This document is scheduled to be published in the Federal Register on 10/21/2021 and available online at **federalregister.gov/d/2021-22836**, and on **govinfo.gov**

DEP

Docket No. DHS-2021-0041

Privacy Act of 1974; System of Records

AGENCY: Office of Inspector General, U.S. Department of Homeland Security.

ACTION: Notice of a Modified Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS), Office of Inspector General (OIG), proposes to modify and reissue a current DHS system of records titled, "DHS/OIG-002 Investigative Records System of Records." This system of records allows DHS OIG to collect and maintain records related to alleged violations of criminal, civil, and administrative laws and regulations pertaining to DHS programs, operations, and employees, as well as contractors and other individuals and entities associated with DHS; monitor complaint and investigation assignments, status, disposition, and results; manage investigations and information provided during the course of such investigations; audit actions taken by DHS management regarding employee misconduct and other allegations; audit legal actions taken following referrals to the U.S. Department of Justice (DOJ) for criminal prosecution or litigation; provide information relating to any adverse action or other proceeding that may occur as a result of the findings of an investigation; and provide a system for calculating and reporting statistical information. DHS OIG is updating this system of records notice to provide notice of changes to the Authorities, Categories of Records, Record Source Categories, and Routine Uses. Additionally, DHS is issuing an updated 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.

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 DHS-2021-0041 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: Lynn Parker Dupree, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2021-0041. 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 and privacy questions, please contact: Lynn Parker Dupree, (202) 343-1717, Chief Privacy Officer, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

The U.S. Department of Homeland Security (DHS), Office of Inspector General (OIG), is modifying and reissuing this system of records notice under the Privacy Act of 1974 (5 U.S.C. sec. 552). DHS OIG is responsible for a wide range of oversight functions, including to initiate, conduct, supervise, and coordinate audits, investigations, inspections, and other reviews relating to the programs and operations of DHS. DHS OIG promotes economy, efficiency, and effectiveness within DHS and prevents, detects, and investigates

employee corruption, fraud, waste, and abuse in its programs and operations. DHS OIG is responsible for investigating allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, and DHS programs and activities. These investigations can result in criminal prosecutions, fines, civil monetary penalties, and administrative sanctions. While DHS OIG is operationally a part of DHS, it operates independently of DHS and all offices within it.

The DHS/OIG-002 Investigative Records System of Records assists DHS OIG with receiving and processing allegations of misconduct, including violations of criminal and civil laws, as well as administrative policies and regulations pertaining to DHS employees, contractors, grantees, and other individuals and entities within DHS. The system includes complaints and investigation-related files. DHS OIG manages information provided during the course of its investigations to: create records showing dispositions of allegations; audit actions taken by DHS management regarding employee misconduct; audit legal actions taken following referrals to the U.S. Department of Justice (DOJ) for criminal prosecution or civil action; calculate and report statistical information; manage OIG investigators' training; and manage Government-issued investigative property and other resources used for investigative activities.

DHS OIG is modifying the DHS/OIG-002 Investigative Records System of Records to update the Authorities, Categories of Records, Record Source Categories, and Routine Uses. The Authorities section is being updated to provide more precise statutes for collection: 6 U.S.C. sec. 113(b); 6 U.S.C. sec. 795; 6 U.S.C. sec. 142; 6 U.S.C. sec. 345; and the Inspector General Act of 1978, as amended 5 U.S.C. App. §§ 1-13. The Categories of Records are being updated to include: 1) information obtained from social media; 2) video and photographic digital images; 3) case administrative information (e.g., status, reference number, method complaint received); 4) demographic information (e.g., gender, race, ethnicity); and 5) other types of credentials (e.g., driver's license, state ID, passport).

The Categories of Records have also been updated to clarify the types of relevant information from inspections, reviews, and inquiries that may be collected.

The Record Source Categories has been updated to clarify that records may be obtained from a variety of sources, to include: subjects, witnesses and others associated with investigations; other DHS Components and federal, state, local, nongovernmental and foreign agencies; educational institutions; credit bureaus; medical service providers; financial institutions; commercial sources; and open source or publicly available information.

Routine use (E) is being modified and a new routine use (F) is being added to conform to Office of Management and Budget Memorandum M-17-12. Routine use (P) was added to describe sharing required when testing new technologies, under the approval of the Chief Privacy Officer. In addition, a redundant routine use has been removed. All subsequent routine uses have been renumbered to account for these changes. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Consistent with DHS's information sharing mission, information stored in the DHS/OIG-002 Investigative Records 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, DHS OIG 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.

There will be no change to the Privacy Act exemptions currently in place for this system of records and therefore they remain in effect. This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act codifies fair information practice principles in a 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 JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/OIG-002 Investigative Records 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: U.S. Department of Homeland Security (DHS)/ Office of Inspector General (OIG)-002 Investigative Records System of Records.

SECURITY CLASSIFICATION: Classified, sensitive, unclassified.

SYSTEM LOCATION: Records are maintained at the DHS OIG Headquarters in Washington, D.C. and field offices. Generally, OIG maintains electronic records in the OIG Enterprise Data System (EDS).

