DEPARTMENT OF HOMELAND SECURITY

[Docket No. ICEB-2024-0013]

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 current DHS system of records titled, "DHS/U.S. Immigration and Customs Enforcement (ICE)-008 Search, Arrest, and Seizure Records (SAS)." ICE collects and maintains information in the SAS in order to document searches of individuals and property, arrests of individuals, and detentions and seizures of property and goods pursuant to ICE law enforcement authorities. ICE is updating this system of records notice to modify the purpose of the system; modify existing, and add new, categories of individuals; modify and update the categories of records; and update, modify, and remove routine uses. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. All exemptions listed for this system in the existing system of records notice will continue to be applicable for this updated notice, as currently implemented in 6 C.F.R. Part 5, Appendix C. This updated system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. New or modified routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number ICEB-2024-0013 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, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number ICEB-2024-0013. 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: U.S. Immigration and Customs Enforcement (ICE), 500 12th Street SW, Mail Stop 5004, Washington, D.C. 20536. For privacy questions, please contact: Roman Jankowski, Privacy@hq.dhs.gov, Chief Privacy Officer, Department of Homeland Security, Washington, D.C. 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 notice (SORN) titled, "DHS/ICE-008 Search, Arrest, and Seizure Records (SAS)." SAS systems maintain records regarding searches of individuals and property, arrests of individuals, and detentions and seizures of property and goods in support of the ICE statutory law enforcement, immigration, counterterrorism, and homeland security missions. This information

consists of audio and video data, including Body Worn Camera (BWC) footage, recorded during the search, seizure, or arrest of a person or goods in furtherance of ICE law enforcement actions. These actions include investigations of potential criminal activity and threats to national security; enforcing immigration and customs laws; and upholding and enforcing the law and ensuring public safety.

The system of records notice's scope includes advanced technological methods employed by ICE during searches and seizures which includes ICE's use of new and emerging information technology (IT). The term IT includes computers; support equipment (including imaging devices, input, output, and storage devices necessary for security and surveillance); equipment designed to be controlled by the central processing unit of a computer; software; firmware and similar procedures; services (including support services); and related resources. ICE employs IT to improve law enforcement search, arrest, and seizure efficacy to better counter the methods of increasingly sophisticated criminal actors. Information on law enforcement personnel who have created the records or participated in a search, arrest, and seizure is also shared with systems supported by the SAS System of Records Notice.[1]

The purpose of this system remains to document all information and activity related to ICE searches of individuals and property, arrests of individuals, and seizures of goods, as well as related information about the individuals or entities suspected of violations of laws and regulations enforced by ICE. The system is also intended to facilitate communication between ICE and foreign and domestic law enforcement agencies for the purpose of enforcement and administration of laws, including immigration and customs laws. A supplemental purpose is to increase agency transparency to the public regarding interactions between ICE and the populace by

[1] Such systems include the following: Telecommunications Linking (TLS) System, Title III Tracking, Body Worn Camera (BWC) System, ICE Case Management (ICM) System, and Repository for Analytics in a Virtualized Environment (RAVEN).

documenting ICE law enforcement actions, such as through the use of BWCs; this increased transparency will lead to greater accountability by the agency.

The following list includes the full explanation of changes to this system of records notice:

(1) The purpose of the system has been modified to include the documentation of enforcement actions between ICE and the public via video and audio recording. This includes audio and video documentation for which express consent is not required (e.g., via a body worn camera in public view with no reasonable expectation of privacy). The purpose of the audio and video recording of interactions with the public is to improve policing practices and build community trust and legitimacy. ICE interactions that may be recorded include, but are not limited to, interactions arising out of:

- At-large arrests, including searches incident(al) to that arrest;
- Search, arrest, and seizure related detentions, however brief, including frisks conducted during the detentions;
- Execution of, and attempting execution, criminal and administrative arrest warrants;
- Execution of search warrants, including during the time securing the location to be searched as well as the ultimate search of the locations; and
- Questioning of any individual encountered during the above-listed activities in the field.

(2) The categories of individuals have been updated to include individuals with knowledge of the alleged activity, witnesses, and witness bystanders; as well as victims, detainees, and other individuals (minors and non-minors) whose images and audio are captured incidentally by search, arrest, or seizure activity through the use of recording devices such as body worn cameras, security camera footage,

and bystander smart phone or other mobile device. It must be noted that only individuals are covered by this notice for those recordings where ICE retrieves information by a personal identifier in their normal course of business.

