ''[t]he name, address, citizenship, and principal business of any person or entity that directly or indirectly owns at least ten percent (10%) of the equity of the licensee, and the percentage of equity owned by each of those entities (to the nearest one percent (1%)).'' In the *2024 Cable NPRM,* the Commission proposed revisions to § 1.768(e)(4) that would be consistent with the ownership reporting requirements of other submarine cable applications and notifications. Specifically, we amend § 1.768(e)(4) to require that licensees must provide the name, address, citizenship, and principal businesses of any individual or entity that directly or indirectly owns 10% or more of the equity interests and/or voting interests, or a controlling interest, of the licensee, and the percentage of equity and/or voting interest owned by each of those entities (to the nearest one percent). We find there is a public benefit in ensuring that ownership reporting requirements are consistent across the Commission's submarine cable rules. We disagree with NASCA who argues that the Commission should ''only require ownership restatements with substantive applications involving a change in control or notification of *pro forma* ownership changes.'' Any application that a licensee is required to file thereafter should include relevant and consistent information.

170. NASCA also contends that the Commission should ''reassess the rule's purpose'' and ''the rule should be narrowed to apply only to foreign carriers in the countries where the relevant cable lands,'' but offers no justification for this proposal nor explains with particularity how this would be implemented. In any event, we find that our regulatory framework ensures that the Commission considers whether foreign participation in U.S. markets would raise national security, law enforcement, foreign policy, and/or trade policy concerns due to an applicant's foreign ownership, as well as potential anti-competitive behavior by a carrier with market power at the foreign end of a U.S. cable.

8. Other Administrative Changes

171. *Contact Information.* We adopt the proposals in the *2024 Cable NPRM* regarding requirements for applicants to provide contact information. Specifically, we amend the rules to expressly require the provision of contact information for applications to modify, renew or extend a cable landing license. We will also require all applicants for cable landing licenses and for modification, assignment, transfer of control, and renewal or extension of licenses to provide an email address on behalf of the applicant and an email address on behalf of the officer and any other contact point, to whom correspondence regarding the application can be addressed. In addition, we require while an application is pending for purposes of § 1.65 of the rules, the applicant for a modification and renewal or extension of a cable landing license must notify the Commission and the Committee of any changes in the licensee information and/or contact information promptly, and in any event within thirty (30) days. We did not receive any comments on these proposals.

172. *Eliminate Certain Rules.* We adopt the proposals to eliminate record-keeping or disclosure rules, 47 CFR 1.767(c), (d), and (f), as described in the *2024 Cable NPRM,* because they are no longer applicable or consistent with the Commission's current rules or practice. These actions today strike a balance between modernizing the rules for current needs and securing sensitive submarine cable infrastructure information.

173. In the *2024 Cable NPRM,* the Commission proposed to remove 47 CFR 1.767(c) and (d). These rule requirements direct the Commission to keep: (a) original applications, documents and exhibits for submarine cable licenses the Commission granted since June 30, 1934, with some exceptions for certain maps; and (b) original files, license applications, and licenses for cable landing operations prior to June 30, 1934. Both rules either permanently or on a temporary basis, directed the Commission to hold these files for public inspection. No comments were received on the proposals. These rules no longer reflect current record keeping requirements, are not statutorily required under the Cable Landing License Act or Executive Order 10530, nor are they consistent with a different rule, § 1.767(n)(1), that requires information filed in § 1.767 be submitted electronically. Therefore, we adopt the Commission's proposals and eliminate § 1.767(c) and (d).

174. Similarly, in the *2024 Cable NPRM,* the Commission proposed to remove 47 CFR 1.767(f). This rule directs submarine cable applicants to furnish information about submarine cables' construction location and timing, within 30 days upon written request from the public. No comments were received on this proposal. We find that the requirement in § 1.767(f) to disclose information is inconsistent

with a different rule, § 0.457(c)(1)(i), which provides that cable maps with exact locations should be withheld from public inspection. Further, this requirement is inconsistent with the proposal in the *2024 Cable NPRM* to provide confidential treatment for the exact addresses and specific geographic coordinates of cable landing stations, beach manholes, and other sensitive locations associated with a submarine cable system.'' Thus, we adopt the proposal to eliminate § 1.767(f).

175. *Amendments.* We adopt the proposal to codify long standing practices regarding amendments to pending submarine cable applications. No commenter addressed these proposals. Any submarine cable application may be amended as a matter of right prior to the date of any final action taken by the Commission or designation for hearing. Amendments to applications shall be signed and submitted in the same manner as the original application. If a petition to deny or other formal objection has been filed in response to the application, the amendment shall be served on the parties.

176. *Other Administrative Changes.* We adopt the proposals in the *2024 Cable NPRM* and redesignate the submarine cable rules under subpart FF as stated in Appendix A, Final Rules, of the released document. We received no comment on these proposals. We also adopt the ministerial, non-substantive changes throughout Appendix A that the Commission proposed in the *2024 Cable NPRM,* such as the conversion of Notes into respective subsections for consistency with the Office of Federal Register requirements. We decline to adopt the requirement that applicants file a copy of a submarine cable application with CISA, DHS or to remove cross-references to other sections of our rules in Appendix A, Final Rules. We note that DHS already receives a cable landing license application as a member of the Committee and pursuant to our adopted rules in this *Report and Order,* DHS will also receive a copy of the Foreign Adversary Annual Reports filed by required licensees, pursuant to its status as a member of the Committee. We decline to remove the proposed cross-references in our adopted rules because we find that it will ensure clarity. We note that if we were to repeat the language of the cross-referenced section of the Commission's rules and such section is amended, this would require an amendment to the cable rules as well. We delegate to OIA the authority to amend the relevant rule (after notice and comment if OIA deems required or advisable) and to amend the referenced website therein as necessary to update contact information and the list of agencies for filing with the Executive Branch agencies. We also adopt an administrative change to § 1.767(g)(4) by revising the text ''traffic'' to instead state ''telecommunications services,'' and therefore clarify the applicability of the rule consistent with section 214 of the Communications Act.

*G. Foreign Adversary Annual Report*

177. We adopt an annual report requirement for existing licensees that meet certain conditions below. We adopt this Foreign Adversary Annual Report to ensure that the Commission has the information it needs to timely monitor and continually assess national security or other risks that may arise over the course of a licensee's 25-year license term, which may inform decisions to revoke or impose additional conditions upon a license in response to changed circumstances. In the *2024 Cable NPRM,* the Commission explained that it is critical that the Commission has a continuous and systematic understanding of who owns and controls submarine cables and how they are used because submarine cables are a critical component of the global communications ecosystem. The Commission further explained that outside of certain transactions, foreign carrier notifications, or renewal applications, it does not ordinarily receive updated information about changes in the ownership of licensees or the submarine cable system itself over the course of the 25-year license term. For this reason, the Commission likely has incomplete or outdated information regarding cable landing licensees with foreign ownership and the submarine cable system. The Commission tentatively concluded that the periodic reporting requirement would improve the Commission's oversight of cable landing licenses and ensure that the license continues to serve the public interest during the license term.

178. In an effort to ease burdens on licensees that do not meet the applicable criteria, we adopt a routine condition as proposed in the *2024 Cable NPRM* in lieu of periodic reporting. Many commenters raised concerns with the Commission's original proposal to require three-year periodic reporting of all licensees. For example, commenters contended that the three-year periodic reporting will result in administrative burden to licensees, and if the Commission chooses to adopt the reporting, it must be tailored and not duplicative to the reporting required by licensees who are parties to a mitigation agreement with the Committee. We agree that a three-year periodic reporting requirement as applied to all licensees could be burdensome to licensees that are already subject to consistent monitoring by the Committee. Yet certain information is necessary to our oversight of cable landing licensees.

179. We require existing licensees that meet one or more of the criteria below to provide an annual report. We find that although the frequency of filing for the annual report is more than would be required for the three-year periodic report, the burden is outweighed by the benefit because the licensees subject to this requirement present a potentially heightened national security risk. This annual reporting requirement applies to an existing licensee:

(1) That is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g);

(2) That is identified on the Covered List that the Commission maintains pursuant to the Secure Networks Act;

(3) Whose authorization, license, or other Commission approval, whether or not related to operation of a submarine cable, was denied or revoked and/or terminated or is denied or revoked and/or terminated in the future on national security and law enforcement grounds, as well as the current and future affiliates or subsidiaries of any such entity; and/or

(4) Whose submarine cable system is licensed to land or operate in a foreign adversary country, as defined in § 1.70001(f).

180. *Information Content.* For existing licensees that meet the above criteria, we adopt the information content of the report as proposed in the *2024 Cable NPRM* and listed in Appendix A of the released document, § 1.70017, as modified according to the *Report and Order* we adopt today. The content of the Foreign Adversary Annual Report will therefore require the following information that is current as of thirty (30) days prior to the date of the submission: (1) the information as required in § 1.70005(a) through (g), (i), and (m), and (2) certifications as set forth under § 1.70006.

181. *Reporting Deadlines.* In the *2024 Cable NPRM,* the Commission proposed to assign, in Appendix D of the released document, each existing submarine cable system and license file number one of four categories with a different deadline to file the originally-proposed three-year periodic report. The entities in Category 1 of Appendix D of the *2024 Cable NPRM* likely meet at least one of the articulated criteria above for those

existing licensees that must file a Foreign Adversary Annual Report. The Commission recognizes that other licensees that have not been identified might meet one or multiple of the articulated criteria. We will require those licensees to self-identify and fulfill the reporting requirements for the Foreign Adversary Annual Report, depending on whether the licensee had been licensed pursuant to the requirements under § 1.767(h) of the Commission's current rule. We note that licensees that are owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, are typically not parties to a mitigation agreement with the Committee or its predecessor because such agreements are traditionally entered into by the U.S.-incorporated co-licensee in the case of a consortium cable. This removes concerns of duplicative reporting between the Commission and the Committee as to these particular licensees.

182. We adopt the requirement that licensees that meet the criteria under our newly adopted rule, § 1.70017, shall submit their initial Foreign Adversary Annual Report within six months of the effective date of the new rules, and each year. We delegate authority to OIA to establish and modify, as appropriate, deadlines for the report.

183. *Manner of Filing Foreign Adversary Annual Report.* Licensees that meet the criteria under section III.G. of this *Report and Order* shall submit a Foreign Adversary Annual Report in the relevant license file number in the Commission's International Communications Filing System (ICFS), or any successor system.

184. *Application Fees.* We adopt the requirement that licensees must pay a fee when submitting the Foreign Adversary Annual Reports and that the fee required be in the amount of $1,445. In the *2024 Cable NPRM* the Commission sought comment on whether to require cable landing licensees to pay a fee when submitting reports.

185. Section 8(a) of the Communications Act mandates that the Commission assess and collect application fees based on the Commission's costs to process applications. Section 8(c) also requires the Commission to amend the application fee schedule if the Commission determines that the schedule requires amendment to ensure that: (1) such fees reflect increases or decreases in the costs of processing applications at the Commission or (2) such schedule reflects the consolidation or addition of new categories of applications.

186. The Commission processes a wide range of applications that are subject to a filing fee. Based on the comments, we determine that the filing fee for Foreign Adversary Annual Reports should be lower than the fee for the three-year periodic reports proposed in the *2024 Cable NPRM.* Most commenters disagree with the application fee for the three-year periodic reports, which we decline to adopt as discussed above. NASCA, in addition to disagreeing with the three-year periodic reporting proposal as a whole, critiqued the Commission's proposed fee, noting that the Commission's estimate of 29 total labor hours to review the report is greater than the 24 hours the Commission estimates a licensee would spend preparing and submitting the report. We agree with NASCA's critique and lower the estimate of time required to review Foreign Adversary Annual Reports, relative to the proposed estimate for reviewing the proposed three-year periodic reports in the *2024 Cable NPRM.* The estimated hours, though lower than the Commission's previous estimate, take into account the Commission's review time, which is necessary to protect national security. We also conclude the fee for the Foreign Adversary Annual Report should be consistent with that of a cable landing license modification, as the information sought and the Commission's effort to review is comparable.

### *H. Modifying the Capacity Data Collection for National Security and Other Purposes*

187. We modify the circuit capacity reporting requirements to enhance the quality and usefulness of the data for national security and other purposes, provide greater clarity on the reporting requirements to Filing Entities, and eliminate duplicative burdens. The Commission has found that the data from the circuit capacity reports are necessary for the Commission to fulfill its statutory obligations and serve a vital role by sharing this information with other federal agencies. The Committee regularly requests these data for its work on national security and law enforcement issues, as has DHS for its national security and homeland security functions. We find that the data provided through the Capacity Holder Reports provides the information necessary for these purposes and thus eliminate the Cable Operator Report. We direct OIA to revise the Filing Manual to conform with the changes we adopt here.

#### 1. Elimination of the Cable Operator Report

188. Based on our review of the record, we eliminate the requirement for licensees to file a Cable Operator Report. Microsoft and NASCA propose eliminating the Cable Operator Report, as it requires joint licensees for a system to share competitively sensitive information with each other and the information provided is redundant of the Capacity Holder Reports. The Coalition supports ''allowing for each licensee on a cable to report its 'available capacity' on the cable on an individual basis,'' and suggests the Commission could aggregate the data provided by each licensee to determine the total capacity for each system, which ''would necessarily require each licensee to report its own capacity in order for the Commission to have accurate data.'' We agree with commenters that certain data collected in the Cable Operator Report and Capacity Holder Report are redundant. We find that we can streamline the reporting requirements by eliminating the Cable Operator Report and collecting the information currently obtained through the Cable Operator Report in the Capacity Holders Reports which will eliminate the concerns about sharing confidential information with other licensees on the cable.

189. While we will no longer collect the total ''available capacity'' on a per system basis through the Cable Operator Report, we provide definitional clarifications, as discussed in section III.H.3., to ensure we can reliably assess the ''owned capacity'' data individually and in the aggregate to ascertain the total available capacity of each submarine cable.

190. In addition, we will retain important information from the Cable Operator Report by integrating planned capacity data and design capacity data into the Capacity Holder Report. As explained below, we modify the approach raised in the *2024 Cable NPRM* in light of our review of the record and elimination of the Cable Operator Report. Therefore, the licensee or licensees of a U.S.-international submarine cable will no longer be required to file a Cable Operator Report on a per system basis showing the planned capacity and design capacity of the submarine cable. Instead, each cable landing licensee and common carrier will be required to include in the Capacity Holder Report its planned capacity and design capacity on each submarine cable landing in the United States.

2. Reporting of Capacity Holdings on Domestic Submarine Cables

191. We modify the rules to require Capacity Holder Reports for domestic cables licensed by the Commission. We find that the lack of information on domestic cables creates a critical gap in the Commission's insight into the ownership and use of capacity on submarine cables regulated by the Commission. We find that extending the capacity reporting requirements to domestic submarine cables will strengthen our ability and that of the Committee to identify and assess national security, law enforcement, and other risks to this critical U.S. communications infrastructure.

192. We disagree with commenters' arguments that the Commission should not extend the annual capacity reporting requirements to domestic submarine cables because it would ''impose burdens disproportionate to their benefit'' and domestic submarine cables ''do not implicate the national security risks that the [*2024 Cable*] NPRM seeks to address.'' Currently, the Commission has no visibility into which entities hold capacity on other domestic submarine cables and whether any such capacity holders are associated with foreign adversaries. Commenters provide no arguments or evidence that refute or dispel these concerns. Indeed, the Committee states that ''the United States and its networks are under constant threat from various foreign adversaries, particularly China,'' noting, for example, how Chinese state-sponsored hackers ''were hiding within the U.S. networks waiting to attack our critical U.S. telecommunications infrastructure, which in turn serves other critical sectors such as energy, water, and government services.'' We find that the lack of information regarding domestic submarine cables creates a serious gap in the Commission's knowledge regarding ownership and use of capacity on critical U.S. communications infrastructure.

193. We therefore modify § 43.82 to require cable landing licensees and common carriers to file Capacity Holder Reports for their capacity holdings on domestic submarine cables. We find it is appropriate to require Filing Entities to report the same capacity information that we collect for U.S.-international submarine cables, especially in light of other changes we adopt for the circuit capacity reporting requirements. Accordingly, Filing Entities shall report their capacity holdings on domestic submarine cables in accordance with § 43.82, as amended in this proceeding.

3. Modifications to the Capacity Holder Report

a. Reporting of Available, Planned and Design Capacity

194. We find that eliminating the Cable Operator Report and consolidating the capacity data into the Capacity Holder Reports—a report filed by each Filing Entity on an individual basis—will enable the Commission to continue collecting accurate and important data for national security and public safety purposes while addressing the concerns of commenters about sharing competitively sensitive information with other joint licensees and duplicative reporting requirements. We will therefore amend the Capacity Holder Report to integrate information about available, planned and design capacity that was previously reported in the Cable Operator Report. We also clarify the definitions to provide clarity to Filing Entities and improve the consistency and reliability of the data. We believe that clarifying the definitions will better ensure that Filing Entities report their data accurately and consistently, and consequently, will enable the Commission to rely on aggregation of owned capacity data from the Capacity Holder Reports to assess the total available capacity of a submarine cable in absence of the Cable Operator Report.

195. *Available Capacity.* We define ''available capacity'' on a submarine cable as all of the capacity (both lit and unlit capacity) based on equipment currently used on the submarine cable. The Coalition supports clarification of the terms ''available capacity'' and ''design capacity,'' and recommends a similar definition of ''available capacity'' as capacity that is ''presently possible to provide across the cable as a result of the type of electronic equipment currently attached to the cable.'' The Coalition explains this is the widely accepted definition of ''available capacity'' in the industry, while ''design capacity'' is ''the maximum amount of capacity that can be handled by the fibers themselves regardless of the type of electronic equipment utilized.'' Other commenters did not specifically address this issue or propose alternative approaches, but recommend generally that the Commission clarify existing requirements. To further reduce confusion for Filing Entities, we will also refer to ''available capacity'' as ''current equipped capacity.''

196. Accordingly, we will apply this definition of ''available capacity'' to the existing categories of capacity holdings in the Capacity Holder Report. These categories include (1) owned capacity (''Cable Ownership''), (2) the net amount of IRUs, (3) net amount of ICLs, (4) net capacity, (5) activated (*i.e.,* lit) capacity, and (6) non-activated (*i.e.,* unlit) capacity. Consistent with this definition of ''available capacity,'' these capacity holdings should be reported based on equipment currently used on the submarine cable. To further ensure consistency in the data, we also clarify that ''owned capacity'' is the capacity that an entity holds through its direct ownership or controlling interest in a submarine cable pursuant to § 1.767(h). With few exceptions, ''owned capacity'' is reported by the licensee(s) of the submarine cable. To the extent an entity other than the licensee(s) of the submarine cable holds capacity through a direct ownership or controlling interest in the cable that does not meet the threshold licensing requirements of § 1.767(h), the entity should report that capacity as ''owned capacity.''

