Dated: October 20, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–25929 Filed 10–27–09; 8:45 am]

BILLING CODE 9110–9B–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0094]

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

AGENCY: Privacy Office, DHS.

ACTION: Notice of revised Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 the Department of Homeland Security proposes to revise a system of records titled, Department of Homeland Security Office of Inspector General—002 Investigative Records System of Records, previously titled, Department of Homeland Security Office of Inspector General—002 Investigations Data Management System of Records. As a result of the biennial review of this system and changes to the application software, the Department of Homeland Security is proposing changes to the system name, system classification, categories of individuals and records in the system, authorities for maintenance of the system, routine uses, as well as storage, safeguards, retention and disposal, and notification procedures. There will be no change to the Privacy Act exemptions currently in place for this system of records, however, the Department is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register** to reflect the system name change. This revised system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before November 27, 2009. Changes to this system will be effective November 27, 2009.

ADDRESSES: You may submit comments, identified by Docket Number DHS–2009–0094, by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 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: Doris A. Wojnarowski (202–254–4211), Department of Homeland Security, Office of Inspector General, Mail Stop 2600, 245 Murray Drive, SW., Building 410, Washington, DC 20528; or by facsimile (202) 254–4299. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 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 Department is updating and reissuing the DHS/OIG–002 Investigations Data Management System of Records (IDMS) (70 FR 58448, October 6, 2005) under a new name, the DHS/OIG–002 Investigative Records System of Records, to cover these and additional records.

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 fraud, waste, and abuse in its programs and operations. The OIG's Office of Investigations 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, the Office of Investigations provides oversight and monitors the investigative activity of DHS' various internal affairs offices.

The DHS/OIG–002 Investigative Records System of Records assists the OIG with receiving and processing allegations of violation of criminal, civil, and administrative laws and regulations relating to DHS employees, contractors, grantees, and other individuals and entities associated with DHS. The system includes both paper investigative files and the Enforcement Data System (EDS), an electronic case management and tracking information system which also generates reports. EDS allows the OIG to manage information provided during the course of its investigations, and, in the process, to facilitate its management of investigations and investigative resources. Through EDS, the OIG can create a record showing disposition of allegations; track actions taken by management regarding misconduct; track legal actions taken following referrals to the U.S. Department of Justice for prosecution or civil action; provide a system for creating and reporting statistical information; and track OIG investigators' qualifications as well as government property and other resources used in investigative activities.

This system notice makes several changes to the existing record system. It changes the name of the system; adds unclassified information to system classification; adds Federal agencies, DHS contractors, DHS grantees, DHS components, and DHS OIG employees performing investigative functions to categories of individuals covered by the system; completely updates categories of records within the system; adds new authorities for maintenance of the system to include 6 U.S.C. 113(b) and the Inspector General Act of 1978, as amended; revises the routine uses to conform with the needs of DHS OIG; updates storage, safeguards and retention and disposal of the system; and outlines notification procedures for 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, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine 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, DHS/OIG–002 Investigative Records System of Records, previously titled, DHS/OIG–002 Investigations Data Management System of Records (70 FR 58448,

October 6, 2005). As a result of the biennial review of this system and changes to the application software, DHS is proposing changes to the system name, system classification, categories of individuals and records in the system, authorities for maintenance of the system, routine uses, as well as storage, safeguards, retention and disposal, and notification procedures. There will be no change to the Privacy Act exemptions currently in place for this system of records, however, DHS is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register** to reflect the system name change. This revised system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates 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 where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by submitting a request pursuant to DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to which their records are put, and to assist individuals to more easily find such files within the agency. Below is the revised 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:

DHS–OIG–002.

SYSTEM NAME:

Department of Homeland Security Office of Inspector General Investigative Records System of Records.

SECURITY CLASSIFICATION:

Classified, sensitive, unclassified.

