9110-9B

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2015-0040]

Privacy Act of 1974; Department of Homeland Security Office of the Inspector General-002 Investigative Records System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974 the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled, "Department of Homeland Security/ Office of Inspector General-002 Investigative Records System of Records." This system of records was previously titled, "Department of Homeland Security Office of Inspector General-002 Investigations Data Management System of Records." As a result of a biennial review of this system and changes to the application software, the Department of Homeland Security is proposing changes to the system name, category of individuals, and category of records in the system. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. There will be no change to the Privacy Act exemptions currently in place for this system of records. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This updated system 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-2015-0040, 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: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this notice. 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: Melinda D. Holliday McDonald, Esq. (202) 254-4284, Department of Homeland Security, Office of Inspector General, Mail Stop 2600, 245 Murray Drive, S.W., Building 410, Washington, D.C. 20528; or by facsimile (202) 254-4299. For privacy issues please contact: Karen L. Neuman (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of Homeland Security (DHS) Office of Inspector General (OIG) is revising a system of records under the Privacy Act of 1974 (5 U.S.C. 552a), for its investigative files.

The DHS Inspector General is responsible for conducting and supervising independent and objective audits, inspections, and investigations of the programs and operations of DHS. The OIG promotes economy, efficiency, and effectiveness within the Department and prevents and detects employee corruption, fraud, waste, and abuse in its programs and operations. The OIG's Office of Investigations (OI) investigates allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, and Departmental programs and activities. These investigations can result in criminal prosecutions, fines, civil monetary penalties, and administrative sanctions. Additionally, OI provides oversight and monitors the investigative activity of DHS's various internal affairs offices.

The DHS/OIG-002 Investigative Records System of Records assists the OIG with receiving and processing allegations of violations of criminal and civil law as well as administrative policies and regulations relating to DHS employees, contractors, grantees, and other individuals and entities associated with DHS. The system includes both paper complaint and investigation-related files as well as the Enterprise Data System (EDS). The OIG uses EDS to: manage information received concerning allegations (i.e., complaints) provided during the course of its investigations; 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 in investigative activities. This system of records notice makes several changes to the existing system of records. DHS/OIG is updating this system of records notice to: (1) rename this system of records notice "DHS/OIG-002 Investigative Records System of Records" and (2) include DHS OIG employees as a category of individuals covered by the system.

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, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine law enforcement related uses set forth in this system of records notice.

In accordance with the Privacy Act of 1974, DHS proposes to revise a system of records titled, Department of Homeland Security Office of Inspector General-002 Investigations Data Management System of Records and rename the system of records DHS/OIG-002 Investigative Records System of Records. There will be no change to the Privacy Act exemptions currently in place for this system of records. This revised system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies 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 the 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 United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/OIG-002 Investigative Records System of Records.

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

System of Records

Department of Homeland Security (DHS)/Office of the Inspector General (OIG)-002

System name:

DHS/OIG-002 Investigative Records System of Records.

Security classification:

Classified, sensitive, unclassified.

System location:

Records are maintained at the OIG Headquarters in Washington, D.C. and in OIG offices nationwide. Generally, OIG maintains electronic records in EDS.

Categories of individuals covered by the system:

Categories of individuals in this system include:

- Individuals filing complaints of criminal, civil, or administrative violations, including, employee corruption, fraud, waste, or mismanagement;
- Individuals alleged to have been involved in such violations;
- Individuals identified as having been adversely affected by matters investigated by the OIG;
- Individuals who have been identified as possibly relevant to, or who are contacted as part of, an OIG investigation, including:
    - Current and former employees of DHS, other federal agencies, and DHS contractors, grantees, and persons whose association with current and former employees relate to alleged violations under investigation; and
    - 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 authorized OIG audits, inspections, and/or investigations.

Categories of records in the system:

Categories of records in this system include:

- Individual's name and aliases;
- Date of birth;
- Social Security number;
- Telephone and cell phone numbers;

- Physical and mailing addresses;
- Electronic mail addresses;
- Physical description;
- Citizenship;
- Biometrics;
- Photographs;
- Education;
- Medical history;
- Travel history including passport information;
- Financial data;
- Criminal history;
- Work experience;
- Relatives and associates;
- Any other personal information relevant to the subject matter of an OIG investigation;
- Investigative files containing allegations and complaints; witness statements; transcripts of electronic monitoring; subpoenas and legal opinions and advice; reports of investigation; reports of criminal, civil, and administrative actions taken as a result of the investigation; and other relevant evidence;
- Training records and firearms qualification records of employees responsible for performing investigative functions; and
- Government owned and issued investigative property records.

Authority for maintenance of the system:

5 U.S.C. § 301; 6 U.S.C. § 113(b); the Inspector General Act of 1978, as amended.

Purpose(s):

DHS OIG uses records and information collected and maintained in this system to receive and adjudicate allegations of violations of criminal, civil, and administrative laws and regulations relating 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 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.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 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 DOJ, including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in 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 or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 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 the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this

system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; 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 compromise and prevent, minimize, or remedy such harm.

F. 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.

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 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 other information for the purposes of 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.

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

J. 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 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 when disclosure is appropriate to the proper performance of the official duties of the person making the request.

K. 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.

L. 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.

M. 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.

N. 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 or when disclosure is necessary to preserve confidence in the integrity of DHS, or 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 an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

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

Retrievability:

DHS OIG retrieves paper media alphabetically by name of subject or complainant, by complaint or investigation number, or by investigator's name and/or employee identifying number. DHS OIG retrieves electronic media by the name or identifying number for a complainant, subject, victim, or witness; by case complaint or

investigation number; by investigator's name or other personal identifier; or by investigating office designation.

Safeguards:

DHS OIG safeguards information in this system in accordance with applicable laws, rules, and policies, including all applicable DHS automated systems security and access policies. DHS imposes 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.

Retention and disposal:

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 National Archives and Records Administration 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.

System manager(s) and address:

The System Manager is the Policy Specialist, Office of Investigations, DHS OIG, Mail Stop 2600, 245 Murray Drive, S.W., Building 410, Washington, D.C. 20528.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, the Office of Inspector General will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content may submit a request in writing to the Headquarters or Office of Inspector General's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts." 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, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528-0655.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your 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, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you;
- Identify which Component(s) of the Department you believe may have the information about you;
- Specify when you believe 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 your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the Component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See "Notification Procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Records are obtained from sources including the individual record subjects; DHS officials and employees; employees of federal, state, local, and foreign agencies; and other persons and entities.

Exemptions claimed for the system:

The Secretary of Homeland Security, pursuant to 5 U.S.C. § 552a(j)(2), has exempted this system from the following provisions of the Privacy Act, subject to the

limitations set forth in 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), (k)(2), and (k)(5), has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. § 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f).

Dated: July 10, 2015.

Karen L. Neuman,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2015-18385 Filed: 7/24/2015 08:45 am; Publication Date: 7/27/2015]