197. *Planned Capacity and Design Capacity.* We define ''planned capacity'' as the intended capacity (both lit and unlit capacity) on the submarine cable two years from the reporting date (December 31 of the preceding calendar year) that includes any current plans to upgrade the technology. Further, we will no longer use the definition currently reflected in the Filing Manual, where ''available capacity'' of a submarine cable is also referred to as ''design capacity,'' and instead define ''design capacity'' as the maximum theoretical capacity on the submarine cable regardless of equipment currently used or current plans to upgrade the technology. Our definition incorporates the Coalition's recommendation that ''design capacity'' is ''the maximum amount of capacity that can be handled by the fibers themselves regardless of the type of electronic equipment utilized.'' We note that planned capacity data and design capacity data should be reported separately from the existing categories of capacity holdings, consistent with our definitional clarifications herein.

b. Additional Categories of Capacity Holdings

198. In light of the national security and other risks raised in the record, and the important role of capacity data for advancing national security purposes, we adopt additional categories for reporting capacity holdings to include data for fiber and spectrum holdings. The current circuit capacity data collection does not provide visibility into how and to what extent capacity holders, including any entity that is owned and/or controlled by foreign

adversaries, use their capacity to access, route, and maintain such ''connectivity comparable to operating their own communications cable to the United States.'' We find that this information gap presents serious national security, law enforcement, and other vulnerabilities to this critical U.S. communications infrastructure. We therefore will require licensees and common carriers to identify in the Capacity Holder Report whether they sold or leased out and/or purchased or leased a fiber pair and/or spectrum on any submarine cable landing in the United States as of the reporting date.

199. While industry commenters did not address these issues specifically, a few commenters generally oppose expanding the capacity reporting requirements and argue the Commission should focus on clarifying and simplifying existing requirements. We agree with the Committee, however, that it would be useful to identify in the Capacity Holder Reports how the capacity is held ''on a fiber or spectrum basis.'' The Committee explains that an entity with a dark fiber interest in a submarine cable ''typically is responsible for 'lighting' its own dark fiber or spectrum'' and may ''attach its own SLTE, or equivalent equipment, to the fiber, in its own facility to route its own U.S. communications traffic, all operated, monitored, and secured by its own network operations center (NOC) and its own employees and service providers.'' Significantly, as noted by the Committee, ''[a] foreign adversary-controlled non-licensee entity that owns, controls, or operates its own SLTE, or equivalent equipment, on a submarine cable landing in the United States may have connectivity comparable to operating their own communications cable to the United States without a license, or any regulatory review, mitigation, or monitoring for national security or law enforcement risk.''

200. Accordingly, licensees and common carriers will be required to identify, with respect to each sale, lease, or purchase of a fiber pair and/or spectrum, the submarine cable, the U.S. and foreign landing points of the fiber pair and/or spectrum, and the entity that manages the fiber pair and/or spectrum, if different from the entity that owns it. We thus will apply consistent reporting requirements where, for example, a Filing Entity sold, leased, or purchased whole fiber pairs or spectrum partitioned on a fiber. We will tailor these requirements by not requiring licensees and common carriers to separately report the amount of capacity that is sold, leased, and/or purchased by fiber pair or spectrum. We expect this capacity information will be represented in the data that Filing Entities must report under existing categories of owned capacity, net IRUs, and net ICLs.

c. Reporting of SLTEs on Submarine Cables Landing in the United States

201. Consistent with other actions in this *Report and Order,* we will require cable landing licensees and common carriers to provide certain information about their SLTEs in the Capacity Holder Report. As the Commission stated in the *2024 Cable NPRM,* and consistent with our findings today, the SLTE is among the most important equipment associated with the submarine cable system for national security and law enforcement purposes. We find that identifying which entities own or control an SLTE on Commission-licensed submarine cables will, among other things, enable the Committee and Commission to identify licensees that ''have increased exposure to foreign adversary entities'' and also ''enhance the Committee's ability to triage risks when deciding whether to initiate *ad hoc* reviews of existing licenses.''

202. The Coalition opposes incorporating ''a new reporting category regarding SLTE ownership and operation on a cable system,'' arguing that it is unnecessary and, ''[w]ithout a demonstrable gain to national security, increases in the reporting and compliance burdens on the industry should be avoided.'' We disagree with the Coalition's views that there is no ''demonstrable gain to national security'' in collecting this information. Indeed, we find that addressing this critical information gap is essential for our national security objectives. Moreover, as discussed above, the Committee emphasizes the importance of obtaining information about entities with access to, or ownership or control of, SLTE and equivalent equipment in light of ''the risk of foreign adversary-controlled non-licensee entities owning, controlling, and operating SLTE, or equivalent equipment, on submarine cables landing in the United States.''

203. We therefore modify § 43.82 to require cable landing licensees and common carriers to identify in the Capacity Holder Report whether they *own or control* an SLTE on the U.S. and/or foreign ends of each submarine cable landing in the United States. For purposes of circuit capacity reporting, we will require Filing Entities to report information about their SLTEs directly to the Commission. Moreover, we clarify that this requirement will apply to all cable landing licensees, including licensees that do not hold capacity on a submarine cable and do not otherwise file Capacity Holder Reports under the current rules. Further, we adopt the Commission's proposal to share with our federal partners the information that is collected pursuant to this requirement, including any information for which confidential treatment is requested, through the procedures discussed below.

d. Which Corporate Entity May File Reports

204. We find that any subsidiary, parent entity, or affiliate should be allowed to file the Capacity Holder Report on behalf of a licensee or common carrier, so long as the legal name of the licensee or common carrier is identified in the report and an officer of the licensee or common carrier certifies that the information in the report is accurate and complete. To the extent a subsidiary, parent entity, or affiliate of a Filing Entity submits the circuit capacity reports on the Filing Entity's behalf, the Filing Entity shall be held accountable for any defects in the certification as to the accuracy and completeness of information filed in the circuit capacity reports. While no commenter addressed these issues, based on Commission staff review of the annual capacity data, we find that allowing any subsidiary, parent entity, or affiliate to file the Capacity Holder Report on behalf of a licensee or common carrier, subject to identification and certification requirements, would be consistent with a common filing practice. Further, we find that our approach will improve the administrative efficiency of our current practice, which involves informal inquiries by Commission staff, to confirm whether the licensee or common carrier has complied with its reporting obligations.

205. To the extent a subsidiary, parent entity, or affiliate files the Capacity Holder Report on behalf of a licensee or common carrier, we will require that the report must identify the legal name of the licensee or common carrier that is subject to the § 43.82 reporting requirements. To the extent a consolidated Capacity Holder Report is filed on behalf of multiple affiliated entities, we will require that the report must identify the legal name of each entity and, where applicable, indicate whether certain information (*e.g.,* ownership or control of an SLTE) pertains to a specific licensee or common carrier. Further, we modify § 43.82 to codify the requirement that licensees and common carriers subject

to § 43.82 shall be held accountable for any defects in the certification as to the accuracy and completeness of information filed in the Capacity Holder Report. To this end, we will also require that an officer of the licensee or common carrier must also certify that the information in the Capacity Holder Report is accurate and complete, notwithstanding any certification that may be provided by a subsidiary, parent entity, or affiliate.

4. Compliance

206. We adopt the Commission's proposal to codify a compliance provision in § 43.82 of the rules. In the *2024 Cable NPRM,* the Commission proposed to state specifically in the rules that filing false or inaccurate certifications or failure to file timely and complete annual capacity reports in accordance with the Commission's rules and the Filing Manual shall constitute grounds for enforcement action, including but not limited to a forfeiture, revocation, or termination of the cable landing license or international section 214 authorization, pursuant to the Communications Act and any other applicable law, including the Cable Landing License Act. We find that having a compliance provision in the rules will ensure greater compliance overall with the reporting requirements. Although we sought comment on whether we should exempt certain entities from filing a capacity report, such as an entity that controls the U.S. landing station but does not hold capacity on the cable, no commenter addressed this issue. We find that it is important to receive as much information about capacity holdings on licensed cables, and thus do not adopt exceptions to reporting for licensees and common carriers subject to § 43.82 of the rules.

5. Sharing the Circuit Capacity Data With Federal Agencies

207. As was proposed in the *2024 Cable NPRM,* we modify § 43.82 of the rules to allow the Commission to share with the Committee, DHS, and the State Department the capacity data filed on a confidential basis without the pre-notification requirements of § 0.442(d). The Commission may share information that has been submitted to it in confidence with other federal agencies when they have a legitimate need for the information and the public interest will be served by sharing the information. We find that the Committee, DHS, and the State Department each have a legitimate need for the capacity data.

208. Since 2019, the Commission has annually issued a Public Notice to announce its intent to share the annual capacity data with DHS and subsequently the Committee pursuant to the procedures set out in § 0.442 of the Commission's rules, and no party has opposed such disclosure of the capacity data for which confidential treatment was requested. The Commission has found that the data provided in the Circuit Capacity Reports ''are essential for our national security and public safety responsibilities in regulating communications submarine cables'' and that ''circuit capacity data are important for the Commission's contributions to the national security and defense of the United States. The data are also useful for federal agencies in fulfilling their other duties and responsibilities.

209. The Committee supports adoption of a rule to allow the Commission to share with other federal government agencies the capacity data filed on a confidential basis without the pre-notification requirements of § 0.442(d) and states that streamlining the sharing of information would ''help the Committee efficiently fill some information gaps on older cable systems and reduce delays, administrative burden, and duplicative filings on behalf of industry.'' The Committee ''recommends that the Commission include at least all the Committee members,'' and states that it ''intends to treat any information, received from the Commission in accordance with Commission confidentially rules . . . and the confidentiality provisions contained in Section 8 of E.O. 13913.'' The Committee states that it also ''intends to treat such information as eligible for exemption under the Freedom of Information Act, to the extent applicable.'' Industry commenters do not object to the sharing of the data with federal agencies provided that ''licensees' requests for confidential treatment are honored'' and ''such information remains confidential.

210. Pursuant to the new rule we adopt today, the Commission will be able to share the confidential data with federal agencies that have a legitimate need for the data consistent with their functions without the delay attendant to providing parties an opportunity to object to the sharing. Further, the rule we adopt will make clear that sharing of the confidential circuit capacity data with other federal government agencies is subject to the requirements of the confidentiality protections contained in the Commission's regulations and 44 U.S.C. 3510, and, in the case of the Committee, section 8 of Executive Order 13913 that require the Committee to keep the information confidential. Therefore, sharing of confidential capacity data will continue to be subject to the requirement that each of the other federal agencies comply with the confidentiality protections applicable both to the Commission and the other agency relating to the unlawful disclosure of information. We will also provide notice to the parties whose information is being shared.

211. We find that the Committee states that it has a legitimate need for reviewing the capacity data to fulfill its mandate under Executive Order 13913, as the data are relevant to its national security and law enforcement reviews and ''[h]aving this information provides a clearer picture of how such cables are being used and by whom and better enables the Committee to evaluate international data flows on various cables.'' We also find that DHS has a legitimate need for the capacity data. In the *2017 Section 43.62 Report and Order,* the Commission specifically noted that DHS ''finds this information to be critical to its national and homeland security functions'' and ''[DHS] states that this information, when combined with other data sources, is used to protect and preserve national security and for its emergency response purposes. Finally, we find that Executive Order 10530 provides a basis for the Commission to share annual capacity data with the State Department in light of the agency's legitimate need for the information in furtherance of its functions related to approving (or disapproving) certain Commission actions on submarine cable licenses.

*I. One-Time Information Collection*

212. We adopt a mandatory one-time information collection applicable to cable landing licensees. As noted above, the one-time information collection is necessary to obtain information to assist the Commission in fulfilling the purposes of the Cable Landing License Act. *First,* we require licensees to provide updated information on currently licensed submarine cables and licensees to assess for any insolvent cables or licensees. This information will enable the Commission to initiate revocation proceedings to revoke the cable landing license or licensee(s) that are insolvent or no longer exist. *Second,* we require all licensees to provide information concerning the SLTE owners and operators on the licensed cable to inform our regulatory approach in the *Further Notice of Proposed Rulemaking. Third,* we require licensees to provide information as to whether or not the licensee currently uses any equipment or services identified on the Commission's Covered List, uses a third-party foreign adversary service

provider, or uses a third-party service provider that can access the submarine cable system from a foreign adversary country. The information collected will provide the Commission with information to assess current national security risks.

213. *Legal Authority.* Pursuant to the Cable Landing License Act and Executive Order 10530, the Commission holds broad legal authority to regulate submarine cables that connect to the United States. Under section 35 of title 47, the Commission has legal authority to withhold or revoke a license if such action will ''promote the security of the United States.'' The Commission is obligated to ensure that a license for a submarine cable system remains in the public interest, which includes obtaining complete and accurate submarine cable and licensee information, obtaining information to inform our regulatory approach on SLTEs, and ensuring that the Commission has information to protect the national security or law enforcement interests of the United States.

214. *Information Collection on Licensees and Cables.* We seek updated information from each cable landing licensee, regardless of whether the licensee is a member of a consortium cable, to provide the name of the submarine cable and identify all of the current licensees and known licensees that are no longer in business or insolvent. The Commission has incomplete information as to all licensees, as the Commission's records in ICFS and other records indicate that some submarine cables licensed by the Commission may not have commenced service and/or some cable landing licensees of record may be insolvent or no longer in operation.

215. *Information Collection on SLTEs.* The Commission has incomplete information as to the identities and the number of SLTE owners and operators that connect to a Commission-licensed submarine cable system and the information collected will inform our regulatory approach in the *Further Notice of Proposed Rulemaking.* Importantly, SLTEs are among the most important equipment associated with the submarine cable system for national security and law enforcement purposes. We adopt information collection requirements for each licensee to provide to the Commission information regarding SLTEs based on the newly adopted rules set forth in § 1.70005(a) through (d), (e)(7)(i) and (iii), (g), and (i) in this *Report and Order.* This will include such information as to the contact and business organizational information of the licensee; information about the landing stations and SLTE; and other information deemed necessary for the purposes of the collection.

216. *Information Collection Regarding the Covered List and Third-Party Service Providers.* We require licensees to disclose whether or not their submarine cable system uses equipment or services identified on the Commission's Covered List; provide information about each particular covered equipment or service that they use in the submarine cable system; disclose whether they use a third-party service provider that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g); or use a third-party service provider that can access the submarine cable system from a foreign adversary country, as defined in § 1.70001(f). For national security reasons, the Commission needs this information to assess the current risks identified in submarine cable infrastructure.

217. *Process and Deadline.* We direct OIA to conduct this information collection, including the creation of forms, to submit the information collection for Office of Management and Budget (OMB) review and, following OMB review, to publish notice of the effective date of the information collection requirement and the filing deadline in the **Federal Register**. The filing deadline shall be no fewer than thirty (30) days following the effective date of this *Report and Order.* OIA also will issue a Public Notice announcing the deadline and will provide instructions for filing this information with the Commission. We note that licensees that fail to comply with the information collection required in this *Report and Order* are subject to monetary forfeitures, in addition to enforcement action up to and including cancellation or revocation/termination of the license.

218. *Certification.* In general, submarine cable owners and operators should have knowledge concerning our information collection requirements above. A cable landing licensee is expected to conduct due diligence. If, after conducting appropriate due diligence, licensees are unable to ascertain all of the requested information, such licensees may certify that the information provided in the one-time information collection is accurate to the best of the licensee's knowledge and explain the reasoning for non-compliance. We anticipate that this standard for our information collection will provide a scope of expectation for cable landing licenses that will not be unduly burdensome, including for small entities.

219. *Surrender of Cable Landing License.* Entities that seek to surrender their cable landing license can file a notification that includes information set out in § 1.70011(d) of our adopted rules before the filing deadline. If the filing is made before the deadline, the entity does not need to respond to the one-time information collection. Cable landing licensees may file a notification in ICFS.

220. *Manner of Authentication of Identify of Filer.* OIA is delegated the authority to determine the appropriate manner of authentication of the identity of each filer in this one-time information collection.

*J. Costs and Benefits*

221. We estimate that the rules that we adopt today will facilitate faster and more efficient deployment of submarine cables, while at the same time ensuring the security and resilience of this critical infrastructure. Applying conservative assumptions, we estimate that licensees will incur total costs of no more than approximately $2.5 million per year to implement the rules. Our estimate includes all the expected ongoing costs that would be incurred as a result of the rules adopted in the *Report and Order.* The benefits of the actions we adopt today are significant and difficult to quantify, such as preventing untrustworthy elements in the communications network from impacting our nation's defense, public safety, and homeland security operations, our military readiness, and our critical infrastructure, not to mention the collateral damage such as loss of life that may occur with any mass disruption to our nation's communications networks. As we explain below, we find that such benefits are likely to substantially outweigh the costs.

222. We implement the following proposals from the *2024 Cable NPRM.* We take action to protect the security, integrity, and resilience of submarine cable systems by targeting foreign adversary threats to this critical United States communications infrastructure. Specifically, we adopt a clear and consistent standard that incorporates the Department of Commerce's definitions for identifying a ''foreign adversary,'' ''foreign adversary country,'' and an individual or entity ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.'' Using these definitions, we adopt rules that will better protect U.S. national security from foreign adversaries.

223. To protect critical U.S. communications infrastructure against foreign adversary threats, we will presumptively preclude the grant of applications filed by: any entity owned by, controlled by, or subject to the jurisdiction or control of a foreign adversary; any entity on the Commission's ''Covered List;'' and/or any entity whose authorization, license, or other Commission approval, whether or not related to operation of a submarine cable, was denied or revoked and/or terminated or is denied or revoked and/or terminated in the future on national security and law enforcement grounds, as well as the current and future affiliates or subsidiaries of any such entity. To ensure that applicants have the requisite character qualifications, we adopt a presumption that an applicant is not qualified to hold a cable landing license if it meets certain criteria. We adopt a presumption that denial of an application is warranted where an applicant seeks to land a new submarine cable in a foreign adversary country, as defined in § 1.70001(f), or that seeks to modify, renew, or extend its cable landing license to add a new landing located in a foreign adversary country, as defined in § 1.70001(f). To ensure that applicants have the requisite character qualifications, we adopt a presumption that an applicant is not qualified to hold a cable landing license if it meets any of the criteria listed below, unless the applicant overcomes the adverse presumption. Additionally, we adopt a condition prohibiting cable landing licensees from entering into new or an extension of existing arrangements for IRU or leases for capacity on submarine cable systems landing in the United States, where such arrangement for IRUs or lease for capacity would give the entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, the ability to install, own, or manage SLTE on a submarine cable landing in the United States. For current licensees that meet the above definition or whose cable lands in a foreign adversary country, we adopt increased oversight tools as they must file an annual Foreign Adversary Annual Report containing information about the submarine cable system operations and the licensee and submarine cable system ownership. We also adopt a written hearing process for denial or revocation and/or termination of cable landing licenses.