SYSTEM LOCATION:

Records are maintained at the OIG Headquarters in Washington, DC, and in OIG field offices nationwide.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals filing complaints of criminal, civil, or administrative violations, including, but not limited to, 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: (A) Current and former employees of the DHS, other Federal agencies, and DHS contractors, grantees, and persons whose association with current and former employees relate to alleged violations under investigation; and, (B) witnesses, complainants, confidential informants, suspects, defendants, or parties who have been identified by the DHS OIG, other DHS components, other agencies, or members of the general public in connection with authorized OIG functions; and DHS OIG employees performing investigative functions.

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;
- Fingerprints, voiceprints, and other biometric data;
- 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 complaints and allegations, 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 and firearms qualification records of employees performing investigative functions; and
- Accountable 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):

The records and information collected and maintained in this system are used to receive and process 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 case assignments, status, disposition, and results; manage investigations and information provided during the course of such investigations; track actions taken by management regarding misconduct and other allegations; track legal actions taken following referrals to the Department of Justice for 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; provide a system for creating and reporting statistical information; and to provide a system to track firearms qualification and training records of OIG employees performing investigative functions and accountable property records.

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 the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is 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 of DHS in his/her official capacity;

3. any employee of DHS in his/her individual capacity where the Department of Justice or DHS has agreed to represent the employee; or,

4. the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

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 other Federal agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and § 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, including peer reviews, 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 harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity), or harm to the individuals that rely on 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, where 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.

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, 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/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation arising from the matters of which they complained and/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 it is determined 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:

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.

RETRIEVABILITY:

Paper media are retrieved alphabetically by name of subject or complainant, by case number, and/or by special agent name and/or employee identifying number. Electronic media are retrieved by the name or identifying number for a complainant, subject, victim, or witness; by case number; by special agent name or other personal identifier; or by field office designation.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws, rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed 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:

Investigative case 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 investigative case files are destroyed 20 years after completion of the investigation and all actions based thereon. Accountable property records, training and firearms qualification records, and management reports are destroyed when no longer needed for business purposes.

SYSTEM MANAGER(S) AND ADDRESS:

The System Manager is the Assistant Inspector General for Investigations, DHS OIG, Mail Stop 2600, 245 Murray Drive, SW., Building 410, Washington, DC 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, SW., Building 410, STOP–0550, Washington, DC 20528.

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;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- 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, but not limited to, 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 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) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security 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) pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and (k)(5).

Dated: October 20, 2009.

Mary Ellen Callahan

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–25945 Filed 10–27–09; 8:45 am]

BILLING CODE 9110–9B–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0039]

Privacy Act of 1974; Department of Homeland Security/ALL—001 Freedom of Information Act and Privacy Act Records System of Records

AGENCY: Privacy Office, DHS.

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 Department of Homeland Security system of records notice titled, Department of Homeland Security/ALL—001 Freedom of Information Act and Privacy Act Records System of Records. The updated system of records consists of information that is created and used by the Department's Freedom of Information Act and Privacy Act staff to process requests as well as to manage the Freedom of Information Act and Privacy Act programs. As a result of the biennial review of this system, the Privacy Office has: Updated the system classification to include unclassified information; updated the categories of individuals and records to include individuals who are the subjects of requests, Department of Justice and other government litigators and/or DHS personnel assigned to handle such requests or appeals; revised the routine uses to conform with the needs of the Freedom of Information Act and Privacy Act program; and updated the Privacy Act exemptions for this system of records to include the addition of 5 U.S.C. 552a(k)(3) and (k)(6) of the Privacy Act. A Notice of Proposed Rulemaking is published elsewhere in the **Federal Register** further exempting these records from 5 U.S.C. 552a(k)(3) and (k)(6) of the Privacy Act. The initial Privacy Act exemptions published with this system of records (December 6, 2004), will remain in place until this rule is finalized with the addition of 5 U.S.C. 552a(k)(3) and (k)(6). This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before November 27, 2009. This system will be effective November 27, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2009–0039 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.