(3) The categories of records have been modified to include biometric information, geolocation data records, open-source social media tool use data records, commercial data, records derived from advances in IT hardware/software, advances in currency/financial information (e.g., cryptocurrency), and video/audio that may be obtained during a search, arrest, or seizure.

(4) ICE is modifying Routine Uses A through I to conform to DHS guidance. ICE is also adding routine uses K, O, P, and re-lettering several routine uses to account for the newly added routine uses. Below is a summary of those routine uses and their corresponding letter.

Routine Use A is being updated to include disclosures before "any court, adjudicative or administrative body when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:"

Routine Use E is being modified and a new 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 K is being added to allow DHS to exchange relevant data in furtherance of coordinating and collaborating with other organizations for the purpose of developing, testing and/or implementing new software or technology solutions which have a purpose that is related to the purpose of this system of records;

Routine Use O is being added to permit sharing of identifying information with federal, state, local, tribal, territorial, international, or foreign government agencies or

entities for the purpose of consulting with those agencies or entities for purposes of assisting with an individual's request for redress;

Routine Use P is being added to clarify the disclosure to the Department of State, "when it 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 alien or an enforcement operation with transnational implications;"

Additionally, this notice includes non-substantive changes to simplify formatting and text of the previously published notice.

Consistent with DHS's information sharing mission, information stored in the DHS/ICE-008 Search, Arrest, and Seizure 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.

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 individuals' records. 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" refers to a natural person who is a citizen of a covered country.

Below is the description of the DHS/ICE-008 Search, Arrest, and Seizure System of Records.

In accordance with 5 U.S.C. sec. 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)-008 Search, Arrest, and Seizure Records.

SECURITY CLASSIFICATION: Unclassified, Law Enforcement Sensitive.

SYSTEM LOCATION: Records are maintained at the U.S. Immigration and Customs Enforcement Headquarters in Washington D.C. and field offices, or designated cloud computing environments. Records are maintained in such systems as the following: Telecommunications Linking (TLS) System, Title III Tracking, Body Worn Camera (BWC) System, ICE Case Management (ICM) System, and Repository for Analytics in a Virtualized Environment (RAVEN).

SYSTEM MANAGER(S): Deputy Assistant Director, Homeland Security Investigations Cyber and Operational Technology Division, 202-732-5200, 500 12th Street, SW, Washington, D.C. 20536.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 6 U.S.C. 202-203; 8 U.S.C. 1357; 18 U.S.C. 554; 8 U.S.C. 2518; 19 U.S.C. 66; 19 U.S.C. 1431; 19 U.S.C. 1509; 19 U.S.C. 1603; 19 U.S.C. 2072; 21 U.S.C. 967; 22 U.S.C. 2778; other applicable authorities from Title 18, United States Code; and Title 19, United States Code as

delegated by the Secretary of Homeland Security under his or her authority granted by the Homeland Security Act of 2002 (Pub. L. 107-296); 31 CFR part 103; 19 U.S.C. secs. 66, 1618, 1625; 19 U.S.C. sec. 19 CFR Parts 171 and 172.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to:

(1) Document relevant information and activity related to ICE searches of individuals and property; arrests of individuals; seizures of goods, property, and non-physical property (data, bank accounts); as well as related information about the individuals or entities suspected of violations of laws and regulations enforced by ICE.

(2) Collect video/audio documentation of interactions:

- (i) Between ICE and partner law enforcement and the public in furtherance of an active search, arrest, and seizure;
- (ii) Between ICE and individuals who are aliens or foreign nationals encountered near/on the United States border; and
- (iii) During significant public events requiring ICE's involvement to ensure documentation of a search, arrest, or seizure so long as the sole purpose is not to record individuals who are engaged in activity protected by the First Amendment.

(3) Facilitate communication between ICE and foreign and domestic law enforcement agencies for the purpose of enforcement and administration of laws, including immigration and customs laws.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by this system include:

(1) Individuals who violated, or are believed to have violated, the laws and regulations enforced by ICE or partner law enforcement agencies, including those who have been administratively or criminally charged with violations of such laws and regulations;

(2) Individuals related to arrested individuals, including guardians or custodians of minors, sponsors, or hosts of individuals who are dependent guests or visitors;

(3) Individuals who are witnesses, and individuals who may have knowledge of alleged illegal activity (e.g., victims, associates) related to a search, arrest, and/or seizure;

(4) Individuals who may be recorded incidentally by video or audio during a search, arrest, and/or seizure;

(5) Owners, claimants, and other interested parties relating to detained seized, seized and/or forfeited goods and property;

(6) Law enforcement personnel (e.g., ICE personnel, foreign and domestic law enforcement partners, and task force participants) or other assigned government personnel both directly involved in law enforcement duties and encountered incidental to enforcement duties.