224. We modernize our submarine cable rules by adopting a definition of the term, ''submarine cable system,'' that acknowledges the range of technological advancement in existing submarine cable systems. This definition incorporates the future technological evolution of submarine cable systems, all of which include SLTE as a significant component of the system itself. While at this time we decline to require SLTE owners and operators to become licensees, we take steps to identify, through a one-time information collection, how many entities currently own or operate SLTEs on existing licensed cable systems. The one-time information collection we adopt will further inform the Commission about the identities of SLTE owners and operators and their respective role in operating a portion of the submarine cable system, including information about system capacity, spectrum, or the lighting of a fiber. The one-time collection will also assess for insolvent cables or licensees, and require licensees to disclose whether they use covered equipment or services.

225. We also codify the Commission's longstanding practice of requiring a cable landing license for submarine cables that lie partially outside of U.S. territorial waters. Moreover, while we do retain a number of our current rules, we eliminate the requirement that entities that solely own, and do not control, a U.S. cable landing station must be applicants for, and licensees on, a cable landing license. We also update our application rules to ensure applicants provide sufficient information about the submarine cable infrastructure for which they are seeking a license and to require compliance with ongoing certifications regarding cybersecurity and physical security risk management plans and use of equipment and services identified on the Covered List. These rules will ensure that licensees protect their networks from cybersecurity threats and threats from individuals and entities subject to foreign adversary ownership, control, jurisdiction, or direction. We clarify when a modification of an existing license is required and whether the change requires prior approval or a post-action notification. We formalize rules for applications to renew a cable landing license upon expiration of the license term and for special temporary authority. To make it easier for applicants and licensees to navigate our rules, we update the organization of rules for applications to modify, assign, transfer control of, or renew or extend a cable landing license or request special temporary authority. We adopt rules to obligate licensees to keep the Commission abreast of changes to important information such as the contact information of the licensee and other information that will enable the Commission to maintain accurate records regarding licensees. We eliminate the requirement for licensees to file a Cable Operator Report about the capacity on a cable. We will require licensees and common carriers to report their capacity on domestic as well as international cables and clarify the types of capacity that need to be reported

226. The rules we adopt today should benefit national security, law enforcement, foreign policy, and trade policy, as well as fulfill our public interest responsibilities under the Cable Landing License Act. The rules overall will increase our ability to monitor international data flows over the international submarine cable network, to identify those entities that are using the cables, and to detect attacks on the U.S. government, private sector, and critical infrastructure. Updating the circuit capacity data collection to include more granular information on submarine cable equipment and more precise measures of circuit capacity should enable the Commission to identify new risks to submarine cables. Including SLTE in the formal definition of a submarine cable system should strengthen our oversight of potentially vulnerable SLTE end points which should increase the security of the entire submarine cable network. Adopting an information collection on cable landing licensees to learn about SLTE owners and operators and whether the licensee currently uses any equipment or services identified on the ''Covered List,'' uses a third-party foreign adversary service provider, or uses a third-party service provider that can access the submarine cable system from a foreign adversary country should inform our efforts in coordination with the Committee to respond to potential vulnerabilities of the submarine cable system.

227. We couple our rules improving risk identification and monitoring with rules that allow us to mitigate potential risks. Strengthening our rules on presumptive denials of certain applications filed by applicants with previous adverse actions on national security grounds should reduce the surveillance of sensitive data and disruption to online commerce and international financial transactions. By prohibiting IRUs and leasing capacity agreements owned by foreign adversaries, we are reducing their access to capacity on submarine cables that access the United States, thereby mitigating the risk of hostile actions.

Prohibiting new cables from using covered equipment and strengthening certification requirements should reduce the risk of cyberattacks by foreign adversaries through covered equipment accessing the United States.

228. Our actions today balance the need to strengthen national security with efforts to expedite and streamline our processes, thereby reducing the burden of compliance. By narrowing the Commission's proposals to require applicants to report whether or not they use and/or will use third-party foreign adversary service providers in the operation of a submarine cable, we balance our goals of strengthening national security while minimizing the burden on our trading partners and allies. Similarly, streamlining the information sharing procedures with the Committee should reduce the burden on industry of preparing reports and filings while expediting coordinated efforts across the federal government to protect U.S. cable systems from foreign adversary attacks.

229. Submarine cables are estimated to carry 99% of intercontinental internet traffic and serve as the backbone to global communications. In updating our submarine cable rules for the first time since 2001, the Commission is responding to recent geopolitical developments and addressing potential hostile actions by foreign adversaries against our submarine cable network, including potentially severing submarine cables or damaging equipment located at cable landing stations, disrupting communications, and negatively impacting international financial transactions and online commerce. In recent years the threat of malicious cyberattacks by foreign adversaries, most notably China, on U.S. telecommunications companies and critical infrastructure has become more significant. Cyber threats to the U.S. government, private sector, and infrastructure include espionage, surveillance, and the suppression of communications. There has been an increase in reports of physical cutting of submarine cable infrastructure, and these incidents appear to be deliberately targeting the key linkages between the United States and its trading partners. Cybercrime and malicious cyber activities have become more costly over the past decade. The hacking group Salt Typhoon compromised the networks of several major U.S. Internet companies in 2024. A third party entity reports that the volume of attacks by China to the U. S. government, technology and communications sectors increased by 50% between 2023 and 2024.

230. The U.S. gross domestic product was over $29 trillion in 2024. The digital economy added approximately $2.6 trillion in value to the overall U.S. economy in 2022, representing approximately 10% of gross domestic product, and represents a rapidly growing segment of the overall economy. Globally, the volume of financial transactions flowing over submarine cables has been estimated to be greater than ten trillion dollars per day. Thus, even a temporary, localized disruption to data passing through submarine cables would likely result in very substantial economic losses. The harms would encompass business imports and exports, the operations of multinational corporations, international financial flows, online commerce, residential and government communications, and online access to information including emergency services. Although such losses are very difficult to measure, on an annual basis, we find that they are likely well in excess of the annual costs that we estimate would be associated with our rules.

231. Our revised estimate of costs is $2.5 million per year, including all additional expected costs that would be incurred as a result of the rules adopted in this *Report and Order.* We note that our revised estimate represents an increase of $1.2 million over the estimate provided in the *Notice.* This increase reflects two primary factors. First, the *Report and Order* more clearly defines the additional information required under the application requirements, including: the location of all landing points and branching units of the cable by segment, the number of segments in the submarine cable system and the designation of each, the length of the cable by segment and in total, the location of each cable landing station, the number of optical fiber pairs by segment, the design capacity by segment, the anticipated time frame when the cable system will be placed in service, route position lists, location of SLTE, location of NOC or backup NOC, location of SOC or backup SOC, third-party foreign adversary service provider information, cybersecurity certifications, covered list certification, and foreign carrier affiliations. Second, in response to commenter input, we have attempted to lighten the regulatory burden on industry by declining to adopt the proposal for a 3-year reporting requirement for all licensees and instead focusing our review on foreign adversaries, declining to include service providers and SLTE owners as applicants, harmonizing cybersecurity requirements based on common standards, and by revising the estimated number of hours required to prepare an application.

232. We base our cost estimate on the Commission's records that indicate, as of July 31, 2025, there are currently 91 submarine cable systems licensed by the Commission that are owned by approximately 147 unique licensees. Furthermore, we estimate that there are approximately ten (10) applications for new cables landing licenses filed every year. We also estimate that there are approximately 24 applications filed every year for modification, assignment, or transfer of control of a cable landing license. Based on these estimated numbers of applications, and our estimate that there will be four renewal applications filed annually, we estimate that 38 submarine cable applications are submitted annually.

233. Our cost estimate assumes that approximately 114 licensees will undergo the application process each year for the estimated 38 cable systems that are submitting applications for that year. We base this on the conservative assumption that each cable landing license application will have an average of three licensees. In addition, we estimate that applicants will incur an additional cost associated with the rules we adopt to certify compliance with baseline cybersecurity standards, including implementing the cybersecurity and physical security risk management plans. We expect that the amount of work associated with preparing a new license application likely will be similar to the work associated with preparing a renewal application.

234. In the *2024 Cable NPRM,* we estimated that the preparation of a new or renewal application for each submarine cable system by an average of three licensees will require 80 hours of work by attorneys and 80 hours of work by support staff at a cost of $27,200 per application. NASCA states that the Commission understated the costs of preparing a license application. Similarly, the Coalition states that the proposals in the *2024 Cable NPRM* will result in significantly higher compliance costs than the estimate. While neither commenter provided alternative estimates, in order to have confidence that we do not underestimate the costs borne by filers, we double the estimated number of hours required to 160 hours of work by attorneys and 160 hours of work by support staff, at a cost of $54,400 per application. To this cost, we add the cost of cybersecurity certification required for all new and renewal applications, which we

estimate to be $9,100. We then multiply the sum of these costs by 38 to produce an estimate of approximately $2.5 million per year for annual application costs. We estimate that the Foreign Adversary Annual Report will require twelve hours of attorney time and twelve hours of support staff time, at a cost of $4,100. We multiply this amount by ten to account for the total cost that U.S. entities may incur in preparing these reports. We sum these costs to produce a total estimate of approximately $2.5 million per year for the 25-year period, as a baseline estimate of the annual application and license review costs.

## IV. Severability

235. The rules adopted in this *Report and Order* advance the Commission's comprehensive strategy to facilitate submarine cable deployment while protecting submarine cable infrastructure. Though complementary, each of the separate rules serves their own distinct and specific purpose to promote these goals. Therefore, it is our intent that each of the rules adopted in this *Report and Order* shall be severable. If any of the rules are declared invalid or unenforceable for any reason, we find that the remaining portions of the regulatory framework continue to fulfill our goal of promoting faster and more efficient deployment of submarine cables while simultaneously protecting submarine cable infrastructure, and that any remaining rules not deemed invalid or unenforceable shall remain in effect and be enforced to the fullest extent permitted by law.

## V. Procedural Matters

236. *Transition of Rules.* Until the new rules become effective, we will retain §§ 1.767 and 1.768 to ensure that the Commission may continue to receive and process applications and related filings. The specific rules that are retained until the respective transition are identified in paragraph 336 below.

237. *Regulatory Flexibility Act.* The Regulatory Flexibility Act of 1980, as amended (RFA), requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that ''the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities.'' Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this *Report and Order* on small entities. The FRFA is set forth in Appendix C of the released document.

238. *Paperwork Reduction Act.* This *Report and Order* may contain new or substantively modified information collections subject to the Paperwork Reduction Act of 1995 (PRA), 44 U.S.C. 3501–3521. All such new or modified information collections will be submitted to the Office of Management and Budget (OMB) for review under section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on any new or modified information collections contained in this proceeding. Additionally, this document may contain non-substantive modifications to approved information collections. Any such modifications will be submitted to OMB for review pursuant to OMB's non-substantive modification process. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees. In this present document, we have assessed the effects of obtaining information about covered equipment and services in submarine cable systems, and other related information important for, and find that the impact to small entities and businesses is difficult to ascertain but will not be disproportionate to the impact on larger businesses and entities.

239. Additionally, this *Report and Order* may contain non-substantive modifications to approved information collections. Any such modifications will be submitted to OMB for review pursuant to OMB's non-substantive modification process.

240. *OPEN Government Data Act.* The OPEN Government Data Act requires agencies to make ''public data assets'' available under an open license and as ''open Government data assets,'' *i.e.,* in machine-readable, open format, unencumbered by use restrictions other than intellectual property rights, and based on an open standard that is maintained by a standards organization. This requirement is to be implemented ''in accordance with guidance by the Director'' of the OMB. The term ''public data asset'' means ''a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under [the Freedom of Information Act (FOIA)].'' A ''data asset'' is ''a collection of data elements or data sets that may be grouped together,'' and ''data'' is ''recorded information, regardless of form or the media on which the data is recorded.''

241. *Congressional Review Act.* The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is non-major under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this Report and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

242. *Availability of Documents.* Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS. When the FCC Headquarters reopens to the public, these documents will also be available for public inspection during regular business hours in the FCC Reference Center, Federal Communications Commission, 45 L Street NE, Washington, DC 20554.

## VI. Final Regulatory Flexibility Analysis

243. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Federal Communications Commission (Commission) incorporated an Initial Regulatory Flexibility Analysis (IRFA) in the *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules* (*2024 Cable NPRM*), released in November 22, 2024. The Commission sought written public comment on the proposals in the *2024 Cable NPRM,* including comment on the IRFA. No comments were filed addressing the IRFA. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA and it (or summaries thereof) will be published in the **Federal Register**.

### *A. Need for, and Objectives of, the Rules*

244. In this *Report and Order,* we undertake the first major comprehensive update of our submarine cable rules since 2001. Since that time, technology, consumer expectations, international submarine cable traffic patterns, and investment in and construction of submarine cable infrastructure have greatly changed. This *Report and Order* modernizes and streamlines the Commission's submarine cable rules to facilitate faster and more efficient deployment of submarine cables, while at the same time ensuring the security,

resilience, and protection of this critical infrastructure. We adopt rules that place a strong emphasis on prohibiting and mitigating national security risks from foreign adversaries, while welcoming investment from United States allies and partners. We also lighten the regulatory burden on industry by modernizing and simplifying the submarine cable license approval process.

245. Specifically, we adopt a standard for identifying a ''foreign adversary,'' ''foreign adversary country,'' and an individual or entity ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,'' and use these to adopt rules that will better protect U.S. national security and critical U.S. communications infrastructure from foreign adversaries. We presumptively preclude the grant of applications filed by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; any entity identified on the Commission's ''Covered List''; and/or any entity whose authorization, license, or other Commission approval, whether or not related to operation of a submarine cable, was denied or revoked and/or terminated or is denied or revoked and/or terminated in the future on national security and law enforcement grounds, as well as the current and future affiliates or subsidiaries of any such entity. We adopt a presumption that an applicant is not qualified to hold a cable landing license if it meets any of the criteria identified in the *Report and Order,* unless the applicant overcomes the adverse presumption. We adopt a presumption that denial of an application is warranted where an applicant seeks to land a new submarine cable in a foreign adversary country. Additionally, we adopt a condition prohibiting cable landing licensees from entering into a new or extension of an existing arrangement for Indefeasible Rights of Use (IRU) or leases for capacity on submarine cable systems landing in the United States, where such arrangement would give certain entities the ability to install, own, or manage Submarine Line Terminal Equipment (SLTE) on a submarine cable landing in the United States. For certain entities, we adopt a requirement to file an annual report (Foreign Adversary Annual Report) containing information about the submarine cable system operations and the licensee and submarine cable system ownership. We also adopt a written hearing process for denial or revocation and/or termination of cable landing licenses.

246. We define the term, ''submarine cable system,'' that acknowledges the range of technological advancement in existing submarine cable systems, including SLTEs. We adopt a one-time information collection to collect the number of entities that currently own or operate SLTEs on existing licensed cable systems, and the respective SLTE owners and operators' identities and their role in operating a portion of the submarine cable system, among other information. The one-time collection will also assess for insolvent cables or licensees, and require licensees to disclose whether they use covered equipment or services.

247. We also codify the Commission's longstanding practice of requiring a cable landing license for submarine cables that lie partially outside of U.S. territorial waters. We eliminate the requirement that entities that solely own, and do not control, a U.S. cable landing station must be applicants for, and licensees on, a cable landing license. We require a statement that grant of the application is in the public interest, to ensure applicants provide sufficient information about the submarine cable system for which they are seeking a license, to report whether or not they use and/or will use third-party foreign adversary service providers in the operation of the submarine cable, and to require compliance with ongoing certifications regarding cybersecurity and physical security risk management plans and use of equipment and services identified on the Covered List. We clarify when a modification of an existing license is required and whether the change requires prior approval or a post-action notification. We formalize rules for applications to renew or extend a cable landing license upon expiration of the license term and for special temporary authority. We update the organization of rules for applications to modify, assign, transfer control of, or renew or extend a cable landing license or request special temporary authority. We adopt rules for licensees to keep the Commission abreast of changes to important information such as the contact information of the licensee and other information that will enable the Commission to maintain accurate records regarding licensees. We eliminate the requirement for licensees to file a Cable Operator Report about the capacity on a cable. We require licensees and common carriers to report their capacity on domestic as well as international cables and clarify the types of capacity that need to be reported.

*B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA*

248. No comments were made on the record on the IRFA specifically. However, several commenters addressed the impact of the Commission's proposed rules in the *2024 Cable NPRM* on small businesses or smaller players in specific industries. We summarize these comments here and analyze the impact of the Commission's adopted rules in section F, *infra.*

249. Commenters raised small business impacts in the context of the Commission's seeking comment on whether to retain the requirement that an entity that owns or controls a 5% or greater interest in the cable and uses the U.S. points of the cable system be an applicant for and licensee on a cable landing license. As an example, the Submarine Cable Coalition argues in favor of keeping the 5% or greater threshold for licensing and claimed ''[a]ny proposed changes to modify the 5% ownership threshold . . . will specifically and disproportionately impact small carriers and investors.'' Microsoft similarly argues the Commission should not ''impos[e] unnecessary burdens on small investors'' who do not have the ability to materially influence the operation of the cable.

250. The Commission's proposal in the *2024 Cable NPRM* to license data center owners received comment on its impact to smaller data center owners. The Submarine Cable Coalition supported the Commission maintaining its current practice of waiving licensing to ''avoid unnecessarily burdening . . . passive infrastructure owners,'' stating that requiring data center owners who only own the facility in which the cable landing station is located to be licensed would ''disparately impact smaller data center owners that do not have the necessary resources to address the myriad of reporting and compliance requirements that come along with becoming a submarine cable licensee.'' INCOMPAS supports the Commission codifying its practice of waiving licensing for data center operators, claiming ''[s]maller data center operators face significant market and cost pressure that continually increases with no end in sight . . . Adding unnecessary, duplicative, and burdensome regulation to the market will further this negative trend . . . ultimately leav[ing] small data center operators unable to compete effectively in the market with larger operators.''

251. Commenters noted the burdens of the *2024 Cable NPRM's* proposed

three-year periodic reports on smaller businesses and small entities. CTIA advocated the Commission revise the proposal, noting it would ''impose significant new administrative burdens, particularly on smaller companies.'' CTIA noted that the ''frequent reporting cadence could deter smaller companies . . . ultimately limiting competition and innovation in the industry.'' CTIA also claimed the three-year periodic reports would place greater burdens and slow the submarine cable license approval process, which would cause ''substantial difficulty'' to small- and medium-sized enterprises seeking to attract capital to deploy submarine cables.

