Dated: July 17, 2025.

Bruce A. George,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2025–13669 Filed 7–18–25; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Center for Scientific Review; Notice of Closed Meetings

Pursuant to section 1009 of the Federal Advisory Committee Act, as amended, notice is hereby given of the following meetings.

The meetings will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: Center for Scientific Review Special Emphasis Panel; Career Development Review in Alzheimer's Disease and Related Dementias.

Date: August 19, 2025.

Time: 9:00 a.m. to 6:00 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Kristin L McNally, Ph.D., Scientific Review Officer, Scientific Review Program, Immunology Review Branch, National Institutes of Health, Hamilton, MT 59840, *mcnallyk@niaid.nih.gov.*

Name of Committee: Center for Scientific Review Special Emphasis Panel; Collaborative Applications: Review of Complex Integrated Multi-Component Projects in Aging Research.

Date: August 20–21, 2025.

Time: 10:00 a.m. to 6:00 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Bo-Shiun Chen, Ph.D., Scientific Review Officer, Scientific Review Branch, NINDS/NIH NCS, 6001 Executive Blvd., Suite 3208, NCS 9529, Bethesda, MD 20892, (301) 496–9223, *bo-shiun.chen@nih.gov.*

(Catalogue of Federal Domestic Assistance Program Nos. 93.306, Comparative Medicine; 93.333, Clinical Research, 93.306, 93.333, 93.337, 93.393–93.396, 93.837–93.844, 93.846–93.878, 93.892, 93.893, National Institutes of Health, HHS)

Dated: July 16, 2025.

Bruce A. George,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2025–13584 Filed 7–18–25; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Center for Scientific Review; Amended Notice of Meeting

Notice is hereby given of a change in the meeting of the Center for Scientific Review Special Emphasis Panel, Cellular and Molecular Aspects of the Blood-Brain Barrier and Neurovascular System and Therapeutic Strategies, August 07, 2025, 09:00 a.m. to August 07, 2025, 05:30 p.m., National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD, 20892 which was published in the **Federal Register** on July 02, 2025, 90 FR 29030, Doc.2025–12382

This meeting is being amended to change the contact person from Eric Tucker to Jacek Topczewski, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, Bethesda, MD 20892, *topczewskij2@csr.nih.gov.* The meeting is closed to the public.

Dated: July 16, 2025.

Bruce A. George,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2025–13585 Filed 7–18–25; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2025–0097]

Notification of the Removal of Conditions of Entry on Vessels Arriving From the Republic of Djibouti

AGENCY: Coast Guard, DHS.

ACTION: Notice.

SUMMARY: The Coast Guard announces that it is removing the conditions of entry on vessels arriving from the Republic of Djibouti.

DATES: The policy announced in this notice is effective on July 21, 2025.

FOR FURTHER INFORMATION CONTACT: For information about this document call or email J.J. Hudson, Chief, Office of International and Domestic Port Security, United States Coast Guard, telephone 571–607–6445, *Juliet.J.Hudson@uscg.mil.*

SUPPLEMENTARY INFORMATION:

Background and Purpose

The authority for this notice is 5 U.S.C. 552(a) (''Administrative Procedure Act''), 46 U.S.C. 70110 (''Maritime Transportation Security Act''), and Department of Homeland Security Delegation No. 0170.1(II)(97.f). As delegated, section 70110(a) authorizes the Coast Guard to impose conditions of entry on vessels arriving in U.S. waters from ports that the Coast Guard has not found to maintain effective anti-terrorism measures.

In 2019, the Coast Guard determined that effective anti-terrorism measures were not in place in the ports of Djibouti. Accordingly, conditions of entry were imposed on vessels arriving from Djibouti. Based on recent assessments, the Coast Guard has determined that Djibouti is maintaining effective anti-terrorism measures, and is, accordingly, removing the conditions of entry announced in previously published Notices. With this notice, the current list of countries assessed and not maintaining effective anti-terrorism measures is as follows: *Cambodia, Cameroon, Comoros, Cuba, Equatorial Guinea, Federated States of Micronesia, The Gambia, Guinea-Bissau, Iran, Iraq, Libya, Madagascar, Nauru, Nigeria, Sao Tome and Principe, Seychelles, Sudan, Syria, Timor-Leste, Venezuela, Yemen.* The current Port Security Advisory is available at: *http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/International-Domestic-Port-Assessment/.*

Thomas G. Allan Jr.,

Vice Admiral, USCG, Acting Deputy Commandant for Operations.

