service, grant, or cooperative agreement with HUD, when necessary to accomplish an agency function related to a system of records. Disclosure requirements are limited to only those data elements considered relevant to accomplishing an agency function.

(10) To the National Archives and Records Administration, Office of Government Information Services (OGIS), to the extent necessary to fulfill its responsibilities in 5 U.S.C. 552(h), to review administrative agency policies, procedures and compliance with the Freedom of Information Act (FOIA), and to facilitate OGIS' offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies.

(11) To the U.S. Department of the Treasury when disclosure of the information is relevant to review payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state (meaning a state of the United States, the District of Columbia, a territory or possession of the United States, or a federally recognized Indian tribe) in a state-administered, federally funded program.

(12) To the U.S. Treasury for transactions such as disbursements of funds and related adjustments.

(13) To the IRS for reporting payments for goods and services and for reporting of discharge indebtedness.

In addition to the routine uses described above, HUD provides notice pursuant to 31 U.S.C. 3711(e) that information contained in this system of records may also be disclosed to a consumer reporting agency when trying to collect a claim owed on behalf of the government.

The disclosure is limited to information to establish the identity of the individual, including name, social security number, and address; the amount, status, history of the claim, and the agency or program under which the claim arose solely to allow the consumer reporting agency to prepare a credit report.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in paper and electronic format.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by Vendor Name, Vendor Number (*e.g.,* Employer Identification Number (EIN), Social Security Number (SSN), or Taxpayer Identification Number (TIN), UEI, Schedule Number, Voucher Number, and Contract Number.

POLICIES AND PRACTICIES FOR RENTENTION AND DISPOSAL OF RECORDS:

General Records Schedule 1:1; Financial Management and Reporting Records. This schedule covers records created by Federal agencies in carrying out the work of financial management.

Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

All HUD employees have undergone background investigations. HUD buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures. Access is restricted to authorized personnel or contractors whose responsibilities require access. System users must take the mandatory security awareness training annually as mandated by the Federal Information Security Modernization Act (FISMA). Users must also sign a Rules of Behavior form certifying that they agree to comply with the requirements before they are granted access to the system. LOCCS resides in the Microsoft Azure environment, a FedRAMP certified Infrastructure-as-a-Service (IaaS). The system is limited to those with a business need to know. LOCCS Authorizing Officials authorize LOCCS access for users, and OCFO ensures the user is eligible for access (*e.g.,* suitability, System Security Administrator approval), which allow for segregation of duties. OCFO limits access to records that contain PII on a need-to-know basis, user recertification is performed, audit logs are reviewed, security assessments are conducted, and background checks are completed prior to granting elevated access.

RECORD ACCESS PROCEDURES:

Individuals requesting records of themselves should address written inquiries to the Department of Housing Urban and Development 451 7th Street SW, Washington, DC 20410–0001. For verification, individuals should provide their full name, current address, and telephone number. In addition, the requester must provide either a notarized statement or an unsworn declaration made under 24 CFR 16.4.

CONTESTING RECORD PROCEDURES:

The HUD rule for contesting the content of any record pertaining to the individual by the individual concerned is published in 24 CFR 16.8 or may be obtained from the system manager.

NOTIFICATION PROCEDURES:

Individuals requesting notification of records of themselves should address written inquiries to the Department of Housing Urban Development, 451 7th Street SW, Washington, DC 20410–0001. For verification purposes, individuals should provide their full name, office or organization where assigned, if applicable, and current address and telephone number. In addition, the requester must provide either a notarized statement or an unsworn declaration made under 24 CFR 16.4.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

Docket No. FR–7092–N–13, 89 FR 5923, January 30, 2024, as modified by Docket No. FR–7106–N–12, 91 FR 2137, January 16, 2026.

Kimberly Morton,

Acting Chief Privacy Officer, Office of Administration.

[FR Doc. 2026–11611 Filed 6–9–26; 8:45 am]

BILLING CODE 4210–67–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7106–N–27]

Privacy Act of 1974; System of Records

AGENCY: Office of Chief Information Officer (OCIO), and Infrastructure and Operations (IOO), HUD.

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of Housing and Urban Development (HUD), Office of Chief Information Officer (OCIO), and Infrastructure and Operations (IOO), is issuing a public notice of its intent to establish a Privacy Act System of Records Notice (SORN) titled ''Sumo Logic.'' Sumo Logic serves as HUD's Security Information and Event Management (SIEM) tool, supporting centralized log collection, aggregation, and security monitoring. It collects system log data from HUD applications, infrastructure, security tools, and cloud platforms, and performs event correlation, custom searches, dashboard monitoring, scheduled reporting, and other standard security monitoring. This newly established system will be included in HUD's inventory of record systems.