252. USTelecom generally expressed support for the Commission's proposed cybersecurity requirements and noted that its small and medium enterprise members ''have a mature cybersecurity culture,'' agreed with the Commission on letting companies demonstrate compliance with proposed cybersecurity requirements by following an established risk management framework like the NIST CSF and using government resources. USTelecom advocated allowing organizations to combine their cybersecurity risk management and supply chain risk management plans, citing ''unnecessary administrative burdens, particularly on small and medium-sized enterprises.''

253. USTelecom also notes that a ''rip and replace'' mandate would be especially difficult for ''smaller and rural operators'' to implement overall.

254. The Committee notes that ''[s]maller businesses are more likely to acquire lit capacity, fiber, or spectrum leaseholds from dark fiber owners or IRU holders'' rather than own, control, or operate their own SLTE, and therefore claims the new SLTE reporting requirements suggested in the *2024 Cable NPRM* are ''narrowly tailored to capture information on entities effectively operating submarine cables to the United States without imposing undue burdens on small businesses.''

255. Finally, AP&T notes the general burden of regulation on small businesses, ''the administrative burden is same for large and small carriers alike . . . small carriers have fewer customers, the fixed costs of managing the carrier's regulatory requirements are significantly more burdensome on a per-customer basis.''

256. The Commission responds to the concerns of commenters by not adopting some of the proposals from the *2024 Cable NPRM* and implementing others in a modified, narrowed fashion. The Commission has considered the above-mentioned comments and has adopted alternatives, discussed in Section F below, to address some of the concerns raised by small entities.

### *C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration*

257. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and provide a detailed statement of any change made to the proposed rules as a result of those comments. The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

### *D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply*

258. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein. The RFA generally defines the term ''small entity'' as having the same meaning as under the Small Business Act. In addition, the term ''small business'' has the same meaning as the term ''small business concern'' under the Small Business Act.'' A ''small business concern'' is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.

259. *All Other Telecommunications.* This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Providers of internet services (*e.g.* dial-up ISPs) or Voice over internet Protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $40 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Based on this data, the Commission estimates that the majority of ''All Other Telecommunications'' firms can be considered small.

260. *Competitive Local Exchange Carriers (CLECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 3,378 providers that reported they were competitive local service providers. Of these providers, the Commission estimates that 3,230 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

261. *Computer Infrastructure Providers, Data Processing, Web Hosting, and Related Services.* This industry comprises establishments primarily engaged in providing computing infrastructure, data processing services, Web hosting services (except software publishing), and related services, including streaming support services (except streaming distribution services). Cloud storage services, computer data storage services, computing platform infrastructure provision Infrastructure as a service (IaaS), optical scanning services, Platform as a service (PaaS), and video and audio technical streaming support services are included in this industry. Data processing establishments provide complete processing and specialized reports from data supplied by clients or provide automated data processing and data entry services. The SBA small business size standard for this industry classifies firms with annual receipts of $40 million or less as small. U.S. Census Bureau data for 2017 indicate that 9,058 firms in this industry were operational for the entire year. Of this total, 8,345 firms had revenue of less than $25 million. Thus, under the SBA size standard the majority of firms in this industry are small.

262. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 127 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 109 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

263. *Internet Publishing and Broadcasting and Web Search Portals.* This industry comprises establishments primarily engaged in (1) publishing and/or broadcasting content on the internet exclusively or (2) operating websites that use a search engine to generate and maintain extensive databases of internet addresses and content in an easily searchable format (and known as Web search portals). The publishing and broadcasting establishments in this industry do not provide traditional (non-internet) versions of the content that they publish or broadcast. They provide textual, audio, and/or video content of general or specific interest on the internet exclusively. Establishments known as web search portals often provide additional internet services, such as email, connections to other websites, auctions, news, and other limited content, and serve as a home base for internet users. The SBA small business size standard for this industry classifies firms having 1,000 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were firms that 5,117 operated for the entire year. Of this total, 5,002 firms operated with fewer than 250 employees. Thus, under this size standard the majority of firms in this industry can be considered small.

264. *Internet Service Providers (Non-Broadband).* Internet access service providers using client-supplied telecommunications connections (*e.g.,* dial-up ISPs) as well as VoIP service providers using client-supplied telecommunications connections fall in the industry classification of All Other Telecommunications. The SBA small business size standard for this industry classifies firms with annual receipts of $40 million or less as small. For this industry, U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Consequently, under the SBA size standard a majority of firms in this industry can be considered small.

265. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, in general, a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses. Next, ''small organizations'' are not-for-profit enterprises that are independently owned and operated and not dominant their field. While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees. Finally, ''small governmental jurisdictions'' are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand. Based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.

266. *Wired Broadband Internet Access Service Providers (Wired ISPs).* Providers of wired broadband internet access service include various types of providers except dial-up internet access providers. Wireline service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules. Wired broadband internet services fall in the Wired Telecommunications Carriers industry. The SBA small business size standard for this industry classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees.

267. Additionally, according to Commission data on internet access services as of June 30, 2019, nationwide there were approximately 2,747 providers of connections over 200 kbps in at least one direction using various wireline technologies. The Commission does not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, in light of the general data on fixed technology service providers in the Commission's *2022 Communications Marketplace Report,* we believe that the majority of wireline internet access service providers can be considered small entities.

268. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.

269. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged in the provision of fixed local services. Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.

Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

*E. Description of Economic Impact and Projected Reporting, Recordkeeping and Other Compliance Requirements for Small Entities*

270. The RFA directs agencies to describe the economic impact of proposed rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for preparation of the report or record.

271. It is not possible to separately estimate the costs of compliance for large and small entities. The cost estimate for compliance with the new rules is no more than approximately $2.5 million per year for licensees, including all additional expected costs that would be incurred as a result of the rules adopted in this *Report and Order.* We note that our revised estimate represents an increase of approximately $1.2 million per year over the estimate provided in the *2024 Cable NPRM.* This increase reflects two primary factors. First, the *Report and Order* more clearly defines the additional information required under the application requirements, including: the location of all landing points and branching units of the cable by segment, location of SLTE, location of NOC or backup NOC, location of SOC or backup SOC, the number of segments in the submarine cable system and the designation of each, the length of the cable by segment and in total, the location of each cable landing station, the number of optical fiber pairs by segment, the design capacity by segment, the anticipated time frame when the cable system will be placed in service, route position lists, third-party foreign adversary service provider information, cybersecurity and physical security certifications, covered list certification, and foreign carrier affiliations. Second, in response to commenter input, we have attempted to lighten the regulatory burden on industry by declining to adopt the proposal for a 3-year reporting requirement for all licensees and instead focusing our review on foreign adversaries, declining to include service providers and SLTE owners as applicants, harmonizing cybersecurity and physical security requirements based on common standards, and by revising the estimated number of hours required to prepare an application.

272. We based our cost estimate on the Commission's records that indicate, as of July 31, 2025, there are currently 91 submarine cable systems licensed by the Commission that are owned by approximately 147 unique licensees. Furthermore, we estimate that there are approximately ten (10) applications for new cable landing licenses filed every year. We also estimate that there are approximately 24 applications filed every year for modification, assignment, or transfer of control of a cable landing license. Based on these estimated numbers of applications, and our estimate that four (4) renewal applications are filed annually, we estimate that 38 submarine cable applications are submitted annually.

273. Our cost estimate assumes that approximately 114 licensees will undergo the application process each year for the estimated 38 cable systems that are submitting applications for that year. We base this on the conservative assumption that each cable landing license application will have an average of three licensees. In addition, we estimate that applicants will incur an additional cost associated with the rules we adopt to certify compliance to baseline cybersecurity and physical security standards, including implementing the cybersecurity and physical security risk management plans. We expect that the amount of work associated with preparing a new license application likely will be similar to the work associated with preparing a renewal or extension application.

274. In the *2024 Cable NPRM,* we estimated that the preparation of a new or renewal application for each submarine cable system by an average of three licensees will require 80 hours of work by attorneys and 80 hours of work by support staff at a cost of $27,200 per application. NASCA states that the Commission understated the costs of preparing a license application. Similarly, the Coalition states that the proposals in the *2024 Cable NPRM* will result in significantly higher compliance costs than the estimate. While neither commenter provided alternative estimates, in order to have confidence that we do not underestimate the costs borne by filers, we accept their comments and double the estimated number of hours required to 160 hours of work by attorneys and 160 hours of work by support staff, at a cost of $54,400 per application. To this cost, we add the cost of cybersecurity and physical security certification required for all new and renewal applications, which we estimate to be $9,100.We then multiply the sum of these costs by 38 to produce an estimate of approximately $2.4 million per year for annual application costs. We estimate that the Foreign Adversary Annual Report will require twelve hours of attorney time and twelve hours of support staff time, at a cost of $4,100. We multiply this amount by ten to account for the total cost that U.S. entities may incur in preparing these reports. We sum these costs to produce a total estimate of approximately $2.5 million per year for the 25-year period, as a baseline estimate of the annual application and license review costs.

275. We do not believe these rules would disproportionately impact small entities; all applicants are required to submit the additional information required for applications. We also deliberately chose a cybersecurity and physical security compliance requirement that is flexible and can be customized for different types of entities. We also clarified that the requirement pertains to the reasonable measures to protect the system and services that could affect the provision of communications services through the submarine cable system. The Foreign Adversary Annual Report would impact large and small entities alike.

276. The one-time information collection requirement will only apply to current cable landing licensees, and so will not have a significant impact on a substantial number of small entities.

*F. Discussion of Steps Taken To Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered*

277. The RFA requires an agency to provide, ''a description of the steps the agency has taken to minimize the significant economic impact on small entities . . . including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected.''

278. Commenters expressed concern about impact on small businesses or smaller carriers of removing the 5% threshold for licensing. We retain the existing requirement that an entity owning or controlling a 5% or greater interest in the cable system and using the U.S. points of the cable system must submit an application to become a licensee, and decline to adopt any other proposals at this time. We agree with the commenters that there is not a sufficient reason to disturb the existing requirement. Lowering or removing the 5% threshold would increase the number of entities that must comply

with our regulatory framework, and we believe our approach, coupled with new rules that tailor the licensing requirements to identify entities that can exercise ownership or control over a submarine cable system allow us to achieve the goals we sought in proposing to lower the ownership threshold, without impacting small businesses.

279. Commenters raised implications for smaller entities in the context of the proposal to license data center owners. We adopt rules to limit licensing to entities that control the cable landing station, which would exclude entities that may own the cable landing station but are not directly involved in cable operations and do not control the cable system's operations. We believe this strikes the right balance between our need to license those who control the submarine cable system while not burdening data center owners who do not control the system.

280. Commenters expressed concern about the burden of the three-year periodic reports. We do not adopt the proposed three-year periodic reports, rather adopt only a Foreign Adversary Annual Report, which will impact only those licensees that meet specific criteria. We do not believe any small businesses will fall into the category required to file the Foreign Adversary Annual Report, but if any do, we deem the national security benefits of the Foreign Adversary Annual Report significant enough to justify the burden.

281. With regard to commenters advocating for allowing organizations to combine their cybersecurity risk management and supply chain risk management plans to avoid administrative burdens on small or medium-sized enterprises, the rules we adopt today regarding cybersecurity and physical security risk management plans permit a great deal of flexibility for structuring such plans. We do not require any particular framework, rather find that applicants and licensees will presumptively satisfy the Commission's cybersecurity and physical security risk management plan requirement if their plan is structured according to an established risk management framework such as the NIST CSF, and follows an established set of best practices, such as the standards and controls set forth in the CISA CPGs or the CIS Controls.

282. Commenters noted that a proposed ''rip and replace'' mandate would be especially difficult for smaller operators to implement. We do not adopt a requirement that licensees remove ''Covered List'' equipment from their systems currently, and so this burden will not impact smaller operators.

283. We decline to adopt rules for SLTE owners and operators in the *Report and Order,* and instead propose and seek comment in the *Further Notice of Proposed Rulemaking.* Therefore, at this time there should be no burden on smaller entities that own or operate SLTE.

284. Regarding the general burden placed on smaller entities by regulation, throughout this item we considered options and adopt rules that focus reporting or other requirements on the narrow set of entities that we describe may involve foreign adversary threats, keeping regulatory burdens to a minimum for other entities.

*G. Report to Congress*

285. The Commission will send a copy of the *Submarine Cable Report and Order,* including this Final Regulatory Flexibility Analysis, in a report to Congress pursuant to the Congressional Review Act. In addition, the Commission will send a copy of the *Submarine Cable Report and Order,* including this Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the SBA and will publish a copy of the *Submarine Cable Report and Order,* and this Final Regulatory Flexibility Analysis (or summaries thereof) in the **Federal Register**.

## VII. Ordering Clauses

286. *It is ordered* that, pursuant to sections 1, 4(i), 4(j), 201–255, 303(r), 403, 413 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i), 154(j), 201–255, 303(r), 403, 413, and the Cable Landing License Act of 1921, 47 U.S.C. 34–39, and Executive Order No. 10530, section 5(a) (May 12, 1954) reprinted as amended in 3 U.S.C. 301, this Report and Order and Notice of Proposed Rulemaking is hereby adopted.[2]

287. *It is further ordered* that this Report and Order and Further Notice of Proposed Rulemaking *shall be effective* 30 days after publication in the **Federal Register**, except that the amendments to 47 CFR 1.70002(b), 1.70003, 1.70005, 1.70006, 1.70007(f) through (h), (l), (m), (q), (s), (t), (v), and (x), 1.70008, 1.70009, 1.70011, 1.70012, 1.70013, 1.70016(b)(2), 1.70017, 1.70020, 1.70023, 1.70024, and 43.82, and the one-time information collection, which may contain new or substantively modified information collections, will not become effective until the Office of Management and Budget completes review of any information collections that the Office of International Affairs determines is required under the Paperwork Reduction Act. The Commission directs the Office of International Affairs to announce the effective date for §§ 1.70002(b), 1.70003, 1.70005, 1.70006, 1.70007(f) through (h), (l), (m), (q), (s), (t), (v), and (x), 1.70008, 1.70009, 1.70011, 1.70012, 1.70013, 1.70016(b)(2), 1.70017, 1.70020, 1.70023, 1.70024, and 43.82 by notice in the **Federal Register** and by subsequent public notice, and directs the Office of International Affairs to publish notice of the effective date of the one-time information collection and the filing deadline in the **Federal Register**.

288. *It is further ordered* that the following sections shall be removed and reserved upon 30 days after publication in the **Federal Register**: 47 CFR 1.767(b) through (d), (f), (g)(1) through (5), (9) through (11), (14), and (16), (i) through (l), (o), and final note, and 43.82(a)(1). Sections 1.767 and 1.768, 47 CFR 1.767 and 1.768, shall be removed upon the completion of the review of any information collections by the Office of Management and Budget under the Paperwork Reduction Act and the announcement by the Office of International Affairs of the effective date of the new rules.

289. *It is further ordered* that the Office of International Affairs shall conduct the information collection required by the Report and Order, including the creation of any information collection forms or other instrument, and shall publish notice of the effective date of the information collection required by the Report and Order and the filing deadline in the **Federal Register**. The filing deadline shall be no fewer than 30 days following the effective date of the Report and Order. The Office of International Affairs shall announce the effective date and the filing deadline for the requirements in the Report and Order by subsequent Public Notice.

290. *It is further ordered* that the Office of the Managing Director, Performance Program Management, shall send a copy of this Report and in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. 801(a)(1)(A).

291. *It is further ordered* that the Commission's Office of the Secretary shall send a copy of this Report and Order the Final Regulatory Flexibility Analyses, to the Chief Counsel for Advocacy of the Small Business Administration.

[2] Pursuant to Executive Order 14215, 90 FR 10447 (Feb. 20, 2025), this regulatory action has been determined to be significant under Executive Order 12866, 58 FR 68708 (Dec. 28, 1993).

**List of Subjects in 47 CFR Parts 0, 1, and 43**

Communications, Communications common carriers, Communications equipment, Cuba, Internet, Security measures, Reporting and recordkeeping requirements, Telecommunications.

Federal Communications Commission.

**Aleta Bowers,**

*Federal Register Liaison Officer, Office of the Secretary.*

**Final Rules**

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 0, 1, and 43 as follows:

## PART 0—COMMISSION ORGANIZATION

■ 1. The authority citation for part 0 continues to read as follows:

**Authority:** 47 U.S.C. 151, 154(i), 154(j), 155, 225, 409, and 1754, unless otherwise noted.

■ 2. Amend § 0.351 by revising paragraph (a)(9) to read as follows:

**§ 0.351 Authority delegated.**

(a) * * *

(9) To act upon applications for cable landing licenses or revoke or terminate cable landing licenses under the Cable Landing License Act, 47 U.S.C. 34 through 39, and Executive Order 10530, dated May 10, 1954.

* * * * *

■ 3. Amend § 0.457 by adding paragraph (c)(1)(iv) to read as follows:

**§ 0.457 Records not routinely available for public inspection.**

* * * * *

(c) * * *

(1) * * *

(iv) The exact specific geographic location information of submarine cables as specified in § 1.70005(e)(7) and (f) of this chapter.

* * * * *

## PART 1—PRACTICE AND PROCEDURE

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

**Authority:** 47 U.S.C. chs. 2, 5, 9, 13; 28 U.S.C. 2461 note; 47 U.S.C. 1754, unless otherwise noted.

### Subpart E—Complaints, Applications, Tariffs, and Reports Involving Common Carriers

**§ 1.767 [Amended]**

■ 5. Amend § 1.767 by:

■ a. Removing and reserving paragraphs (b) through (d), (f), (g)(1) through (5), (g)(9) through (11), (14), and (16), (i) through (l), and (o); and

■ b. Removing the note to § 1.767.

**§ 1.767 [Removed]**

■ 6. Delayed indefinitely, remove § 1.767.

**§ 1.768 [Removed]**

■ 7. Delayed indefinitely, remove § 1.768.

### Subpart G—Schedule of Statutory Charges and Procedures for Payment

■ 8. Amend § 1.1107 by adding the entry ''Foreign Adversary Annual Report'' at the end of table 1 to read as follows:

**§ 1.1107 Schedule of charges for applications and other filings for the international services.**

TABLE 1 TO § 1.1107

| International services | | | |
|---|---|---|---|
| Cable landing license, per application | Payment type code | New fee | |
| * * * * * | * | * | |
| Foreign Adversary Annual Report | DAQ | 1,445 | |

* * * * *

■ 9. Add subpart FF, consisting of §§ 1.70000 through 1.70024, to read as follows:

### Subpart FF—Cable Landing Licenses

Sec.