[FR Doc. 2025–13656 Filed 7–18–25; 8:45 am]

BILLING CODE P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. ICEB–2023–0014]

Privacy Act of 1974; System of Records

AGENCY: U.S. Immigration and Customs Enforcement, Department of Homeland Security.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a DHS system of records titled, ''DHS/U.S. Immigration and Customs Enforcement (ICE)–006 ICE Intelligence Records Systems (IIRS).'' The IIRS system of records incorporates ICE systems that contain raw intelligence and intelligence products collected to support its law enforcement intelligence, counterterrorism, and homeland security mission. DHS/ICE is modifying this system of records notice (SORN) to: document the decommissioning of two technology systems and reflect the information collected and maintained by DHS/ICE program offices in accordance with their respective missions; update and clarify the categories of individuals; update the categories of records; and update routine uses. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This modified system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before August 20, 2025. This modified system will be effective upon publication. New or modified routine uses will be effective August 20, 2025.

ADDRESSES: You may submit comments, identified by docket number ICEB–2023–0014 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* (202) 343–4010.
- *Mail:* Roman Jankowski, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528–0655.

Instructions: All submissions received must include the agency name and docket number ICEB–2023–0014. 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: For general questions, please contact: *ICEPrivacy@dhs.gov,* U.S. Immigration and Customs Enforcement, 500 12th Street SW, Washington, DC 20356. For privacy questions, please contact: Roman Jankowski, *Privacy@hq.dhs.gov,* Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528–0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS)/U.S. Immigration and Customs Enforcement (ICE) proposes to modify and reissue a current DHS system of records titled, ''DHS/ICE–006 ICE Intelligence Records Systems (IIRS) System of Records.'' IIRS contains information collected to support DHS/ICE's law enforcement intelligence, counterterrorism, and homeland security mission. This information includes raw intelligence collected by DHS/ICE's Homeland Security Investigations (HSI) Office of Intelligence (INTEL), public source information, and information initially collected by ICE pursuant to its immigration and enforcement authorities, which is then analyzed and incorporated into law enforcement intelligence products.

ICE systems whose records are covered by IIRS allow ICE to manage intelligence requirements and leverage intelligence capabilities and to conduct sophisticated and complex analysis of criminals and their networks in support of HSI investigations and investigative priorities, classified communications program, and emergency management and continuity functions. Furthermore, the systems allow ICE to produce timely, comprehensive, and accurate analysis that enables criminal investigators to identify, prioritize, disrupt, and dismantle transnational terrorist and criminal networks and identify any other individual or organization that threatens national security or seeks to exploit the customs and immigration laws of the United States.

As part of the intelligence process, ICE investigators and analysts must review large amounts of data to identify and understand relationships between individuals, entities, threats, and events to generate law enforcement intelligence products that provide ICE operational units with actionable information for law enforcement, intelligence, and other homeland security purposes. To automate and expedite this process, ICE uses several information technology systems, tools, and applications to allow for the efficient research and analysis of data from a variety of sources.

DHS/ICE is updating this system of records notice to document the decommissioning of two ICE technology systems, (1) ICE Gangs and (2) the Intelligence Fusion System (IFS). Both have been decommissioned in an effort to consolidate the various analytical interface applications within ICE. DHS/ICE is also updating the IIRS System of Records Notice to clarify the categories of individuals covered under this system of records to include informants associated with immigration investigations, law enforcement investigations, and other activities conducted by ICE and individuals who have made credible threats against ICE personnel or facilities; and updating the categories of records collected to include social media and location-related data.