DATES: Comments will be accepted on or before July 10, 2026. This proposed

action will be effective on the date following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number or by one of the following methods:

Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions provided on that site to submit comments electronically.

Fax: 202–619–8365.

Email: privacy@hud.gov.

Mail: Attention: Privacy Office; Kimberly Morton, Acting Chief Privacy Officer; The Executive Secretariat; 451 7th Street SW, Room 10139; Washington, DC 20410–0001.

Instructions: 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.

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

FOR FURTHER INFORMATION CONTACT: The Privacy Office, Kimberly Morton; 451 7th Street SW, Room 10139; Washington, DC 20410–0001; telephone number (804) 822–4801 (this is not a toll-free number). HUD welcomes and is prepared to receive calls from individuals who are deaf or hard of hearing, as well as individuals with speech or communication disabilities. To learn more about how to make an accessible telephone call, please visit *https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs.*

SUPPLEMENTARY INFORMATION: The Department of Housing and Urban Development (HUD), Office of Chief Information Officer (OCIO), maintains the ''Sumo Logic'' system of records. This system enhances enterprise-wide cybersecurity monitoring and incident response. By consolidating log data from HUD systems and platforms, Sumo Logic supports real-time threat detection, reporting and compliance with federal information security standards.

SYSTEM NAME AND NUMBER:

Sumo Logic, HUD/OCIO–05.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

HUD Headquarters, 451 7th Street SW, Washington, DC 20410–0001.

SYSTEM MANAGER(S):

Thomas Zeppa, Acting Director, Office of Chief Information Officer (OCIO), Cyber Security Operations Center, 451 7th Street SW, Washington, DC 20410–0001; Telephone (202) 227–5276.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Federal Information System Modernization Act of 2014 (FISMA), Public Law 113–283, 44 U.S.C. 3554; Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021); and OMB Memorandum 21–31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (August 27, 2021).

PURPOSE(S) OF THE SYSTEM:

Sumo Logic supports HUD's cybersecurity operations by enabling centralized system monitoring, threat detection, event correlation and incident investigation.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system covers federal employees, contractors, detail personnel, and other personnel who access, administrate, or use agency information systems. As well as individuals whose accounts, credentials, or devices interact with HUD networks, applications, or services, such as vendors, partners or members of the public.

CATEGORIES OF RECORDS IN THE SYSTEM:

Device identifiers, email addresses, full names, geolocation information, phone numbers, user IDs, and web uniform resource locator(s).

RECORD SOURCE CATEGORIES:

Amazon Web Services Cloud Computing, and Mainframe (IBM) systems.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

(1) To a congressional office from the record of an individual, in response to an inquiry from the congressional office made at the request of that individual.

(2) To contractors, grantees, experts, consultants, Federal agencies, and non-Federal entities, including, but not limited to, State and local governments and other research institutions or their parties, and entities and their agents with whom HUD has a contract, service agreement, grant, cooperative agreement, or other agreement, for the purposes of statistical analysis and research in support of program operations, management, performance monitoring, evaluation, risk management, and policy development, to otherwise support the Department's mission, for other research and statistical purposes not otherwise prohibited by law or regulation. Records under this routine use may not be used in whole or in part to make decisions that affect the rights, benefits, or privileges of specific individuals. The entity receiving information under this routine use may not further disclose the records in an identifiable form.

(3) To contractors, grantees, experts, consultants and their agents, or others performing or working under a contract, service, grant, cooperative agreement, or other agreement, with HUD, when necessary to accomplish an agency function related to this system of records. Disclosure requirements are limited to only those data elements considered relevant to accomplishing an agency function.

(4) To contractors, experts and consultants with whom HUD has a contract, service agreement, or other assignment of the Department, when necessary to utilize relevant data for the purpose of testing new technology and systems designed to enhance program operations and performance.

(5) To appropriate agencies, entities, and persons when: (1) HUD suspects or has confirmed that there has been a breach of the system of records; (2) HUD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, HUD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with HUD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(6) To another Federal agency or Federal entity, when HUD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

(7) To appropriate Federal, State, local, tribal, or governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where

HUD determines that the information would assist in the enforcement of civil or criminal laws and when such records, either alone or in conjunction with other information, indicate a violation or potential violation of law.