SYSTEM MANAGER(S): Chief System Security Officer, U.S. Department of Homeland Security, Office of Inspector General, Washington, D.C., 20528.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 6 U.S.C. sec. 113(b); 6 U.S.C. sec. 795; 6 U.S.C. sec. 142; 6 U.S.C. sec. 345; and the Inspector General Act of 1978, as amended 5 U.S.C. App. §§ 1-13.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to collect and maintain records concerning DHS OIG investigations, including allegations of misconduct, violations of criminal, civil, and administrative laws and regulations pertaining to DHS programs, operations, employees, contractors, and other individuals or entities associated with DHS. This system of records is intended to support and protect the integrity of DHS OIG operations; to ensure compliance with applicable laws, regulations, and policies; and to ensure the integrity of DHS employees' conduct and those acting on behalf of DHS.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Any individual filing complaints of or related to criminal, civil, or administrative violations, including employee misconduct, fraud, waste, or mismanagement; current or former DHS employees and contractors; current or former employees of other federal agencies; contractor applicants; contractors, grantees, and individuals whose association with current and former employees relate to alleged violations under investigation; witnesses, complainants, sources of information, suspects, defendants, or parties who have been identified by DHS OIG, other DHS Components, other agencies, or members of the general public in connection with complaints, audits, inspections, and/or investigations.

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

- Full name and aliases;
- Date of birth;
- Social Security number;
- Citizenship status;
- Driver's license, state ID, passport, or other government-issued credential information;
- Demographic information (e.g., gender, race, ethnicity);
- Addresses;

- Contact information (e.g., phone numbers, email addresses);
- Employment information (e.g., duty station, grade, job series, entrance on duty date);
- Relevant information from background investigations;
- Education/training history;
- Medical history;
- Criminal history;
- Travel history, including passport information;
- Financial history;
- Relevant information from inspections, reviews, and inquiries, including records collected in response to an allegation, such as;
    - Government emails;
    - Time and attendance records;
    - Government credit card bills;
    - Building access logs;
    - Government phone bills/records;
    - Government property records;
    - Government travel records;
    - Computer forensic files;
    - Open source or publicly available information, such as social media postings;
    - Police reports; and
    - Any other information gathered in the course of or relating to an integrity or disciplinary inquiry, review, inspection, or investigation of a criminal, civil, or administrative nature;
- Investigative records of a criminal, civil, or administrative nature;

- Biometrics;
- Letters, emails, memoranda, video, photograph and digital images, and reports;
- Exhibits, evidence, statements, and affidavits;
- Relatives and associates;
- Allegations received and method received;
- Incident location/date;
- Case reference numbers;
- Case status;
- Case agent/officer or supervisor;
- Any other personal information relevant to the subject matter of an OIG investigation; and
- Investigative case files containing allegations and complaints; witness statements; transcripts of electronic monitoring; subpoenas and legal opinions and advice; reports of investigations (ROI); and reports of criminal, civil, and administrative actions taken as a result of the investigation.

RECORD SOURCE CATEGORIES: Records are obtained from individuals who are the subject of the investigation or inquiry, employers, law enforcement organizations, detention facilities, members of the public, witnesses, educational institutions, government agencies, nongovernmental organizations, credit bureaus, references, neighborhood checks, confidential sources, medical service providers, personal interviews, photographic images, military records, financial institutions, free and for-purchase commercial records, open source or publicly available information, citizenship records, and the personnel history and application forms of agency applicants, employees, or contractors. Records are also collected from other DHS Components.

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 the U.S. Attorneys Offices, or other federal agencies 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, 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, 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, state, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive when the security of the borders which DHS is tasked with maintaining are at risk of being compromised.

J. To international and foreign governmental authorities in accordance with law and formal or informal international agreements.

K. To an appropriate federal, state, local, tribal, foreign, or international agency, pursuant to a request, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual or issues 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 making the request.

L. 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 officer making the disclosure.

M. To the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and other federal agencies, as necessary, if the records respond to an audit, investigation, or review conducted pursuant to an authorizing law, rule, or regulation, and in particular those conducted at the request of the CIGIE's Integrity Committee pursuant to statute.

N. To complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigation arising from the matters of which they complained or of which they were a victim.

O. 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 testing new technology.

P. 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 OIG stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS OIG may retrieve records by the individual's name, date of birth, Social Security number, or any other unique identifier listed above.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records will be retained pursuant to DHS OIG National Archives and Records Administration (NARA) retention schedule N1-563-07-5 (October 11, 2007). Complaint and investigative record files that involve substantive information relating to national security or allegations against senior DHS officials, that attract national media or congressional attention, or that result in substantive changes in DHS policies or procedures are permanent and are transferred to the NARA 20 years after completion of the investigation and all actions based thereon. All other complaint and investigative record files are destroyed 20 years after completion of the investigation and all actions based thereon. Government issued investigative property records and management reports are destroyed when no longer needed for business purposes.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS OIG safeguards records in this system according to applicable rules and policies, including all

applicable DHS automated systems security and access policies. DHS OIG 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 certain notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act, if applicable. However, DHS 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 OIG Privacy Officer and OIG Freedom of Information Act Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contact Information." 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, U.S. Department of Homeland Security, Washington, D.C., 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. 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 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 JRA 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. sec. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. sec. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), e)(4)(I), (e)(5), (e)(8), (f); and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(k)(1), (k)(2), and (k)(5), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. sec. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

HISTORY: 80 Fed. Reg. 44372 (July 27, 2015).

Lynn Parker Dupree,
Chief Privacy Officer,
U.S. Department of Homeland Security.
[FR Doc. 2021-22836 Filed: 10/20/2021 8:45 am; Publication Date: 10/21/2021]