1.70000 Purpose.
1.70001 Definitions.
1.70002 General requirements.
1.70003 [Reserved]
1.70004 Additional presumptive disqualifying conditions.
1.70005–1.70006 [Reserved]
1.70007 Routine conditions.
1.70008–1.70009 [Reserved]
1.70010 Amendment of applications.
1.70011–1.70013 [Reserved]
1.70014 Processing of applications.
1.70015 Quarterly reports.
1.70016 Eligibility for streamlining.
1.70017–1.70020 [Reserved]
1.70021 Electronic filing.
1.70022 Action on applications, revocation, and termination.
1.70023–1.70024 [Reserved]

**§ 1.70000 Purpose.**

The provisions contained in this subpart implement the Cable Landing License Act of 1921, codified at 47 U.S.C. 34 through 39, as amended, and section 5(a) of Executive Order 10530, dated May 10, 1954, and provide requirements for initial applications for a cable landing license; certifications; routine conditions; requests for special temporary authority; foreign carrier affiliation notifications; amendment of applications; modification applications; substantial assignment and transfer of control of a cable landing license; *pro forma* assignment and transfer of control notifications; requests for streamlining of applications; quarterly reports; foreign adversary annual reports; renewal or extension applications; public viewing of applications; electronic filing; and provide for the grant, denial, revocation, and termination of cable landing license applications or licenses.

**§ 1.70001 Definitions.**

(a) *Affiliated.* The term ''affiliated'' as used in this subpart is defined as in § 63.09 of this chapter.

(b) *Country.* The term ''country'' as used in this subpart refers to the foreign points identified in the U.S. Department of State's list of Independent States in the World and its list of Dependencies and Areas of Special Sovereignty. *See https://www.state.gov.*

(c) *Foreign carrier.* The term ''foreign carrier'' as used in this subpart is defined as in § 63.09 of this chapter except that the term ''foreign carrier'' shall also include any entity that owns or controls a cable landing station in a foreign market.

(d) *Third-party service provider.* The term ''third-party service provider'' as used in this subpart is defined as an entity that is involved in providing, hosting, analyzing, repairing, and maintaining the equipment of a submarine cable system, including

third-party owners and operators of network operations centers (NOCs).

(e) *Foreign adversary.* The term ''foreign adversary'' as used in this subpart is defined as any foreign government or foreign non-government person determined by the Secretary of Commerce, pursuant to Executive Order 13873 of May 15, 2019, to 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 United States persons as identified in 15 CFR 791.4.

(f) *Foreign adversary country.* The term ''foreign adversary country'' as used in this subpart refers to foreign governments identified as foreign adversaries in 15 CFR 791.4, and countries controlled by a foreign adversary identified in 15 CFR 791.4.

(1) The term ''foreign adversary country'' includes Venezuela to the extent Venezuelan politician Nicolás Maduro (Maduro Regime) is identified as a foreign adversary in 15 CFR 791.4.

(2) [Reserved]

(g) *Owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.* The term ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'' as used in this subpart applies to:

(1) Any individual or entity, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of an individual or entity whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary;

(2) Any individual, wherever located, who is a citizen of a foreign adversary or a country controlled by a foreign adversary, and is not a United States citizen or permanent resident of the United States;

(3) Any entity, including a corporation, partnership, association, or other organization, that has a principal place of business in, or is headquartered in, incorporated in, or otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary; or

(4) Any entity, including a corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs (g)(1) through (3) of this section possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority (10% or greater) of the total outstanding voting interest and/or equity interest, or through a controlling interest, in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity.

(h) *Submarine cable system.* The term submarine cable system as used in this subpart is defined as a cable system that carries bidirectional data and voice telecommunications traffic consisting of one or more submarine cable(s) laid beneath the water, and all associated components that support the operation of the submarine cable system end-to-end, including the segments up to the system's terrestrial terminations at one or more Submarine Line Terminal Equipment (SLTEs) as well as the transponders that convert optical signals to electrical signals and vice versa.

**§ 1.70002 General requirements.**

(a) *Cable landing license requirements.* A cable landing license must be obtained prior to landing a submarine cable that connects:

(1) The continental United States with any foreign country;

(2) Alaska, Hawaii, or the U.S. territories or possessions with—

(i) A foreign country;

(ii) The continental United States; or

(iii) Each other; or

(3) Points within the continental United States, Alaska, Hawaii, or a territory or possession in which the cable is laid in areas beyond the U.S. territorial waters, which extend 12 nautical miles seaward from the coastline.

(b) [Reserved]

(c) *Character presumptive disqualifying condition*—(1) *Presumptive disqualifying condition.* An applicant will be presumed not to possess the requisite character qualifications to become a cable landing licensee if the applicant has within the last 20 years:

(i) Materially violated the Cable Landing License Act, 47 U.S.C. 34 through 39, where the violation—

(A) Was not remediated with an adjudication involving a consent decree and/or compliance plan;

(B) Resulted in a loss of Commission license or authorization; or

(C) Was found by the Commission to be intentional;

(ii) Committed national security-related violations of the Communications Act, 47 U.S.C. 151 *et seq.,* or Commission rules as identified in Commission orders, including but not limited to violations of rules concerning the Covered List that the Commission maintains on its website pursuant to the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act), 47 U.S.C. 1601 through 1609;

(iii) Made materially false statements or engaged in fraudulent conduct concerning national security or the Cable Landing License Act;

(iv) Been subject to an adjudicated finding of making false statements or engaging in fraudulent conduct concerning national security before another U.S. Government agency; or

(v) Materially failed to comply with the terms of a cable landing license, including but not limited to a condition requiring compliance with a mitigation agreement with the Executive Branch agencies, including the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee), where the violation—

(A) Was not remediated with an adjudication involving a consent decree and/or compliance plan;

(B) Resulted in a loss of Commission license or authorization; or

(C) Was found by the Commission to be intentional.

(2) *Applicability.* The presumptive disqualifying condition shall apply to the following applications:

(i) *Initial application.* An initial application for a cable landing license that is filed after November 26, 2025;

(ii) *Application filed by licensees whose cable landing license is granted after November 26, 2025.* An application for modification, assignment, transfer of control, or renewal or extension of a cable landing license that is filed after November 26, 2025, by a licensee whose initial application for a cable landing license is granted after such date; and

(iii) *Application filed by licensees whose cable landing license is granted prior to November 26, 2025.* An application for modification, assignment, transfer of control, or renewal or extension of a cable landing license that is filed after November 26, 2025, by a licensee whose cable landing license was or is granted prior to such date and that does not exhibit any of the criteria in paragraphs (c)(1)(i) through (v) of this section prior to such date.

(3) *Presumption.* An applicant subject to paragraphs (c)(1) and (2) of this section can overcome the adverse presumption only by establishing that the applicant has the requisite character, despite its past conduct. An applicant need not disclose pending investigations, but rather must only

disclose violations as preliminarily or finally determined by the Commission, and as adjudicated by another U.S. Government agency or a court in the United States.

(d) *State Department coordination.* Cable landing licenses shall be granted or revoked by the Commission after obtaining the approval of the Secretary of State and such assistance from any executive department or establishment of the Government as the Commission may deem necessary. See section 5(a) of Executive Order 10530, dated May 10, 1954.

**§ 1.70003 [Reserved]**

**§ 1.70004 Additional presumptive disqualifying conditions.**

(a) *Foreign adversary presumptive disqualifying condition*—(1) *Presumptive disqualifying condition.* The disqualifying condition will presumptively preclude the grant of an application, as specified in paragraph (a)(2) of this section, filed by any applicant:

(i) That is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g);

(ii) That is identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601 through 1609; and/or

(iii) Whose authorization, license, or other Commission approval, whether or not related to the operation of a submarine cable, was denied or revoked and/or terminated or is denied or revoked and/or terminated in the future on national security and law enforcement grounds, as well as the current and future affiliates and subsidiaries of any such entity as defined in § 2.903(c) of this chapter.

(2) *Applicability.* The presumptive disqualifying condition shall apply to the following applications:

(i) *Initial application.* An initial application for a cable landing license that is filed after November 26, 2025;

(ii) *Application filed by licensees whose cable landing license is granted after November 26, 2025.* An application for modification, assignment, transfer of control, or renewal or extension of a cable landing license that is filed after November 26, 2025, by a licensee whose initial application for a cable landing license is granted after such date; and

(iii) *Application filed by licensees whose cable landing license is granted prior to November 26, 2025.* An application for modification, assignment, transfer of control, or renewal or extension of a cable landing license that is filed after November 26, 2025, by a licensee whose cable landing license was or is granted prior to such date and that does not exhibit any of the criteria in paragraphs (a)(1)(i) through (iii) of this section prior to such date.

(3) *Presumption.* An applicant subject to paragraphs (a)(1) and (2) of this section can overcome the adverse presumption only by establishing through clear and convincing evidence that the applicant does not fall within the scope of the adverse presumption, or that grant of the application would not pose risks to national security or that the national security benefits of granting the application would substantially outweigh any risks.

(b) *Foreign adversary cable landing presumptive disqualifying condition*—(1) *Presumptive disqualifying condition.* The disqualifying condition will presumptively preclude the grant of an application, as specified in paragraph (b)(2) of this section, filed by any applicant:

(i) That seeks to land a new submarine cable in a foreign adversary country, as defined in § 1.70001(f).

(ii) That seeks to modify, renew, or extend its cable landing license to add a new landing located in a foreign adversary country, as defined in § 1.70001(f).

(2) *Applicability.* The presumptive disqualifying condition shall apply to the following applications:

(i) *Initial application.* An initial application for a cable landing license that is filed after November 26, 2025;

(ii) *Application filed by licensees whose cable landing license is granted after November 26, 2025.* An application for modification or renewal or extension of a cable landing license that is filed after November 26, 2025, by a licensee whose initial application for a cable landing license is granted after such date; and

(iii) *Application filed by licensees whose cable landing license is granted prior to November 26, 2025.* An application for modification or renewal or extension of a cable landing license that is filed after November 26, 2025, by a licensee whose cable landing license was or is granted prior to such date.

(3) *Presumption.* An applicant subject to paragraphs (b)(1) and (2) of this section can overcome the adverse presumption only by establishing through clear and convincing evidence that the applicant does not fall within the scope of the adverse presumption, or that grant of the application would not pose risks to national security or that the national security benefits of granting the application would substantially outweigh any risks.

**§§ 1.70005–1.70006 [Reserved]**

**§ 1.70007 Routine conditions.**

Except as otherwise ordered by the Commission, this section applies to each licensee of a cable landing license.

(a) Grant of the cable landing license is subject to:

(1) All rules and regulations of the Federal Communications Commission in this chapter;

(2) Any treaties or conventions relating to communications to which the United States is or may hereafter become a party; and

(3) Any action by the Commission or the Congress of the United States rescinding, changing, modifying or amending any rights accruing to any person by grant of the license.

(b) The location of the cable system within the territorial waters of the United States of America, its territories and possessions, and upon its shores shall be in conformity with plans approved by the Secretary of the Army. The cable shall be moved or shifted by the licensee at its expense upon request of the Secretary of the Army, whenever he or she considers such course necessary in the public interest, for reasons of national defense, or for the maintenance and improvement of harbors for navigational purposes.

(c) The licensee shall at all times comply with any requirements of United States government authorities regarding the location and concealment of the cable facilities, buildings, and apparatus for the purpose of protecting and safeguarding the cables from injury or destruction by enemies of the United States of America.

(d) The licensee, or any person or company controlling it, controlled by it, or under direct or indirect common control with it, does not enjoy and shall not acquire any right to handle telecommunications services to or from the United States, its territories or its possessions unless such service is authorized by the Commission pursuant to section 214 of the Communications Act, as amended.

(e) The following prohibition on special concessions applies:

(1) The licensee shall be prohibited from agreeing to accept special concessions directly or indirectly from any foreign carrier, including any entity that owns or controls a foreign cable landing station, where the foreign carrier possesses sufficient market power on the foreign end of the route to affect competition adversely in the U.S. market, and from agreeing to accept special concessions in the future.

(2) For purposes of this section, a special concession is defined as an

exclusive arrangement involving services, facilities, or functions on the foreign end of a U.S. international route that are necessary to land, connect, or operate submarine cables, where the arrangement is not offered to similarly situated U.S. submarine cable owners, indefeasible-right-of-user holders, or lessors, and includes arrangements for the terms for acquisition, resale, lease, transfer and use of capacity on the cable; access to collocation space; the opportunity to provide or obtain backhaul capacity; access to technical network information; and interconnection to the public switched telecommunications network.

(3) Licensees may rely on the Commission's list of foreign carriers that do not qualify for the presumption that they lack market power in particular foreign points for purposes of determining which foreign carriers are the subject of the requirements of this section. The Commission's list of foreign carriers that do not qualify for the presumption that they lack market power is available from the Office of International Affairs' website at: *https://www.fcc.gov/international-affairs.*

(f)–(h) [Reserved]

(i) The Commission reserves the right to require the licensee to file an environmental assessment should it determine that the landing of the cable at the specific locations and construction of necessary cable landing stations may significantly affect the environment within the meaning of § 1.1307 implementing the National Environmental Policy Act of 1969. See § 1.1307(a) and (b). The cable landing license is subject to modification by the Commission under its review of any environmental assessment or environmental impact statement that it may require pursuant to its rules. See also note 1 to § 1.1306 and § 1.1307(c) and (d).

(j) The Commission reserves the right, pursuant to section 2 of the Cable Landing License Act, 47 U.S.C. 35, Executive Order 10530 as amended, and section 214 of the Communications Act of 1934, as amended, 47 U.S.C. 214, to impose common carrier regulation or other regulation consistent with the Cable Landing License Act on the operations of the cable system if it finds that the public interest so requires.

(k) The licensee, or in the case of multiple licensees, the licensees collectively, shall maintain *de jure* and *de facto* control of the U.S. portion of the cable system, including the cable landing stations in the United States, sufficient to comply with the requirements of the Commission's rules in this chapter and any specific conditions of the license.

(l)–(m) [Reserved]

(n) The cable landing license is revocable or subject to termination by the Commission after due notice and opportunity for hearing pursuant to section 2 of the Cable Landing License Act, 47 U.S.C. 35, or for failure to comply with the terms of the license or with the Commission's rules in this chapter.

(o) The cable landing license shall expire twenty-five (25) years from the in-service date, unless renewed or extended upon proper application. Upon expiration, all rights granted under the license shall be terminated.

(p) The licensee(s) must commence service provided under its license within three years following the grant of its license.

(1) The licensee must notify the Commission within thirty (30) days of the date the cable is placed into service.

(2) Failure to notify the Commission of commencement of service within three years following the grant of the license shall result in automatic termination of the license after the Commission receives approval from the State Department, unless the licensee submits a request for waiver showing good cause why it is unable to commence commercial service on the cable, why the license should not be terminated, and the expected commencement of service date. The requirement to commence service may be extended upon a showing of good cause.

(q) [Reserved]

(r) Licensees shall file submarine cable outage reports as required in part 4 of this chapter.

(s)–(t) [Reserved]

(u) A licensee whose application for a cable landing license is filed and granted after November 26, 2025, shall not use equipment or services identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601 through 1609, on its submarine cable system under the license.

(1) A licensee whose modification application to add a new segment is filed and granted after November 26, 2025, shall not use equipment or services identified on the Covered List on the new segment and the new landing point. No licensee shall add to its submarine cable system(s) under its respective license(s) equipment or services identified on the Covered List; except, this paragraph (u)(1) shall not apply to a licensee that is identified on the Covered List whose cable landing license was or is granted prior to November 26, 2025.

(2) [Reserved]

(v) [Reserved]

(w) The licensee shall not enter into a new or extension of an existing arrangement for Indefeasible Rights of Use (IRUs) or leases for capacity on submarine cable systems landing in the United States, where such arrangement for IRUs or lease for capacity would give an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g), the ability to install, own, or manage SLTE on a submarine cable landing in the United States, unless so authorized by the Commission.

(1) A licensee may petition the Commission for waiver of the condition; however, any waiver of the condition would be granted only to the extent the licensee demonstrates by clear and convincing evidence that a new or extension of an existing arrangement for IRUs or lease for capacity subject to this subpart would serve the public interest and would present no risks to national security or that the national security benefits of granting the waiver would substantially outweigh any risks.

(2) [Reserved]

(x) [Reserved]

**§§ 1.70008–1.70009 [Reserved]**

**§ 1.70010 Amendment of applications.**

Any application may be amended as a matter of right prior to the date of any final action taken by the Commission or designation for hearing. Amendments to applications shall be signed and submitted in the same manner as was the original application. If a petition to deny or other formal objection has been filed in response to the application, the amendment shall be served on the parties.

**§§ 1.70011–1.70013 [Reserved]**

**§ 1.70014 Processing of applications.**

(a) *Processing of submarine cable applications.* The Commission will take action upon an application eligible for streamlined processing, as specified in § 1.70016, within forty-five (45) days after release of the public notice announcing the application as acceptable for filing and eligible for streamlined processing. If the Commission deems an application seeking streamlined processing acceptable for filing but ineligible for streamlined processing due to national security or law enforcement concerns or other public interest considerations, or if an applicant does not seek streamlined processing, the Commission

will issue public notice indicating that the application is ineligible for streamlined processing. Within ninety (90) days of the public notice, the Commission will take action upon the application or provide public notice that, because the application raises questions of extraordinary complexity, an additional 90-day period for review is needed. Each successive 90-day period may be so extended.

(b) *Submission of application to executive branch agencies.* On the date of filing with the Commission, the applicant shall also send a complete copy of the application, or any major amendments or other material filings regarding the application by electronic mail or postal mail, to: U.S. Coordinator, EB/CIP, U.S. Department of State, 2201 C Street NW, Washington, DC 20520–5818; Office of Chief Counsel/NTIA, U.S. Department of Commerce, 14th St. and Constitution Ave. NW, Washington, DC 20230; and Defense Information Systems Agency, ATTN: OGC/DDC, 6910 Cooper Avenue, Fort Meade, MD 20755–7088, and to electronic mail addresses identified on the FCC website at *https://www.fcc.gov/submarine-cables* and shall certify such service by electronic mail or postal mail on a service list attached to the application or other filing. Authority is delegated to the Office of International Affairs to amend this rule and to amend the referenced website herein as necessary to update contact information and the list of agencies for filing.

**§ 1.70015 Quarterly reports.**

Any licensee that is, or is affiliated with, a carrier with market power in any of the cable's destination countries must comply with the following requirements:

(a) File quarterly reports summarizing the provisioning and maintenance of all network facilities and services procured from the licensee's affiliate in that destination market, within ninety (90) days from the end of each calendar quarter. These reports shall contain the following:

(1) The types of facilities and services provided (for example, a lease of wet link capacity in the cable, collocation of licensee's equipment in the cable station with the ability to provide backhaul, or cable station and backhaul services provided to the licensee);

(2) For provisioned facilities and services, the volume or quantity provisioned, and the time interval between order and delivery; and

(3) The number of outages and intervals between fault report and facility or service restoration; and

(b) File quarterly, within 90 days from the end of each calendar quarter, a report of its active and idle 64 kbps or equivalent circuits by facility (terrestrial, satellite and submarine cable).