(8) To a court, magistrate, administrative tribunal, or arbitrator in the course of presenting evidence, including disclosures to opposing counsel or witnesses or jurors in the course of civil discovery, litigation, mediation, or settlement negotiations, or in connection with criminal law proceedings; when HUD determines that use of such records is relevant and necessary to the litigation and when any of the following is a party to the litigation or have an interest in such litigation: (1) HUD, or any component thereof; or (2) any HUD employee in his or her official capacity; or (3) any HUD employee in his or her individual capacity where HUD has agreed to represent the employee; or (4) the United States, or any agency thereof, where HUD determines that litigation is likely to affect HUD or any of its components.

(9) To any component of the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when HUD determines that the use of such records is relevant and necessary to the litigation and when any of the following is a party to the litigation or have an interest in such litigation: (1) HUD, or any component thereof; or (2) any HUD employee in his or her official capacity; or (3) any HUD employee in his or her individual capacity where the Department of Justice or agency conducting the litigation has agreed to represent the employee; or (4) the United States, or any agency thereof, where HUD determines that litigation is likely to affect HUD or any of its components.

(10) To the National Archives and Records Administration, Office of Government Information Services (OGIS), to the extent necessary to fulfill its responsibilities in 5 U.S.C. 552(h), to review administrative agency policies, procedures and compliance with the Freedom of Information Act (FOIA), and to facilitate OGIS' offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored electronically within the FedRAMP-authorized Sumo Logic Cloud SIEM platform.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records from this system may be retrieved by Full name, user IDs and email address.

POLICIES AND PRACTICIES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are managed in accordance with the General Records Schedule (GRS) 3.2, System Access Records, items 036, which covers Cybersecurity logging records. These records are temporary and can be destroyed when 30 months old, although longer retention is authorized for business use. Disposition Authority: DAA–GRS 2022–0005–0002.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

For Electronic Records: Records are maintained and stored in the Sumo Logic environment, which operates within HUD's infrastructure. Access is restricted based on the user's roles and system privileges. Records reside in an encrypted database, and the environment complies with security and privacy controls outlined in the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) Special Publications, and Federal; Information Processing Standards (FIPS). Access requires a valid HSPD–12 ID credential, connection to HUD's Local Area Network (LAN), a valid User ID, Password and Personalized Identification Number (PIN). Records are accessible only to individuals who require access to perform official duties.

For Electronic Records (cloud based): Records are secured and maintained on a cloud-based server and operating system hosted in a Federal Risk and Authorization Management Program (FedRAMP) authorized, and FISMA Moderate environment. All data is protected by firewalls and encrypted both at rest and in transit, in accordance with HUD encryption standards.

RECORD ACCESS PROCEDURES:

Individuals seeking to determine whether this System of Records contains information on themselves should address written inquiries to the Department of Housing and Urban Development 451 7th Street SW, Washington, DC 20410–0001.

For verification, individuals should provide their full name, current address, and telephone number. In addition, the requester must provide either a notarized statement or an unsworn declaration made under 24 CFR 16.4.

CONTESTING RECORD PROCEDURES:

The HUD rule for accessing, contesting, and appealing agency determinations by the individual concerned are published in 24 CFR part 16.8 or may be obtained from the system manager.

NOTIFICATION PROCEDURES:

Individuals requesting notification of records of themselves should address written inquiries to the Department of Housing and Urban Development, 451 7th Street SW, Washington, DC 20410–0001. For verification purposes, individuals should provide their full name, office or organization where assigned, if applicable, and current address and telephone number. In addition, the requester must provide either a notarized statement, or an unsworn declaration made under 24 CFR 16.4.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Kimberly Morton,

Acting Chief Privacy Officer, Office of Administration.

[FR Doc. 2026–11613 Filed 6–9–26; 8:45 am]

BILLING CODE 4210–67–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

[Docket No. FWS–R7–ES–2025–0506; FXES111607MRG01–267–FF07CAMM00]

Marine Mammals; Proposed Incidental Harassment Authorization for the Southern Beaufort Sea Stock of Polar Bears in the Prudhoe Bay Area of the North Slope Borough, Alaska; Draft Environmental Assessment

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of receipt of application; notice of availability of proposed authorization and draft environmental assessment; request for comments.

SUMMARY: We, the U.S. Fish and Wildlife Service, in response to a request under the Marine Mammal Protection Act of 1972, as amended, from BP America Production Company and BP Remediation Management (collectively BP), propose to authorize nonlethal, incidental take by harassment of small numbers Southern Beaufort Sea (SBS) polar bears (*Ursus maritimus*) between June 1, 2026, and May 31, 2027. The applicant requested this authorization for take by harassment that may result from activities associated with drone site surveys, surface water monitoring, removal of