



9110-9B

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2015-0049]

Privacy Act; Department of Homeland Security/ALL-038 Insider Threat Program

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 establish a new Department of Homeland Security system of records titled, “Department of Homeland Security/ALL-038 Insider Threat Program system of records.” This system allows the Department of Homeland Security to manage insider threat inquiries, investigations, and other activities associated with complaints, inquiries, and investigations regarding the unauthorized disclosure of classified national security information; identification of potential threats to Department of Homeland Security resources and information assets; tracking of referrals of potential insider threats to internal and external partners; and providing statistical reports and meeting other insider threat reporting requirements. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in this Federal Register. This

newly established 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 new 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-2015-0049 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. 20528-0655.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. 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, please visit <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, 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) proposes to establish a new DHS system of records titled “DHS/ALL-038 Insider Threat Program system of records.”

The Department of Homeland Security has created a Department-wide system, known as the Insider Threat Program system of records to manage insider threat matters within DHS. The Insider Threat Program was mandated by E.O. 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,” issued October 7, 2011, which requires Federal agencies to establish an insider threat detection and prevention program to ensure the security of classified networks and the responsible sharing and safeguarding of classified information with appropriate protections for privacy and civil liberties. Insider threats include: attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against DHS and its personnel, facilities, resources, and activities; unauthorized use of or intrusion into automated information systems; unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary information or technology; and indicators of potential insider threats. The Insider Threat Program system may include information from any DHS Component, office, program, record, or source, and includes records from

information security, personnel security, and systems security for both internal and external security threats.

Consistent with DHS' information sharing mission, information stored in the DHS/ALL-038 Insider Threat Program 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 may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in this Federal Register. This newly established system will be included in DHS' 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 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. 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 DHS/ALL-038 Insider Threat Program system of records.

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

System of Records

Department of Homeland Security (DHS)/ALL-038 Insider Threat Program System of Records

System name:

DHS/ALL-038 Insider Threat Program

Security classification:

Unclassified, sensitive, for official use only, and classified.

System location:

Records are maintained at several DHS Headquarters and Component locations in Washington, D.C. and field offices.

Categories of individuals covered by the system:

- DHS current or former employees, contractors, or detailees who have access or had access to national security information, including classified information.

- Other individuals, including Federal, State, local, tribal, and territorial government personnel and private-sector individuals, who are authorized by DHS to access Departmental facilities, communications security equipment, and/or information technology systems that process sensitive or classified national security information.
- Any other individual with access to national security information including classified information, who accesses or attempts to access DHS IT systems, DHS national security information, or DHS facilities.
- Family members, dependents, relatives, and individuals with a personal association to an individual who is the subject of an insider threat investigation; and
- Witnesses and other individuals who provide statements or information to DHS related to an insider threat inquiry.

Categories of records in the system:

Categories of Records in the system include:

Information related to lawful DHS security investigations, including authorized physical, personnel, and communications security investigations, information systems security analysis and reporting, and information derived from Standard Form 86 questionnaires, including:

- Individual's name;
- Date and place of birth;
- Social Security number;

- Address;
 - Publicly available social media account information;
 - Personal and official email addresses;
 - Citizenship;
 - Personal and official phone numbers;
 - Driver's license numbers;
 - Vehicle identification numbers;
 - License plate numbers;
 - Ethnicity and race;
 - Work history;
 - Educational history;
 - Information on family members, dependents, relatives, and other personal associations;
 - Passport numbers;
 - Gender;
 - Hair and eye color;
 - Biometric data;
 - Other physical or distinguishing attributes of an individual;
 - Medical reports;
 - Access control pass, credential number, or other identifying number;
- and

- Photographic images, videotapes, voiceprints, or DVDs;

Records relating to the management and operation of DHS personnel security program, including but not limited to:

- Completed standard form questionnaires issued by the Office of Personnel Management;
- Background investigative reports and supporting documentation, including criminal background, medical, and financial data;
- Other information related to an individual's eligibility for access to classified information;
- Criminal history records;
- Polygraph examination results;
- Logs of computer activities on all DHS IT systems or any IT systems accessed by DHS personnel with security clearances;
- Nondisclosure agreements;
- Document control registries;
- Courier authorization requests;
- Derivative classification unique identifiers;
- Requests for access to sensitive compartmented information (SCI);
- Records reflecting personal and official foreign travel;
- Facility access records;
- Records of contacts with foreign persons;