CATEGORIES OF RECORDS IN THE SYSTEM: Categories of records in this system may include:

Information about individuals:

- Name;
- Nationality;
- Aliases;
- Social Security number;
- A-Number;
- Citizenship;
- Date and place of birth;
- Physical description of individual;
- Addresses;
- Telephone numbers;
- Occupation;

- Place of business;
- Driver's license number and other license information for owners and operators of vehicles, aircraft, and vessels;
- Other biographical information;
- Passport and visa information;
- Criminal history;
- Immigration status and history;
- Employment history;
- Business information, including occupation and place of business;
- Information related to the individual's entry into and exit from the United States;
- Suspicious financial activity, currency transaction reports, and currency or monetary instrument reports;
- Biometric information (i.e., fingerprints, voiceprints or voice audio recognition, iris images, photographs, DNA samples, and any unique numerical identifiers assigned to biometrics for administrative purposes) collected as a result of a search or arrest. DNA samples are collected and sent to the FBI. DNA samples are not retained or analyzed by ICE; and
- Information pertaining to ICE's collection of DNA samples, limited to the date and time of a successful collection and confirmation from the FBI that the sample was able to be sequenced. ICE does not receive or maintain the results of the FBI's DNA analysis (i.e., DNA sequences).

Information about the search, seizure, or detention of goods or property, or the search or arrest of individuals:

- Search/arrest/seizure/detention:
    - Date;
    - Arrest location (public or non-public), including location of safehouse.

- License and registration number of vehicles, aircraft, vessels, merchandise, goods, and other assets;
- License plate vehicle tag number and registration information, including image of license plate characters and associated temporal and location information;
- Individual and/or contraband's mode of entry (e.g., marine vessel), including a description of entry points(s);
- Photographs related to searches, detentions, seizures, or arrests including those captured incidentally by search, arrest, and seizure activity;
- Search, arrest, and seizure audio and or video footage/recordings, overt or covert, of ICE and partner law enforcement encounters, searches, seizures, stops, arrests, or other interactions (i.e., between ICE personnel and the public) including those captured incidentally by search, arrest, and seizure activity from a device mounted on a:
    - Mobile object, including a mobile vehicle or vessel (e.g., uncrewed aerial vehicles (UAS or sUAS); submersible vessels; land vehicles);
    - Stationary object; and
    - Individual, including
        - Law enforcement personnel (e.g., BWC footage); and
        - Citizen witnesses recording a law enforcement encounter(s) with the public (e.g., on a mobile device);
    - Forms that are part of the search arrest seizure process (e.g., declaration forms submitted to U.S. Customs and Border Protection (CBP));
- Receipts of:
    - Cash, currency (e.g., crypto currency) or banking records; and
    - Goods, or other property seized, detained, or forfeited;
- Description of goods or other property seized, detained, searched, or forfeited;

- Estimated foreign value of seized goods or other property;
- Duty paid and owed;
- Domestic value of seized goods or other property;
- Notices provided to owners, claimants, or other interested parties pertaining to seized goods or other property;
- Reports of arrests, searches, detentions, and seizures by ICE including the circumstances of the seizure, including reports from other law enforcement agencies;
- Section of law violated;
- Warrant number;
- Location tracking related data (e.g., geolocation coordinates, Global Positioning System (GPS) use, and cell tower coordinates);
- Information, including that which is received from other governmental agencies, confidential sources, and other sources pertaining to search, arrest, and seizure activity, as well as search, arrest, and seizure referrals from other agencies, tips, and other leads pertaining to potential violations of U.S. customs and immigration law, as well as other laws and regulations within ICE's jurisdiction; and
- Information about other law enforcement personnel (e.g., other Federal governmental and State and Local agencies) involved in an enforcement action, including: name, badge number, and station location.

Any other evidence in any form collected during the course of a search, arrest, or seizure or contained within documents relating to such an action, including:

- Papers, photographs, video, electronic recordings, electronic data, digital, virtual, non-fungible, or video records that was obtained, seized, or otherwise lawfully acquired from any source during the course of a search, arrest, seizure, to the

extent relevant and necessary for the performance of ICE's statutory enforcement authorities. This includes footage created from ICE's use of body-worn cameras.