**§ 1.70016 Eligibility for streamlining.**

(a) *Eligibility for streamlining.* Each applicant must demonstrate eligibility for streamlining, except as otherwise set out in paragraph (b) of this section, by:

(1) Certifying that it is not a foreign carrier and it is not affiliated with a foreign carrier in any of the cable's destination markets;

(2) Demonstrating pursuant to § 63.12(c)(1)(i) through (iii) of this chapter that any such foreign carrier or affiliated foreign carrier lacks market power; or

(3) Certifying that the destination market where the applicant is, or has an affiliation with, a foreign carrier is a World Trade Organization (WTO) Member and the applicant agrees to accept and abide by the reporting requirements set out in § 1.70015. An application that includes an applicant that is, or is affiliated with, a carrier with market power in a cable's non-WTO Member destination country is not eligible for streamlining.

(4) Certifying that all individuals or entities that hold a ten percent or greater direct or indirect equity and/or voting interests, or a controlling interest, in the applicant are U.S. citizens or entities organized in the United States.

(5)(i) For a license to construct and operate a submarine cable system or to modify the construction of a previously approved submarine cable system, the applicant must certify that it is not required to submit a consistency certification to any state pursuant to section 1456(c)(3)(A) of the Coastal Zone Management Act (CZMA), 16 U.S.C. 1456.

(ii) Streamlining of cable landing license applications will be limited to those applications where all potentially affected states, having constructive notice that the application was filed with the Commission, have waived, or are deemed to have waived, any section 1456(c)(3)(A) right to review the application within the thirty-day period prescribed by 15 CFR 930.54.

(b) *Eligibility for streamlining of renewal or extension applications.* Each applicant for a renewal or extension of a cable landing license must demonstrate eligibility for streamlined processing of the application by:

(1) Including the information and certifications required in paragraph (a) of this section.

(2) [Reserved]

**§§ 1.70017–1.70020 [Reserved]**

**§ 1.70021 Electronic filing.**

(a) With the exception of submarine cable outage reports, and subject to the availability of electronic forms, all applications and notifications described in this subpart must be filed electronically through the International Communications Filing System (ICFS). A list of forms that are available for electronic filing can be found on the ICFS homepage. For information on electronic filing requirements, see subpart Y of this part, and the ICFS homepage at *https://www.fcc.gov/icfs.* See also §§ 63.20 and 63.53 of this chapter.

(b) Submarine cable outage reports must be filed as set forth in part 4 of this chapter.

**§ 1.70022 Action on applications, revocation, and termination.**

The Office of International Affairs shall determine appropriate procedures on a case by case basis for grant or denial of an application or revocation and/or termination of a cable landing license, and grant or deny an application, initiate and conduct application, revocation, and/or termination proceedings, and revoke and/or terminate a cable landing license, as required by due process and applicable law and in light of the relevant facts and circumstances, including providing the applicant or licensee with notice and opportunity to cure noncompliance to the extent such an opportunity is required by the Administrative Procedure Act, 5 U.S.C. 558(c), and to respond to allegations and evidence in the record.

**§§ 1.70023–1.70024 [Reserved]**

■ 10. Delayed indefinitely, amend § 1.70002 by adding paragraph (b) to read as follows:

**§ 1.70002 General requirements.**

* * * * *

(b) *Public interest statement.* An applicant seeking a cable landing license or modification, assignment, transfer of control, or renewal or extension of a cable landing license shall include in the application information demonstrating how the grant of the application will serve the public interest.

* * * * *

■ 11. Delayed indefinitely, add § 1.70003 to read as follows:

**§ 1.70003 Applicant/licensee requirements.**

Except as otherwise required by the Commission, the following entities, at a

minimum, shall be applicants for, and licensees on, a cable landing license:

(a) Any entity that controls a cable landing station in the United States; and

(b) All other entities owning or controlling a five percent (5%) or greater interest in the cable system and using the U.S. points of the cable system.

■ 12. Delayed indefinitely, add §§ 1.70005 and 1.70006 to read as follows:

**§ 1.70005 Initial application for a cable landing license.**

An applicant must demonstrate in the initial application for a cable landing license that it meets the requirements under § 1.70002(b) and (c), and the initial application must contain:

(a) The name, address, email address(es), and telephone number(s) of each applicant.

(b) The Government, State, or Territory under the laws of which each corporate or partnership applicant is organized.

(c) The name, title, address, email address(es), and telephone number of the officer and any other contact point, such as legal counsel, of each applicant to whom correspondence concerning the application is to be addressed.

(d) The name of the submarine cable system.

(e) A description of the submarine cable system, including:

(1) The States, Territories, or possessions in the United States and the foreign countries where the submarine cable system will land;

(2) The number of segments in the submarine cable system and the designation of each (*e.g.,* Segment A, Main Trunk, A–B segment);

(3) The length of the submarine cable system by segment and in total;

(4) The location, by segment, of any branching units;

(5) The number of optical fiber pairs, by segment, of the submarine cable system;

(6) The design capacity, by segment, of the submarine cable system;

(7) Specific geographic location information (geographic coordinates, street address, county or county equivalent, as applicable), or if not available, a general geographic description and specific geographic location information to be filed no later than ninety (90) days prior to construction regarding:

(i) Each U.S. and non-U.S. cable landing station and beach manhole;

(ii) Each network operations center (NOC) and backup NOC and, if distinct from the NOC, each security operations center (SOC) and backup SOC, or else a statement that the SOC and backup SOC are not distinct from the NOC and/or backup NOC;

(iii) Where each Power Feed Equipment (PFE) and each Submarine Line Terminal Equipment (SLTE) is connected with the terrestrial land based system(s) and from where each is operated; and

(iv) The route position list including the wet segment of the submarine cable system;

(8) Anticipated time frame when the applicant(s) intends to place the submarine cable system into service; and

(9) For each U.S. cable landing station that is not owned by the applicant(s), provide—

(i) The name of the entity(ies) that owns the cable landing station;

(ii) A statement that the owner(s) of the cable landing station will have no ability to significantly affect the operation of the submarine cable system;

(iii) A statement that the applicant(s) will meet the requirements under § 1.70007(k); and

(iv) A statement that the applicant(s) will ensure the landing station lease agreement(s) have initial terms, with extension options at the sole discretion of the applicant(s), for a total of 25 years, coextensive with the term of the cable landing license.

(f) A specific description of the submarine cable system consistent with paragraph (e)(7) of this section, including a map and geographic data in generally accepted GIS formats or other formats. The Office of International Affairs, in coordination with the Office of Economics and Analytics, shall determine the file formats and specific data fields in which data will ultimately be collected.

(1) The applicant initially may file a general geographic description of the information required in paragraph (e)(7) of this section; however, grant of the application will be conditioned on the Commission's final approval of specific location information, consistent with paragraph (e)(7), to be filed by the applicant no later than ninety (90) days prior to construction. The Commission will give public notice of the filing of each description, and grant of the license will be considered final with respect to that specific geographic location unless the Commission issues a notice to the contrary no later than sixty (60) days after receipt of the specific description, unless the Commission designates a different time period.

(2) Information under paragraph (e)(7) of this section and the exact location information of the wet segment as it approaches the shore, the submarine cable as it reaches the beach manhole, and the dry segment including the cable landing station(s), such as where the SLTE is located and/or from where it is operated, will be withheld from public inspection.

(3) The Commission may disclose to relevant Federal Government agencies information submitted by an applicant, petitioner, licensee, or authorization holder about the submarine cable system, including the location information of cable landing stations, beach manholes, PFE, SLTE, NOCs and backup NOCs, SOCs and backup SOCs, and route position lists. Where such information has been submitted in confidence pursuant to § 0.457 or § 0.459 of this chapter, such information may be shared subject to the provisions of § 0.442 of this chapter and, notwithstanding the provisions of § 0.442(d)(1) of this chapter, notice will be provided at the time of disclosure.

(g) A statement disclosing whether or not the applicant uses and/or will use the following third-party service providers, as defined in § 1.70001(d), in the operation of the submarine cable system:

(1) Any entity that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g);

(2) Any entity identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601 through 1609; and/or

(3) Any entity that can access the submarine cable from a foreign adversary country, as defined in § 1.70001(f), and to identify any such foreign adversary country.

(h) A statement as to whether the cable will be operated on a common carrier or non-common carrier basis. Applicants for common carrier cable landing licenses shall also separately file an application for an international section 214 authorization for overseas cable construction under § 63.18 of this chapter.

(i) A list of all of the proposed owners of the submarine cable system including those owners that are not applicants, their respective equity and/or voting interests in the submarine cable system as a whole, their respective equity and/or voting interests in each U.S. cable landing station including SLTE, and their respective equity and/or voting interests by segment of the cable.

(j) For each applicant:

(1) The information and certifications required in § 63.18(h), (o), (p), and (q) of this chapter;

(2) A certification as to whether or not the applicant is, or is affiliated with, a

foreign carrier, including an entity that owns or controls a cable landing station, in any foreign country. The certification shall state with specificity each such country;

(3) A certification as to whether or not the applicant seeks to land and operate a submarine cable connecting the United States to any country for which any of the following is true. The certification shall state with specificity the foreign carriers and each country:

(i) The applicant is a foreign carrier in that country; or

(ii) The applicant controls a foreign carrier in that country; or

(iii) There exists any entity that owns more than 25 percent of the applicant, or controls the applicant, or controls a foreign carrier in that country; or

(iv) Two or more foreign carriers (or parties that control foreign carriers) own, in the aggregate, more than 25 percent of the applicant and are parties to, or the beneficiaries of, a contractual relation (*e.g.,* a joint venture or market alliance) affecting the provision or marketing of arrangements for the terms of acquisition, sale, lease, transfer and use of capacity on the cable in the United States; and

(4) For any country that the applicant has listed in response to paragraph (j)(3) of this section that is not a member of the World Trade Organization, a demonstration as to whether the foreign carrier lacks market power with reference to the criteria in § 63.10(a) of this chapter.

(5) Under § 63.10(a) of this chapter, the Commission presumes, subject to rebuttal, that a foreign carrier lacks market power in a particular foreign country if the applicant demonstrates that the foreign carrier lacks 50 percent market share in international transport facilities or services, including cable landing station access and backhaul facilities, intercity facilities or services, and local access facilities or services on the foreign end of a particular route.

(k) The certifications in § 1.70006, including a certification that the applicant accepts and will abide by the routine conditions specified in § 1.70007, and information pursuant to §§ 1.70002(c) and 1.70004(a) and (b);

(l) [Reserved]

(m) Each applicant shall certify that it has created and will implement and update a cybersecurity and physical security risk management plan consistent with § 1.70006(c). Applicants shall submit cybersecurity and physical security risk management plans to the Commission upon request. The Office of International Affairs, in coordination with the Public Safety and Homeland Security Bureau, may request, at its discretion, submission of such cybersecurity and physical security risk management plans and evaluate them for compliance with the Commission's rules in this subpart. The cybersecurity and physical security risk management plans provided under this paragraph (m) shall be treated as presumptively confidential.

(n) Any other information that may be necessary to enable the Commission to act on the application.

(o) Applicants for cable landing licenses may be subject to the consistency certification requirements of the Coastal Zone Management Act (CZMA), 16 U.S.C. 1456, if they propose to conduct activities, in or outside of a coastal zone of a state with a federally-approved management plan, affecting any land or water use or natural resource of that state's coastal zone.

(1) Before filing their applications for a license to construct and operate a submarine cable system or to modify the construction of a previously approved submarine cable system, applicants must determine whether they are required to certify that their proposed activities will comply with the enforceable policies of a coastal state's approved management program. In order to make this determination, applicants should consult National Oceanic Atmospheric Administration (NOAA) regulations, 15 CFR part 930, subpart D, and review the approved management programs of coastal states in the vicinity of the proposed landing station to verify that this type of application is not a listed federal license activity requiring review.

(2) After the application is filed, applicants should follow the procedures specified in 15 CFR 930.54 to determine whether any potentially affected state has sought or received NOAA approval to review the application as an unlisted activity. If it is determined that any certification is required, applicants shall consult the affected coastal state(s) (or designated state agency(ies)) in determining the contents of any required consistency certification(s). Applicants may also consult the Office for Coastal Management (OCM) within NOAA for guidance.

(3) The cable landing license application filed with the Commission shall include any consistency certification required by 16 U.S.C. 1456(c)(3)(A) for any affected coastal state(s) that lists this type of application in its NOAA–approved coastal management program and shall be updated pursuant to § 1.65 to include any subsequently required consistency certification with respect to any state that has received NOAA approval to review the application as an unlisted federal license activity. Upon documentation from the applicant—or notification from each coastal state entitled to review the license application for consistency with a federally approved coastal management program—that the state has either concurred, or by its inaction, is conclusively presumed to have concurred with the applicant's consistency certification, the Commission may take action on the application.

**§ 1.70006 Certifications.**

An applicant must certify to the following in the initial application for a cable landing license:

(a) That the applicant accepts and will abide by the routine conditions specified in § 1.70007.

(b) Whether or not it exhibits any of the criteria set out in the presumptive disqualifying conditions per §§ 1.70002(c) and 1.70004(a) and (b):

(1) *Character presumptive disqualifying condition.* An applicant seeking a cable landing license or modification, assignment, transfer of control, or renewal or extension of a cable landing license, shall also certify in the application whether or not the applicant has the requisite character qualifications as set out in § 1.70002(c). In an application for an assignment or transfer of control, the licensee, assignee/transferee, and assignor/transferor must submit this certification;

(2) *Foreign adversary presumptive disqualifying condition.* An applicant seeking a cable landing license or modification, assignment, transfer of control, or renewal or extension of a cable landing license, shall certify in the application whether or not it exhibits any of the criteria set out in the presumptive disqualifying condition under § 1.70004(a); and

(3) *Foreign adversary cable landing presumptive disqualifying condition.* An applicant seeking a cable landing license or modification or renewal or extension of a cable landing license, shall certify whether or not it exhibits any of the criteria set out in the presumptive disqualifying condition under § 1.70004(b).

(c) That the applicant has created and will implement and update a cybersecurity and physical security risk management plan, and:

(1) That the plan describes how the applicant will take reasonable measures to employ its organizational resources and processes to ensure the confidentiality, integrity, and availability of its systems and services that could affect its provision of

communications services through the submarine cable system;

(2) That the plan identifies the cybersecurity risks the applicant faces, the controls it uses or plans to use to mitigate those risks, and how the applicant will ensure that these controls are applied effectively to its operations;

(3) That the plan addresses both logical and physical access risks, as well as supply chain risks;

(4) That the plan has been signed by the entity's Chief Executive Officer, Chief Financial Officer, Chief Technology Officer, Chief Information Security Officer, or similarly situated senior officer responsible for governance of the organization's security practices;

(5) That the applicant will submit cybersecurity and physical security risk management plans to the Commission upon request; and

(6) That the applicant will preserve data and records related to its cybersecurity and physical security risk management plans, including documentation necessary to demonstrate how those plans are implemented, for a period of two years from the date the related risk management plan certification is submitted to the Commission.

(d) That the submarine cable system will not use equipment or services identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601 through 1609.

■ 13. Delayed indefinitely, amend § 1.70007 by adding paragraphs (f) through (h), (l), (m), (q), (s), (t), (v), and (x) to read as follows:

**§ 1.70007 Routine conditions.**

* * * * *

(f) The cable landing license and rights granted in the license shall not be transferred, assigned, or disposed of, or disposed of indirectly by transfer of control of the licensee, except in compliance with the requirements set out in §§ 1.70012 and 1.70013.

(g) Entities that are parties to a *pro forma* assignment or transfer of control must notify the Commission no later than thirty (30) days after the assignment or transfer of control is consummated, and the notification must include information and certifications required under § 1.70013.

(h) Unless the licensee has notified the Commission in the application of the specific geographic location information required by § 1.70005(e)(7) and (f), the licensee shall notify the Commission no later than ninety (90) days prior to commencing construction. The Commission will give public notice of the filing of each description, and grant of the cable landing license will be considered final with respect to that specific geographic location unless the Commission issues a notice to the contrary no later than sixty (60) days after receipt of the specific description, unless the Commission designates a different time period.

* * * * *

(l) The licensee shall comply with the requirements of § 1.70009.

(m) The licensee shall file annual circuit capacity reports as required by § 43.82 of this chapter.

* * * * *

(q) The licensee must implement a cybersecurity and physical security risk management plan consistent with the requirements in § 1.70006(c) as of the date the submarine cable is placed into service.

(1) The licensee must certify to the Commission, within thirty (30) days of the date the submarine cable is placed into service, that it has created and implemented the cybersecurity and physical security risk management plan as of the in-service date.

(2) The licensee must continue to implement and update, as required based on material changes to the cybersecurity and physical security risks and vulnerabilities that the licensee faces, the cybersecurity and physical security risk management plan.

(3) The licensee shall submit cybersecurity and physical security risk management plans to the Commission upon request. The Office of International Affairs, in coordination with the Public Safety and Homeland Security Bureau, may request, at its discretion, submission of such cybersecurity and physical security risk management plans and evaluate them for compliance with the Commission's rules in this subpart. The cybersecurity and physical security risk management plans provided under this paragraph (q)(3) shall be treated as presumptively confidential.

(4) The licensee shall preserve data and records related to its cybersecurity and physical security risk management plans, including documentation necessary to demonstrate how those plans are implemented, for a period of two years from the date the related risk management plan certification is submitted to the Commission.

* * * * *

(s) The licensee shall notify the Commission of any changes to the following within thirty (30) days:

(1) The contact information of the licensee provided under § 1.70005(a) and (c); and

(2) The name of the licensee (including the name under which the licensee is doing business).

(t) The licensee(s) shall notify the Commission of any changes to the name of the licensed submarine cable system within thirty (30) days of such change. If there are multiple licensees of the submarine cable system, the lead licensee shall file the notification.

* * * * *

(v) The licensee(s) that meet the applicant/licensee requirements of § 1.70003 and criteria under § 1.70017(b) shall submit a Foreign Adversary Annual Report every year consistent with the requirements under § 1.70017.

* * * * *

(x) Cable landing licensees with a license granted prior to [effective date of amendatory instruction 13], must submit a route position list consistent with the requirement under § 1.70005(e)(7)(iv) under the relevant license file number in the Commission's International Communications Filing System (ICFS), or any successor system, no later than sixty (60) days after [effective date of amendatory instruction 13]. Licensees may petition the Commission for waiver of the requirement, which may be granted only to the extent the licensee demonstrates that the required information is unavailable by the submission deadline.

■ 14. Delayed indefinitely, add §§ 1.70008 and 1.70009 to read as follows:

**§ 1.70008 Requests for special temporary authority.**

(a) Special temporary authority may be used for construction, testing, or operation of a submarine cable system for a term up to and including 180 days.