Finally, ICE/DHS is updating, adding to, and consolidating the following routine uses within the IIRS System of Records Notice:

- Routine Uses A through I are being updated to be consistent with DHS standard routine uses and all other routine uses have been re-lettered accordingly.
- Routine Use B has been moved to Routine Use J.
- Routine Use E has been modified and Routine Use F has been added to conform to Office of Management and Budget (OMB) Memorandum M–17–12 ''Preparing for and Responding to a Breach of Personally Identifiable Information,'' (Jan. 3, 2017).
- Routine Use G is being added as a DHS standard routine use that covers law enforcement referrals. This routine use requires that a record, either on its face or in conjunction with other information, indicates a violation or potential violation of the law.
- Routine Use M and N have been consolidated and re-lettered to Routine Use P.
- Routine Use U is being updated to be consistent with the DHS standard routine use for technology and is now Routine Use W. This modification eliminates the need for one routine use previously identified as Routine Use V. That routine use has been removed.
- Routine Use Y has been added to permit the sharing of information related to actual or prospective claims filed against DHS.

Non-substantive language changes have been made to additional routine uses to clarify disclosure policies that are standard across DHS and to align with previously published DHS system of records notices.

Consistent with the DHS information sharing mission, information maintained in the DHS/ICE–006 IIRS System of Records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, ICE may share information with appropriate federal, state, local,

tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in the **Federal Register**. This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The fair information practice principles found in the Privacy Act underpin the statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate personally identifiable information. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents.

Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the Judicial Redress Act, along with judicial review for denials of such requests. In addition, the Judicial Redress Act prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act. Under the Judicial Redress Act, a ''covered person'' means a natural person (other than an ''individual'' as defined under the Privacy Act) who is a citizen of a covered country.

Below is the description of the DHS/ICE–006 Intelligence Records System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER:

Department of Homeland Security (DHS)/U.S. Immigration and Customs Enforcement (ICE)–006 ICE Intelligence Records System (IIRS).

SECURITY CLASSIFICATION:

Sensitive But Unclassified, Classified.

SYSTEM LOCATION:

Records are maintained at ICE Headquarters in Washington, DC, ICE fields offices, or designated cloud computing environments.

SYSTEM MANAGER(S):

Deputy Assistant Director, Homeland Security Investigations Cyber and Operational Technology Division, 202–732–5200, 500 12th Street SW, Washington, DC 20536.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

8 U.S.C. secs. 1103, 1105, 1225(d)(3), 1324(b)(3), 1357(a), and 1360(b); 19 U.S.C. secs. 1 and 1509.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is:

(a) To support ICE's collection, analysis, reporting, and distribution of criminal and civil law enforcement, immigration administration, terrorism, intelligence, and homeland security information in support of ICE's law enforcement and immigration administration mission;

(b) To produce criminal and civil law enforcement analysis and intelligence reporting that provides actionable information to ICE's law enforcement and immigration administration personnel and to other appropriate government agencies;

(c) To enhance the efficiency and effectiveness of the research and analysis process for DHS law enforcement, immigration, and intelligence personnel through information technology tools that provide for advanced search and analysis of various datasets, including commercial data and open sources;

(d) To facilitate multi-jurisdictional informational exchange between ICE and other law enforcement agencies regarding known and suspected members of transnational organized crime and associates; and

(e) To identify potential criminal activity, immigration violations; threats to homeland security, ICE personnel, and ICE facilities; to uphold and enforce the law; and to ensure public safety.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include the following:

(1) Individuals (*e.g.,* subjects, victims, witnesses, associates, informants) associated with current or previous immigration and law enforcement investigations and other activities conducted by ICE;

(2) Individuals associated with law enforcement investigations or activities conducted by other federal, state, tribal, territorial, local, or foreign agencies where there is a potential nexus to ICE's law enforcement and immigration enforcement responsibilities or homeland security in general;

(3) Individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism;