- Seized or detained records in both paper and electronic form, including computers, computer records, disks, hard drives, flash drives and other electronic media and storage devices;
- Digital evidence including cyber forensics (e.g., computer code which could reveal a nation-state's or cyber criminal's signature);
- Internet protocol (IP) address, name, and uniform resource locator (URL), including those of website(s) seized; and
- Metadata (data about data) which may include geolocation data, device unique identifier, video clip unique identifier, video clip file name, and video category tags.

RECORD SOURCE CATEGORIES: Records are obtained from individuals who have been subject to search or arrest; owners, claimants, and other interested parties of detained, seized, and/or forfeited property; ICE personnel and ICE IT systems described in Privacy Impact Assessments which are wholly or partially covered by the SAS System of Records Notice; other federal agencies, and state, tribal, local and foreign law enforcement agencies; confidential sources; members of the public; and third-party commercial data brokers, sources or aggregators, or record holders. Sources of information also include: public records; publicly available information including social media; import and export records systems; immigration and admission records systems; victims; witnesses; and those individuals with knowledge of the alleged activity.

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. sec. 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. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys Offices, or other federal agency conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or 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, or individual 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, 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 a federal agency for a statistical or research purpose, including the development of methods or resources to support statistical or research activities, provided that the records support DHS programs and activities that relate to the purpose(s) stated in this SORN, and will not be used in whole or in part in making any determination

regarding an individual's rights, benefits, or privileges under federal programs, or published in any manner that identifies an individual.

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

K. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data, that relate to the purpose(s) stated in this SORN, for purposes of developing, testing, and/or implementing new technology.

L. To international and foreign governmental authorities in accordance with the law and formal or informal international arrangements.

M. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a judge-approved subpoena from a court of competent jurisdiction.

N. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance 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 disclosure is appropriate to the proper performance of the official duties of the person making the request.

O. To federal, state, local, tribal, territorial, international, or foreign government agencies or entities for the purpose of consulting with those agencies or entities: (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 redress on behalf of another individual.

P. To the Department of State when it 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 alien or an enforcement operation with transnational implications.

Q. 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 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 stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may also be stored on magnetic disc, tape, digital media, and CD-ROM. Records covered by this system of records notice may reside on the same on-premise servers or in a FedRAMP authorized cloud computing environment.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: ICE may retrieve records by any of the personal identifier's stored in the system including individual's name, Social Security number, ICE case number, biometric identification or

algorithm (e.g., facial recognition, fingerprint, voice recognition), warrant number, or vehicle, vessel (e.g., marine), or aircraft number. Records may also be retrieved by non-personal information such as search, arrest, and seizure observation device (e.g., camera identification number), serial number/footage and date, description and value of goods or currency seized, encounter date and details, location (e.g., jurisdiction or hideout coordinates), and other information.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The retention period for information contained in search, arrest, and seizure systems varies depending on the type of data. Biometric and biographical records are maintained for seventy-five (75) years in accordance with DHS schedule DA-0563-2013-0001-0006. Investigative case files are retained for twenty years (20) years after the case closure in accordance with N1-36-86-1-161.3 (inv 7B) and Neutrality/Munitions Investigative case files, which are permanent records, in accordance with N1-36-86-1-162.38. Evidentiary recordings are retained in accordance with the applicable ICE retention schedule - this is contingent on the information that is captured in the recording. For example, if the recording captures a use of force incident, it will be retained in accordance with DAA-0567-2015-0008-0001 for 45 years. Non-evidentiary video and audio recordings and associated identification information are retained for sixty (60) days in accordance with DAA-0567-2021-0001-0001. Disposal of paper files occurs by burning or shredding; electronic data is disposed of using methods approved by the DHS Chief Information Security Officer.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: ICE safeguards records in this system according to applicable rules and policies, including all applicable DHS automated system security access policies. 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. For any records covered by this system of records notice that reside in a cloud computing environment, those environments will have undergone a robust FedRAMP authorization process to validate strict controls are employed to protect the confidentiality, integrity, and availability of the records.

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 DHS Chief Privacy Officer and the 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, D.C. 20528-0655. Certain records about an individual may be available under the Freedom of Information Act if they are not available under the Privacy Act or the Judicial Redress 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. sec. 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 1-866-431-0486. 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 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 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. See "Record Access Procedures" above.

NOTIFICATION PROCEDURES: See "Records Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. sec. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), and (e)(4)(H), (e)(5), and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. sec. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f). In addition, to the extent a record contains information from other exempt systems of records, ICE will rely on the exemptions claimed for those original systems.

HISTORY: 73 Fed. Reg. 74732 (December 9, 2008).

****

Roman Jankowski,
Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2025-13609 Filed: 7/18/2025 8:45 am; Publication Date: 7/21/2025]