(b) Applicants seeking special temporary authority must file the requisite application(s) related to the request for special temporary authority. Applicants must identify the file number(s) of any pending application(s) associated with the request for special temporary authority.

(c) An application for special temporary authority must include:

(1) A narrative describing the request for a special temporary authority including the type of request (*e.g.* new request, extension or renewal of previous request, or other), purpose for the special temporary authority (construction, testing, operating, or other), and the justification for such request;

(2) Information required by § 1.70005(a) through (d);

(3) Whether or not the request for special temporary authority is

associated with an application(s) pending with the Commission, and if so, identification of the related file number(s);

(4) The date by which applicants seek grant of the request for special temporary authority and the duration for which applicants seek special temporary authority;

(5) An acknowledgement that any grant of special temporary authority:

(i) Does not prejudice action by the Commission on any underlying application(s);

(ii) Is subject to revocation/cancellation or modification by the Commission on its own motion without a hearing;

(iii) Will expire automatically upon the termination date unless the applicant has made a timely and complete application for extension of the special temporary authority; and

(iv) Does not preclude enforcement action for non-compliance with the Cable Landing License Act, the Communications Act, or the Commission's rules in this chapter for action or failure to act at any time before or after grant of the special temporary authority; and

(6) The certification required in § 63.18(o) of this chapter.

(7) Any other information that may be necessary to enable the Commission to act on the application.

**§ 1.70009 Notification by and prior approval for cable landing licensees that are or propose to become affiliated with a foreign carrier.**

Any entity that is licensed by the Commission (''licensee'') to land or operate a submarine cable landing in a particular foreign destination market that becomes, or seeks to become, affiliated with a foreign carrier that is authorized to operate in that market, including an entity that owns or controls a cable landing station in that market, shall notify the Commission of that affiliation.

(a) *Affiliations requiring prior notification.* Except as provided in paragraph (b) of this section, the licensee must notify the Commission, pursuant to this section, forty-five (45) days before consummation of either of the following types of transactions:

(1) Acquisition by the licensee, or by any entity that controls the licensee, or by any entity that directly or indirectly owns more than twenty-five percent (25%) of the capital stock of the licensee, of a controlling interest in a foreign carrier that is authorized to operate in a market where the cable lands; or

(2) Acquisition of a direct or indirect interest greater than twenty-five percent (25%), or of a controlling interest, in the capital stock of the licensee by a foreign carrier that is authorized to operate in a market where the cable lands, or by an entity that controls such a foreign carrier.

(b) *Exceptions.* (1) Notwithstanding paragraph (a) of this section, the notification required by this section need not be filed before consummation, and may instead by filed pursuant to paragraph (c) of this section, if either of the following is true with respect to the named foreign carrier, regardless of whether the destination market where the cable lands is a World Trade Organization (WTO) or non-WTO Member:

(i) The Commission has previously determined in an adjudication that the foreign carrier lacks market power in that destination market (for example, in an international section 214 application or a declaratory ruling proceeding); or

(ii) The foreign carrier owns no facilities in that destination market. For this purpose, a carrier is said to own facilities if it holds an ownership, indefeasible-right-of-user, or leasehold interest in a cable landing station or in bare capacity in international or domestic telecommunications facilities (excluding switches).

(2) In the event paragraph (b)(1) of this section cannot be satisfied, notwithstanding paragraph (a) of this section, the notification required by this section need not be filed before consummation, and may instead be filed pursuant to paragraph (c) of this section, if the licensee certifies that the destination market where the cable lands is a WTO Member and provides certification to satisfy either of the following:

(i) The licensee demonstrates that its foreign carrier affiliate lacks market power in the cable's destination market pursuant to § 63.10(a)(3) of this chapter; or

(ii) The licensee agrees to comply with the reporting requirements contained in § 1.70015 effective upon the acquisition of the affiliation.

(c) *Notification after consummation.* Any licensee that becomes affiliated with a foreign carrier and has not previously notified the Commission pursuant to the requirements of this section shall notify the Commission within thirty (30) days after consummation of the acquisition.

*Example 1 to paragraph (c).* Acquisition by a licensee (or by any entity that directly or indirectly controls, is controlled by, or is under direct or indirect common control with the licensee) of a direct or indirect interest in a foreign carrier that is greater than twenty-five percent (25%) but not controlling is subject to this paragraph (c) but not to paragraph (a) of this section.

*Example 2 to paragraph (c).* Notification of an acquisition by a licensee of a hundred percent (100%) interest in a foreign carrier may be made after consummation, pursuant to this paragraph (c), if the foreign carrier operates only as a resale carrier.

*Example 3 to paragraph (c).* Notification of an acquisition by a foreign carrier from a WTO Member of a greater than twenty-five percent (25%) interest in the capital stock of the licensee may be made after consummation, pursuant to this paragraph (c), if the licensee demonstrates in the post-notification that the foreign carrier lacks market power in the cable's destination market or the licensee agrees to comply with the reporting requirements contained in § 1.70015 effective upon the acquisition of the affiliation.

(d) *Cross-reference.* In the event a transaction requiring a foreign carrier notification pursuant to this section also requires a transfer of control or assignment application pursuant to the requirements of the license granted under § 1.70007(f) and (g), § 1.70012, or § 1.70013, the foreign carrier notification shall reference in the notification the transfer of control or assignment application and the date of its filing. See § 1.70007.

(e) *Contents of notification.* The notification shall certify the following information:

(1) The name of the newly affiliated foreign carrier and the country or countries at the foreign end of the cable in which it is authorized to provide telecommunications services to the public or where it owns or controls a cable landing station.

(2) Which, if any, of those countries is a Member of the World Trade Organization.

(3) The name of the cable system that is the subject of the notification, and the FCC file number(s) under which the license was granted.

(4) The name, address, citizenship, and principal business of any person or entity that directly or indirectly owns ten percent or more of the equity interests and/or voting interests, or a controlling interest, of the licensee, and the percentage of equity and/or voting interest owned by each of those entities (to the nearest one percent). Where no individual or entity directly or indirectly owns ten percent or more of the equity interests and/or voting interests, or a controlling interest, of the licensee, a statement to that effect.

(i) *Calculation of equity interests held indirectly in the licensee.* Equity interests that are held by an individual or entity indirectly through one or more intervening entities shall be calculated by successive multiplication of the equity percentages for each link in the vertical ownership chain, regardless of whether any particular link in the chain represents a controlling interest in the company positioned in the next lower tier. Example: An entity holds a non-controlling 30 percent equity and voting interest in Corporation A which, in turn, holds a non-controlling 40 percent equity and voting interest in the licensee. The entity's equity interest in the licensee would be calculated by multiplying the individual's equity interest in Corporation A by that entity's equity interest in the licensee. The entity's equity interest in the licensee would be calculated as 12 percent (30% × 40% = 12%). The result would be the same even if Corporation A held a de facto controlling interest in the licensee.

(ii) *Calculation of voting interests held indirectly in the licensee.* Voting interests that are held through one or more intervening entities shall be calculated by successive multiplication of the voting percentages for each link in the vertical ownership chain, except that wherever the voting interest for any link in the chain is equal to or exceeds 50 percent or represents actual control, it shall be treated as if it were a 100 percent interest. A general partner shall be deemed to hold the same voting interest as the partnership holds in the company situated in the next lower tier of the vertical ownership chain. A partner of a limited partnership (other than a general partner) shall be deemed to hold a voting interest in the partnership that is equal to the partner's equity interest. Example: An entity holds a non-controlling 30 percent equity and voting interest in Corporation A which, in turn, holds a controlling 70 percent equity and voting interest in the licensee. Because Corporation A's 70 percent voting interest in the licensee constitutes a controlling interest, it is treated as a 100 percent interest. The entity's 30 percent voting interest in Corporation A would flow through in its entirety to the licensee and thus be calculated as 30 percent (30% × 100% = 30%).

(5) An ownership diagram that illustrates the licensee's vertical ownership structure, including the direct and indirect ownership (equity and voting) interests held by the individuals and entities named in response to paragraph (e)(4) of this section. Every individual or entity with ownership shall be depicted and all controlling interests must be identified.

(6) The name of any interlocking directorates, as defined in § 63.09(g) of this chapter, with each foreign carrier named in the notification.

(7) With respect to each foreign carrier named in the notification, a statement as to whether the notification is subject to paragraph (a) or (c) of this section. In the case of a notification subject to paragraph (a) of this section, the licensee shall include the projected date of closing. In the case of a notification subject to paragraph (c) of this section, the licensee shall include the actual date of closing.

(8) If a licensee relies on an exception in paragraph (b) of this section, then a certification as to which exception the foreign carrier satisfies and a citation to any adjudication upon which the licensee is relying. Licensees relying upon the exceptions in paragraph (b)(2) of this section must make the required certified demonstration in paragraph (b)(2)(i) of this section or the certified commitment to comply with the reporting requirements in paragraph (b)(2)(ii) of this section in the notification required by paragraph (c) of this section.

(f) *Exemptions based on lack of market power.* If the licensee seeks exemption from the reporting requirements contained in § 1.70015, the licensee should demonstrate that each foreign carrier affiliate named in the notification lacks market power pursuant to § 63.10(a)(3) of this chapter.

(g) *Procedure.* After the Commission issues a public notice of the submissions made under this section, interested parties may file comments within fourteen (14) days of the public notice.

(1) If the Commission deems it necessary at any time before or after the deadline for submission of public comments, the Commission may impose reporting requirements on the licensee based on the provisions of § 1.70015.

(2) In the case of a prior notification filed pursuant to paragraph (a) of this section, the authorized U.S. licensee must demonstrate that it continues to serve the public interest for it to retain its interest in the cable landing license for that segment of the cable that lands in the non-WTO destination market. Such a showing shall include a demonstration as to whether the foreign carrier lacks market power in the non-WTO destination market with reference to the criteria in § 63.10(a) of this chapter. In addition, upon request of the Commission, the licensee shall provide the information specified in § 1.70005(j). If the licensee is unable to make the required showing or is notified by the Commission that the affiliation may otherwise harm the public interest pursuant to the Commission's policies and rules in this chapter under 47 U.S.C. 34 through 39 and Executive Order 10530, dated May 10, 1954, then the Commission may impose conditions necessary to address any public interest harms or may proceed to an immediate authorization revocation hearing.

(3) Under § 63.10(a) of this chapter, the Commission presumes, subject to rebuttal, that a foreign carrier lacks market power in a particular foreign country if the applicant demonstrates that the foreign carrier lacks 50 percent market share in international transport facilities or services, including cable landing station access and backhaul facilities, intercity facilities or services, and local access facilities or services on the foreign end of a particular route.

(h) *Continuing accuracy of information.* All licensees are responsible for the continuing accuracy of information provided pursuant to this section for a period of forty-five (45) days after filing. During this period if the information furnished is no longer accurate, the licensee shall as promptly as possible, and in any event within ten (10) days, unless good cause is shown, file with the Commission a corrected notification referencing the FCC file numbers under which the original notification was provided.

(i) *Requests for confidential treatment.* A licensee that files a prior notification pursuant to paragraph (a) of this section may request confidential treatment of its filing, pursuant to § 0.459 of this chapter, for the first twenty (20) days after filing.

(j) *Electronic filing.* Subject to the availability of electronic forms, all notifications described in this section must be filed electronically through the International Communications Filing System (ICFS). A list of forms that are available for electronic filing can be found on the ICFS homepage. For information on electronic filing requirements, see §§ 1.10000 through 1.10018 and the ICFS homepage at *https://www.fcc.gov/icfs.* See also §§ 63.20 and 63.53 of this chapter.

■ 15. Delayed indefinitely, add §§ 1.70011 through 1.70013 to read as follows:

**§ 1.70011 Applications for modification of a cable landing license.**

A separate application shall be filed with respect to each individual submarine cable system for which a licensee(s) seeks to modify the cable landing license. Each modification application shall include a narrative

description of the proposed modification including relevant facts and circumstances leading to the request. Each modification application must contain information pursuant to §§ 1.70002(b) and (c) and 1.70004. Requirements for specific types of modification requests are set out below. For other situations, the licensee(s) should contact Commission staff regarding the required information for the modification application.

(a) An application to add a landing point(s), segment(s), or other like material changes to a submarine cable system must also include the following:

(1) Information as required by § 1.70005(a) through (i), (k), (m), and (o), except as specified in paragraph (a)(2) of this section, as it relates to the modified portion of the cable system and a description of how any new landing point(s) or segment(s) will be connected to the cable system;

(2) Certifications set forth under § 1.70006, except for § 1.70006(d). A licensee seeking a modification of a cable landing license must certify in the application that it has created, updated, and implemented a cybersecurity and physical security risk management plan, consistent with §§ 1.70006(c) and 1.70007(q);

(3) Any other information that may be necessary to enable the Commission to act on the application; and

(4) Signature(s) by each licensee. Joint licensees may appoint one party to act as proxy for purposes of complying with this paragraph (a)(4).

(b) An application to add an applicant as a licensee for an existing cable landing license must also include the following:

(1) Information required by § 1.70005(a) through (c), (g), (j), (k), and (m), except as specified in paragraph (b)(4) of this section, for the proposed new licensee;

(2) Information required by § 1.70005(d) through (f);

(3) Information required by § 1.70005(i) for the proposed new licensee and current owners of the submarine cable system;

(4) Certifications set forth under § 1.70006 for the proposed new licensee, except for § 1.70006(d);

(5) Any other information that may be necessary to enable the Commission to act on the application; and

(6) Signature(s) by the proposed licensee and each current licensee. Joint licensees may appoint one party to act as proxy for purposes of complying with this paragraph (b)(6).

(c) A notification of the removal of a landing point(s), segment(s), or other like changes to a submarine cable system must be filed no later than 30 days after the removal. The notification must also include the following:

(1) Information as required by § 1.70005(a) through (d);

(2) A description of which element(s) were removed from the submarine cable system and the date on which the element(s) was removed from the submarine cable system;

(3) An updated description of the submarine cable system after the removal of the elements of the submarine cable system;

(4) An explanation of what happened with the physical facilities upon removal from the submarine cable system;

(5) An explanation of how the removal affected the ownership of the remaining portions of the submarine cable;

(6) Any other information that may be necessary to enable the Commission to act on the notification; and

(7) Signature(s) by each licensee. Joint licensees may appoint one party to act as proxy for purposes of complying with this paragraph (c)(7).

(d) A notification that a licensee(s) has relinquished an interest in a cable landing license must be filed no later than 30 days after the relinquishment. The notification must also include:

(1) Information required by § 1.70005(a) through (d) for the licensee(s) that relinquished an interest in the submarine cable system;

(2) The ownership interests that were held by that licensee(s) prior to the relinquishment;

(3) Whether the licensee(s) relinquished all of its interests in the submarine cable system or what interests it has retained;

(4) An explanation of what happened to the interests that were relinquished (whether the interests were re-distributed pro rata amongst the remaining licensees or otherwise re-distributed);

(5) A demonstration that the entity is not required to be a licensee under § 1.70003 and that the remaining licensee(s) retain collectively *de jure* and *de facto* control of the U.S. portion of the submarine cable system sufficient to comply with the requirements of the Commission's rules in this chapter and any specific conditions of the license;

(6) A signature(s) from the licensee(s) that relinquished its interest;

(7) Any other information that may be necessary to enable the Commission to act on the notification; and

(8) A certification that the notification was served on each of the other licensees of the submarine cable system.

(e) If any joint licensee(s) of a submarine cable no longer exists and did not file a notification to modify the license to relinquish its interest in the license, the remaining joint licensee(s) of the cable may collectively file a modification notification to remove the licensee from the license. Joint licensees may appoint one party to act as proxy for purposes of complying with this paragraph (e). The notification must also include:

(1) Information required by § 1.70005(a) through (d) for the licensee(s) that seeks to remove a licensee(s) from a cable landing license;

(2) An explanation of why the licensee(s) request removal of a licensee(s) from the license;

(3) A description of the efforts to contact the licensee to be removed;

(4) The ownership interests in the submarine cable held by the licensee(s) to be removed;

(5) An explanation of what will happen to the interests of the licensee(s) that will be removed (whether the interests were re-distributed pro rata amongst the remaining licensees or otherwise re-distributed);

(6) A demonstration that the remaining licensee(s) retain collectively *de jure* and *de facto* control of the U.S. portion of the cable system sufficient to comply with the requirements of the Commission's rules in this chapter and any specific conditions of the license;

(7) A signature(s) from all of the licensee(s) of the submarine cable that seeks to remove the licensee(s);

(8) Any other information that may be necessary to enable the Commission to act on the notification; and

(9) A certification that the notification was served on each of the other licensees of the submarine cable system.

(f) A notification to add, remove, or otherwise change a condition on the cable landing license regarding compliance with a national security mitigation agreement (*e.g.,* Letter of Agreement or National Security Agreement) must be filed no later than 30 days after the change. The notification must include the following:

(1) Information required by § 1.70005(a) through (c) of the licensee(s) that seeks to add, remove, or change a condition;

(2) Information required by § 1.70005(d);

(3) An explanation of the change in the national security condition;

(4) A copy of the new national security mitigation agreement, if applicable;

(5) A certification that the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (Committee) agrees with the change;

(6) A certification that the notification has been served on the Chair of the Committee;

(7) A signature(s) from the licensee(s) that seeks to add, remove, or change a condition; and

(8) Any other information that may be necessary to enable the Commission to act on the notification.

(g) If a landing point is being moved within the same town/city/county as approved in the cable landing license, the licensee(s) must file a notification no later than 30 days after the landing point is moved. The notification must include:

(1) Information as required by § 1.70005(a) through (f), as it relates to the modified portion of the cable system;

(2) Any other information that may be necessary to enable the Commission to act on the notification; and

(3) Signature(s) by each licensee. Joint licensees may appoint one party to act as proxy for purposes of complying with this paragraph (g)(3).

(h) A notification to add an interconnection between two or more licensed cable systems must be filed no later than ninety (90) days prior to construction. The Commission will give public notice of the filing of this description, and grant of the modification will be considered final if the Commission does not notify the applicant otherwise in writing no later than sixty (60) days after receipt of the notification, unless the Commission designates a different time period. If, upon review of the notification, the Commission finds that the proposed interconnection presents a risk to national security, law enforcement, foreign policy, and/or trade policy or raises other concerns, it may require the licensee(s) to file a complete modification application to seek Commission approval for the interconnection. The notification must include:

(1) Information as required by § 1.70005(a) through (c) for each licensee of the submarine cables to be interconnected;

(2) Information as required by § 1.70005(d) and the license file number of each of the cable systems to be interconnected;

(3) A general description of where the interconnection will take place and the terms of the interconnection agreement;

(4) Any other information that may be necessary to enable the Commission to act on the notification; and

(5) Signature(s) by each licensee of each cable to be interconnected. Joint licensees may appoint one party to act as proxy for purposes of complying with this paragraph (h)(5).