(4) Individuals involved in, associated with, or who have reported suspicious activities, threats, or other incidents reported by domestic and foreign government agencies, multinational or non-governmental organizations, critical infrastructure owners and operators, private sector entities and organizations, and individuals;

(5) Individuals who are the subjects of, or otherwise identified in, classified or unclassified intelligence reporting received or reviewed by ICE;

(6) Individuals who are known or suspected gang members or associates;

(7) Individuals not implicated in activities in violation of laws enforced or administered by ICE, but with pertinent knowledge of some circumstance of a case or record subject. Such records may contain any information, including personal identification data, that may assist ICE in discharging its responsibilities generally (*e.g.,* information which may assist in identifying and locating such individuals);

(8) Individuals identified in law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies;

(9) Individuals identified in U.S. visa, border, immigration, and naturalization benefit data, including arrival and departure data;

(10) Individuals identified in DHS law enforcement and immigration records;

(11) Individuals whose passports have been lost or stolen;

(12) Individuals identified in public news reports that may be pertinent to the ICE mission; and

(13) Individuals who have made credible threats against ICE personnel or facilities.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system may include:

- Biographic information (*e.g.,* name, date of birth, Social Security number, A-Number, citizenship/immigration status, passport information, addresses, phone numbers);
- Records of immigration enforcement activities or law enforcement investigations and activities conducted by ICE;
- Information (including documents and electronic data) collected by DHS from or about individuals during investigative activities and border searches;
- Records of immigration enforcement activities and law

enforcement investigations/activities that have a possible nexus to ICE's law enforcement and immigration enforcement responsibilities or homeland security in general;

- Law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies;
- U.S. visa, border, immigration, and naturalization benefit data, including arrival and departure data;
- Terrorist watchlist information compiled by DHS and other terrorism related information regarding threats, activities, and incidents;
- Watchlist information compiled by DHS regarding individuals associated with Transnational Organized Crime and other related criminal threats, activities, and incidents.
- Lost and stolen passport data;
- Records pertaining to known or suspected terrorists, terrorist incidents, activities, groups, and threats;
- ICE-generated intelligence requirements, analysis, reporting, and briefings;
- Third party intelligence reporting, such as information from investigative and intelligence reports prepared by law enforcement agencies and agencies of the U.S. intelligence community;
- Articles, public-source data, and other published information on individuals and events of interest to ICE, including social media account information and social media posts, internet protocol addresses, and usernames;
- Records and information from government data systems or retrieved from commercial data providers in the course of intelligence research, analysis, and reporting;
- Reports of suspicious activities, threats, or other incidents generated by ICE and third parties;
- Additional information about known and suspected transnational organized crime actors and associates such as, gang affiliation, physical description, photos of the individual, field interview notes, and criminal history information;
- Audio and video records retained in support of ICE's law enforcement, national security, or other homeland security missions;
- Additional information about confidential sources or informants;
- Metadata, which may include but is not limited to transaction date, time, location, and frequency;
- Biometric information, including facial images, iris images, and fingerprints; and
- Location-Related Records, including geotags from metadata associated with other record categories collected; geolocation information derived from authorized law enforcement activities, ICE-owned devices, witness accounts, or commercially available data; location tracking tools that maintain a list of tracking devices or personal mobile devices by serial number/Mobile Directory Number (MDN)/International Mobile Equipment Identity (IMEI)/Mobile Equipment ID (MEID)/AD_ID number, and their current locations using Global Positioning System (GPS) and/or assisted Cellular Tower coordinates. These location tracking tools are not only deployed on targets of investigations, vehicles of interest in investigations, contraband, but also on the official vehicles owned by ICE and used by agents and officers in the field, and geographic areas of interest related to criminal and intelligence investigations and activities.

RECORD SOURCE CATEGORIES:

Records are obtained from federal, state, local, territorial, tribal, or other domestic agencies, foreign agencies, multinational or non-governmental organizations, critical infrastructure owners and operators, private sector entities and organizations, individuals, commercial data providers, and public sources such as news media outlets and the internet.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agencies conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant and necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his/her official capacity;
3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (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 DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

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

G. To an appropriate federal, state, tribal, local, territorial, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided

information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To the Department of Justice (DOJ), Civil Rights Division, for the purpose of responding to matters within the DOJ's jurisdiction to include allegations of fraud and/or nationality discrimination.