(i) A notification to add a new connection between a branching unit of a licensed submarine cable and a foreign landing point must be filed no later than ninety (90) days prior to construction. The Commission will give public notice of the filing of this description, and grant of the modification will be considered final if the Commission does not notify the applicant otherwise in writing no later than sixty (60) days after receipt of the notification, unless the Commission designates a different time period. If, upon review of the notification, the Commission finds that the proposed connection presents a risk to national security, law enforcement, foreign policy, and/or trade policy or raises other concerns, it may require the licensee(s) to file a complete modification application to seek Commission approval for the connection. The notification must include:

(1) Information as required by § 1.70005(a) through (c) for each licensee of the Commission-licensed cable whose branching unit will be used to make the connection between two (or more) foreign points;

(2) Information as required by § 1.70005(d) and the license file number of the Commission-licensed cable whose branching unit will be used to make the connection between two (or more) foreign points;

(3) A description of the proposed connection, including which foreign points would be connected;

(4) The relationship between the owner of the proposed connection and the licensees of the Commission-licensed cable whose branching unit will be used to make the connection between two (or more) foreign points;

(5) An explanation of how the proposed connection would not allow for direct connection from the new foreign point(s) to the United States

(6) Any other information that may be necessary to enable the Commission to act on the notification; and

(7) Signature(s) by each licensee of the cable. Joint licensees may appoint one party to act as proxy for purposes of complying with this paragraph (i)(7).

**§ 1.70012 Substantial assignment or transfer of control applications.**

(a) Each application for authority to assign or transfer control of an interest in a cable system shall contain information pursuant to §§ 1.70002(b) and (c) and 1.70004(a). The application shall contain a certification as to whether or not the licensee, assignor/transferor, or assignee/transferee exhibit any of the criteria set out in the presumptive disqualifying conditions under §§ 1.70002(c)(1) and 1.70004(a)(1).

(b) An application for authority to assign or transfer control of an interest in a cable system shall contain a narrative description of the proposed transaction, including relevant facts and circumstances. The application shall also include the following information:

(1) The information requested in § 1.70005(a) through (c) for both the assignor/transferor and the assignee/transferee.

(2) The information required in § 1.70005(d) through (f).

(3) A narrative describing the means by which the assignment or transfer of control will take place.

(4) The information and certifications required in § 1.70005(j) for the assignee or the transferee and the licensee that is the subject of the transfer of control.

(5) The application shall also specify, on a segment specific basis, the percentage of voting and ownership interests being assigned or transferred in the cable system, including in the U.S. portion of the cable system (which includes all U.S. cable landing station(s)).

(6) The information and certifications required in § 1.70005(g) and (m), except as specified in paragraph (b)(7) of this section, for each assignee or licensee that is the subject of a transfer of control.

(7) The certifications set forth in § 1.70006, except for § 1.70006(d). A licensee seeking an assignment or transfer of control of a cable landing license must certify in the application that it has created, updated, and implemented a cybersecurity and physical security risk management plan, consistent with §§ 1.70006(c) and 1.70007(q). The application must also include a certification that the assignee or the transferee and the licensee that is the subject of the transfer of control accepts and will abide by the routine conditions specified in § 1.70007.

(8) In the event the transaction requiring an assignment or transfer of control application also requires the filing of a foreign carrier affiliation notification pursuant to § 1.70009, the application shall reference the foreign carrier affiliation notification and the date of its filing.

(9) The Commission reserves the right to request additional information concerning the transaction to aid it in making its public interest determination.

(10) An assignee or transferee must notify the Commission no later than thirty (30) days after either

consummation of the assignment or transfer or a decision not to consummate the assignment or transfer. The notification shall identify the file numbers under which the initial license and the authorization of the assignment or transfer were granted.

**§ 1.70013 Pro forma assignment and transfer of control notifications.**

(a) A *pro forma* assignee or a licensee that is the subject of a *pro forma* transfer of control of a cable landing license is not required to seek prior approval for the *pro forma* transaction. A *pro forma* assignee or licensee that is the subject of a *pro forma* transfer of control must notify the Commission no later than thirty (30) days after the assignment or transfer of control is consummated.

(b) Assignments or transfers of control that do not result in a change in the actual controlling party are considered non-substantial or *pro forma.* Whether there has been a change in the actual controlling party must be determined on a case-by-case basis with reference to the factors listed in note 1 to § 63.24(d) of this chapter. The types of transactions listed in note 2 to § 63.24(d) of this chapter will be considered presumptively *pro forma* and prior approval from the Commission need not be sought. A notification of a *pro forma* assignment or transfer of control shall include the following information:

(1) The information requested in § 1.70005(a) through (c) for both the assignor/transferor and the assignee/transferee.

(2) The information required in § 1.70005(d).

(3) A narrative describing the means by which the *pro forma* assignment or transfer of control occurred.

(4) The information and certifications required in § 63.18(h), (o), and (q) of this chapter for the assignee or the transferee and the licensee that is the subject of the transfer of control.

(5) The notification shall also specify, on a segment specific basis, the percentage of voting and ownership interests being assigned or transferred in the cable system, including in the U.S. portion of the cable system (which includes all U.S. cable landing station(s)).

(6) The notification must certify that the assignment or transfer of control was *pro forma,* as defined in this paragraph (b), and, together with all previous *pro forma* transactions, does not result in a change of the licensee's ultimate control.

(7) The information and certifications required in § 1.70005(j)(2) through (5).

(8) A certification that the assignee or the transferee and the licensee that is the subject of the transfer of control accepts and will abide by the routine conditions specified in § 1.70007.

(9) A certification as to whether or not the licensee, assignor/transferor, or assignee/transferee exhibit any of the criteria set out in the presumptive disqualifying conditions under §§ 1.70002(c)(1) and 1.70004(a)(1).

(10) The licensee may file a single notification for an assignment or transfer of control of multiple licenses issued in the name of the licensee if each license is identified by the file number under which it was granted.

(11) The Commission reserves the right to request additional information concerning the transaction to aid it in making its public interest determination.

■ 16. Delayed indefinitely, amend § 1.70016 by:

■ a. Removing the period at the end of paragraph (b)(1) and adding ''; and'' in its place; and

■ b. Adding paragraph (b)(2).

The addition reads as follows:

**§ 1.70016 Eligibility for streamlining.**

* * * * *

(b) * * *

(2) Certifying that individuals or entities that hold a ten percent or greater direct or indirect equity and/or voting interests, or a controlling interest, in the applicant are:

(i) U.S. citizens or entities organized in the United States; and/or

(ii) Individuals or entities that have citizenship(s) or place of organization in a foreign country and:

(A) Do not have a citizenship(s) or place of organization in a foreign adversary country, as defined in § 1.70001(f); and

(B) Whose ownership interest in the applicant has been previously reviewed by the Commission and the Committee.

■ 17. Delayed indefinitely, add § 1.70017 to read as follows:

**§ 1.70017 Foreign adversary annual report for licensees.**

(a) *Annual report.* Licensees shall file every year an annual report in the relevant File Number in the Commission's International Communications Filing System (ICFS), or any successor system.

(b) *Criteria for who must report.* The annual reporting requirement in this section applies to a licensee:

(1) That is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in § 1.70001(g);

(2) That is identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601 through 1609;

(3) Whose authorization, license, or other Commission approval, whether or not related to operation of a submarine cable, was denied or revoked and/or terminated or is denied or revoked and/or terminated in the future on national security and law enforcement grounds, as well as the current and future affiliates or subsidiaries of any such entity; and/or

(4) Whose submarine cable system is licensed to land or operate in a foreign adversary country, as defined in § 1.70001(f).

(c) *Information contents.* The Foreign Adversary Annual Report shall include information that is current as of thirty (30) days prior to the filing deadline, as follows:

(1) The information as required in § 1.70005(a) through (g), (i), and (m).

(2) Certifications as set forth under § 1.70006, except for § 1.70006(b) and (d).

(d) *Reporting deadlines.* Licensees shall submit their initial Foreign Adversary Annual Report within six months of [effective date of amendatory instruction 17], and each year. OIA shall establish and modify, as appropriate, the filing manner and associated deadlines for the Foreign Adversary Annual Report. OIA may, if needed, consult with the relevant Executive Branch agencies concerning the filing manner and associated deadlines for the annual reports. Licensees shall file the Foreign Adversary Annual Report pursuant to the deadlines.

(e) *Filing with the committee.* Licensees shall file a copy of the report directly with the Committee.

■ 18. Delayed indefinitely, add § 1.70020 to read as follows:

**§ 1.70020 Renewal and extension applications.**

(a) Licensees seeking to renew or extend a cable landing license shall file an application six months prior to the expiration of the license.

(b) The application must include the information and certifications required in §§ 1.70002(b) and (c), 1.70004, 1.70005, and 1.70006 (except for § 1.70006(d)). A licensee seeking a renewal or extension of a cable landing license must certify in the application that it has created, updated, and implemented a cybersecurity and physical security risk management plan, consistent with §§ 1.70006(c) and 1.70007(q).

(c) Upon the filing of a timely and complete application to renew or extend a cable landing license in accordance with the Commission's rules in this

chapter, a licensee may continue operating the submarine cable system while the application is pending with the Commission.

■ 19. Delayed indefinitely, add §§ 1.70023 and 1.70024 to read as follows:

**§ 1.70023 Covered list certification for cable landing licensees.**

Each cable landing licensee shall submit a certification, within sixty (60) days of [effective date of amendatory instruction 19], that it will not add to its submarine cable system(s) under its respective license(s) equipment or services identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601 through 1609; except, this condition shall not apply to a licensee that is identified on the Covered List whose cable landing license was or is granted prior to [effective date of amendatory instruction 19].

**§ 1.70024 One-time cybersecurity and physical security certification.**

(a) *Existing licensees.* Each licensee whose cable landing license was granted before [effective date of amendatory instruction 19], must:

(1) Implement a cybersecurity and physical security risk management plan consistent with the requirements in § 1.70006(c) within one year of [effective date of amendatory instruction 19]. To the extent the licensee does not commence service on the submarine cable by this timeframe, the licensee must implement a cybersecurity and physical security risk management plan as of the date the submarine cable is placed into service.

(2) Submit a certification to the Commission within thirty (30) days of [effective date of amendatory instruction 19], that it will implement a cybersecurity and physical security risk management plan consistent with the requirements in § 1.70006(c).

(3) The licensee shall submit cybersecurity and physical security risk management plans to the Commission upon request. The Office of International Affairs, in coordination with the Public Safety and Homeland Security Bureau, may request, at its discretion, submission of such cybersecurity and physical security risk management plans and evaluate them for compliance with the Commission's rules in this subpart. The cybersecurity and physical security risk management plans provided under this subsection shall be treated as presumptively confidential.

(4) The licensee shall preserve data and records related to its cybersecurity and physical security risk management plans, including documentation necessary to demonstrate how those plans are implemented, for a period of two years from the date the related risk management plan certification is submitted to the Commission.

(b) *Pending application for cable landing license.* If an application for a cable landing license is filed prior to [effective date of amendatory instruction 19], and remains pending on or after [effective date of amendatory instruction 19], the applicant(s) must submit a certification, within thirty (30) days of [effective date of amendatory instruction 19], attesting that it will create and implement a cybersecurity and physical security risk management plan as of the date the submarine cable is placed into service.

## PART 43—REPORTS OF COMMUNICATION COMMON CARRIERS, PROVIDERS OF INTERNATIONAL SERVICES AND CERTAIN AFFILIATES

■ 20. The authority citation for part 43 continues to read as follows:

**Authority:** 47 U.S.C. 35–39, 154, 211, 219, 220; sec. 402(b)(2)(B), (c), Pub. L. 104–104, 110 Stat. 129.

**§ 43.82 [Amended]**

■ 21. Amend § 43.82 by removing and reserving paragraph (a)(1).

■ 22. Delayed indefinitely, further amend § 43.82 by:

■ a. Revising the heading of paragraph (a);

■ b. Adding paragraph (a)(1);

■ c. Revising paragraph (a)(2);

■ d. In paragraph (b), removing ''Section 0.459(a)(4) of the Commission's rules'' and adding ''§ 0.459(a)(4) of this chapter'' in its place; and

■ e. Adding paragraphs (d) and (e).

The revisions and additions read as follows:

**§ 43.82 Circuit capacity report.**

(a) *Submarine cable capacity.* * * *

(1) *Capacity holder report.* Each cable landing licensee and common carrier shall file a report showing its capacity on submarine cables landing in the United States as of December 31 of the preceding calendar year.

(2) *United States.* United States is defined in section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153.

* * * * *

(d) *Compliance.* Submission of false or inaccurate certifications or failure to file timely and complete annual circuit capacity reports in accordance with the Commission's rules in this chapter and the Filing Manual shall constitute grounds for enforcement action, including but not limited to a forfeiture or cancellation of the cable landing license or international section 214 authorization, pursuant to the Communications Act of 1934, as amended, and any other applicable law.

(e) *Sharing of circuit capacity reports with Federal agencies.* For purposes of the information collected under this subpart, the Commission may disclose to the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector, the Department of Homeland Security, and the Department of State any information submitted by an applicant, petitioner, licensee, or authorization holder under this subpart. Where such information has been submitted in confidence pursuant to § 0.457 or § 0.459 of this chapter, such information may be shared subject to the provisions of § 0.442 of this chapter and, notwithstanding the provisions of § 0.442(d)(1) of this chapter, notice will be provided at the time of disclosure.

[FR Doc. 2025–19658 Filed 10–24–25; 8:45 am]

BILLING CODE 6712–01–P

# Reader Aids

**Federal Register**

Vol. 90, No. 205

Monday, October 27, 2025

## 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

47229–47502 ..... 1
47503–47968 ..... 2
47969–48118 ..... 3
48119–48146 ..... 6
48147–48160 ..... 7
48161–48192 ..... 8
48193–48218 ..... 9
48219–48240 ..... 10
48241–48250 ..... 14
48251–48294 ..... 15
48295–48334 ..... 16
48335–48372 ..... 17
48373–48396 ..... 20
48397–48442 ..... 21
48443–48480 ..... 22
48481–48552 ..... 23
48553–48556 ..... 24
48557–48704 ..... 27

## 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.

### 3 CFR

**Proclamations:**
10976 ..... 48127
10977 ..... 48159
10978 ..... 48217
10979 ..... 48247
10980 ..... 48249
10981 ..... 48331
10982 ..... 48333
10984 ..... 48451
10985 ..... 48477
10986 ..... 48479
**Executive Orders:**
14353 ..... 48143
14354 ..... 48145
14355 ..... 48153
14356 ..... 48387
**Administrative Orders:**
September 30, 2025 ..... 47967
October 6, 2025 ..... 48167
Notices:
Notice of October 16, 2025 ..... 48391
Notice of October 16, 2025 ..... 48393
Notice of October 16, 2025 ..... 48395

### 5 CFR

**Proposed Rules:**
1650 ..... 48267

### 7 CFR

**Proposed Rules:**
905 ..... 47240
925 ..... 47243
930 ..... 47503
956 ..... 47245
984 ..... 47248

### 8 CFR

**Proposed Rules:**
106 ..... 48516
214 ..... 47507
215 ..... 48604
216 ..... 48516
235 ..... 48604

### 10 CFR

**Proposed Rules:**
821 ..... 48268

### 12 CFR

201 ..... 47512
204 ..... 47513
1002 ..... 47514
**Proposed Rules:**
Ch. XV ..... 47251
702 ..... 48409
791 ..... 48409
1209 ..... 47632
1239 ..... 47662
1241 ..... 47662
1261 ..... 47662
1273 ..... 47662
1277 ..... 47662
1281 ..... 47632
1282 ..... 47632

### 14 CFR

39 ..... 47523, 47526, 47530, 47532, 47536, 47538, 47540, 47544, 47546, 48219, 48251, 48254, 48256
97 ..... 47549, 47551
107 ..... 47969
**Proposed Rules:**
39 ..... 47251, 48414

### 15 CFR

744 ..... 48193

### 17 CFR

Ch. I ..... 47556
240 ..... 47552
242 ..... 47552
**Proposed Rules:**
229 ..... 47254
230 ..... 47254
239 ..... 47254
240 ..... 47254
249 ..... 47254

### 18 CFR

2 ..... 48397
5 ..... 48397
36 ..... 48397
131 ..... 48397
153 ..... 48221, 48397
156 ..... 48397
157 ..... 48221, 48397
287 ..... 48397
300 ..... 48397
366 ..... 48397
375 ..... 48397
385 ..... 48397
**Proposed Rules:**
2 ..... 48419
5 ..... 48419
36 ..... 48419
131 ..... 48419
153 ..... 48419
156 ..... 48419
157 ..... 48419
287 ..... 48419
300 ..... 48419
366 ..... 48419
375 ..... 48419
385 ..... 48419

### 19 CFR

12 ..... 47560

### 20 CFR

655 ..... 47914

**21 CFR**

73.....47229
1301.....47561
1308.....48259
1310.....47563
1311.....47566
**Proposed Rules:**
1308.....47663
1310.....47670

**24 CFR**

91.....48443
92.....48443

**26 CFR**

1.....47581
**Proposed Rules:**
1.....48422, 48481

**31 CFR**

Ch. V.....47230
562.....47229
587.....47230
1010.....48295
**Proposed Rules:**
Subtitle A.....47251
Subtitle B.....47251

**33 CFR**

1.....47583
3.....47583
67.....47583
72.....47583
80.....47583
100.....47583
107.....47583
110.....47583
117.....47232, 47583
141.....47583
147.....47583
151.....47583
153.....47583
162.....47583
165.....47234, 47583, 47588, 47589, 47590

**37 CFR**

6.....47592

**38 CFR**

17.....47595
**Proposed Rules:**
4.....47266

**39 CFR**

**Proposed Rules:**
3050.....48268

**40 CFR**

52.....47604, 47607, 47610, 47612, 47615
180.....47235
423.....47617
**Proposed Rules:**
51.....47677
52.....47686, 48481, 48502
63.....47268
81.....47686
84.....47999
423.....47693

**46 CFR**

4.....47583
42.....47583
401.....47583

**47 CFR**

0.....48648
1.....48648
43.....48648
**Proposed Rules:**
1.....48557

**49 CFR**

23.....47969
26.....47969
190.....47620
191.....47620
192.....47621, 47622, 47623, 47624, 47625, 47626
195.....47620, 47625, 47626, 47627
384.....47627
**Proposed Rules:**
40.....47286

**50 CFR**

600.....47982
622.....47628, 47982
635.....48200
648.....47989
660.....47629
679.....47631, 48147, 48241
**Proposed Rules:**
622.....47713
679.....47716

## 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 September 9, 2025**

## 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.