J. To a federal, state, tribal, local, territorial, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) to assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) to verify the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) to verify the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

K. To a former employee of DHS, in accordance with applicable regulations, for purposes of responding to an official inquiry by a federal, state, local, tribal, territorial, government entity, or professional licensing authority; or facilitating communications with a former employee that may be relevant and necessary for personnel-related or other official purposes where the Department requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

L. To an appropriate federal, state, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to the agency's decision concerning the hiring or retention of an individual or the issuance, grant, renewal, suspension or revocation of a security clearance, license, contract, grant, or other benefit; or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person receiving the information.

M. To appropriate federal, state, local, tribal, territorial, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health risk.

N. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

O. To appropriate federal, state, tribal, local, territorial, or foreign government agencies or organizations, international organizations, or multilateral governmental organizations lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, rules, regulations, orders, license, or treaty where DHS determines that the information will enable these entities to carry out their law enforcement responsibilities.

P. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided that disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

Q. To federal, state, local, tribal, or territorial government agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide national security, intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

R. To federal and foreign government intelligence or counterterrorism agencies where DHS becomes aware of an indication of a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, or when such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

S. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent that the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

T. To international, foreign, intergovernmental, and multinational agencies, authorities, and organizations in accordance with law and formal or informal international agreements or arrangements.

U. To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements, or when the Department of State requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about an enforcement operation with transnational implications.

V. To appropriate federal, state, local, tribal, territorial, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to utilize relevant data for purposes of developing, implementing, and testing new software and technologies for the purpose of data sharing to enhance and support homeland security, national security, or law enforcement.

W. To federal, state, local, territorial, tribal, international, or foreign criminal, civil, or regulatory law enforcement authority where the information is necessary for collaboration, coordination and deconfliction of law enforcement investigative matters and prosecutions to avoid duplicative or disruptive efforts and for the safety of law enforcement officers who may be working on related law enforcement investigations and law enforcement intelligence matters.

X. To prospective claimants and their attorneys for the purpose of negotiating the settlement of an actual or prospective claim against DHS or its current or former employees, in advance of the initiation of formal litigation or proceedings.

Y. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent that the Chief Privacy Officer determines that release of the specific information in the

context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

DHS/ICE records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD–ROM.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

DHS/ICE may retrieve records by personal identifiers such as, but not limited to, name, A-Number, phone number, address, Social Security number, or passport number. Records may also be retrieved by non-personal information such as transaction date, entity/institution name, description of goods, value of transactions, and other information.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Intelligence information reports (IIR) will be retained for 22 years after cutoff in accordance with ICE records schedule DAA–0567–2016–0003–0007. Other intelligence records will be retained in accordance with their corresponding disposition within ICE record schedule DAA–0567–2016–0003, to include finished intelligence products (permanent records) and reports and analysis (destroyed 22 years at cut off at end of fiscal year). Records associated with an investigative case file will be retained for 20 years in accordance with legacy customs schedule N1–36–86–1–161.3 (inv 7B), with the exception of N1–36–86–1/162.38, Neutrality Investigative Files, which are permanent records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DHS/ICE safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/ICE has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable, because it is a law enforcement system. However, ICE will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and ICE FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia.* If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, DC 20528–0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, *http://www.dhs.gov/foia* or (866) 431–0486. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered Judicial Redress Act records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES:

See ''Record Access Procedures'' above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2) of the Privacy Act, has exempted this system from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a (k)(1) and (k)(2), has exempted from this system the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

HISTORY:

75 FR 9233 (March 1, 2010); 73 FR 74735 (December 9, 2008).

* * * * *

Roman Jankowski,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2025–13613 Filed 7–18–25; 8:45 am]

BILLING CODE 9111–28–P