- Briefing/debriefing statements for special programs, sensitive positions, and other related information and documents required in connection with personnel security clearance determinations;

Reports of investigation regarding security violations, including but not limited to:

- Individual statements or affidavits and correspondence;
- Incident reports;
- Drug test results;
- Investigative records of a criminal, civil, or administrative nature;
- Letters, emails, memoranda, and reports;
- Exhibits, evidence, statements, and affidavits;
- Inquiries relating to suspected security violations; and
- Recommended remedial actions for possible security violations;

Any information related to the management and operation of the DHS insider threat program, including but not limited to:

- Documentation pertaining to investigative or analytical efforts by DHS insider threat program personnel to identify threats to DHS personnel, property, facilities, and information;
- Records collated to examine information technology events and other information that could reveal potential insider threat activities;
- Travel records;
- Intelligence reports and database query results relating to individuals

covered by this system;

- Information obtained from the Intelligence Community, the Federal Bureau of Investigation (FBI), or from other agencies or organizations about individuals known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to an insider threat, including but not limited to espionage or unauthorized disclosures of classified national security information;
- Information provided by record subjects and individual members of the public; and
- Information provided by individuals who report known or suspected insider threats.

Authority for maintenance of the system:

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458; Intelligence Authorization Act for FY 2010, Pub. L. 111-259; Atomic Energy Act of 1954, 60 Stat. 755, August 1, 1946; Title 6 U.S.C. 341(a)(6), Under Secretary for Management; Title 28 U.S.C. 535, Investigation of Crimes Involving Government Officers and Employees; Limitations; Title 40 U.S.C. 1315, Law enforcement authority of Secretary of Homeland Security for protection of public property; Title 50 U.S.C. 3381, Coordination of Counterintelligence Activities; E.O. 10450, Security Requirements for Government Employment, April 17, 1953; E.O. 12333, United States Intelligence Activities (as amended); E.O. 12829, National Industrial Security Program; E.O.

12968, Access to Classified Information, August 2, 1995; E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008; E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, January 16, 2009; E.O. 13526, Classified National Security Information; E.O. 13,549, Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities, August 18, 2010; E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011; and Presidential Memorandum National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 21, 2012.

Purpose(s):

The purpose of the Insider Threat Program system of records is to manage insider threat matters; facilitate insider threat investigations and activities associated with counterintelligence and counterespionage complaints, inquiries, and investigations; identify threats to DHS resources and information assets; track referrals of potential insider threats to internal and external partners; and provide statistical reports and meet other insider threat reporting requirements.

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

A. To the Department of Justice (DOJ), including 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 or her official capacity;
3. Any employee or former employee of DHS in his or 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 (GSA) 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. DHS 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' 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, territorial, 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 an appropriate Federal, State, local, tribal, territorial, 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, delegation or designation of authority, 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, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

I. To an individual's prospective or current employer to the extent necessary to determine employment eligibility.

J. To third parties during the course of an 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 individual making the disclosure.

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

L. To another federal agency in order to conduct or support authorized counterintelligence activities, as defined by 50 U.S.C. 3003(3).

M. To any Federal, State, local, tribal, territorial, foreign, or multinational government or agency, or appropriate private sector individuals and organizations lawfully engaged in national security or homeland defense for that entity's official responsibilities, including responsibilities to counter, deter, prevent, prepare for, respond to, threats to national or homeland security, including an act of terrorism or espionage.

N. To a Federal, State, local, tribal, or territorial government or agency lawfully engaged in the collection of intelligence (including national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, law enforcement or law enforcement intelligence, and other information, when disclosure is undertaken for intelligence, counterterrorism, homeland security, or related law enforcement purposes, as authorized by U.S. law or E.O.

O. To any individual, organization, or entity, as appropriate, to notify them of a serious threat to homeland security for the purpose of guarding them against or responding to such a threat, or when there is a reason to believe that the recipient is or could become the target of a particular threat, to the extent the information is relevant to the protection of life, health, or property.

P. To members of the U.S. House Committee on Oversight and Government Reform and the Senate Homeland Security and Governmental Affairs Committee pursuant to a written request under 5 U.S.C. 2954, after consultation with the Chief Privacy Officer and the General Counsel.

Q. To individual members the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence in connection with the exercise of the Committees' oversight and legislative functions, when such disclosures are necessary to a lawful activity of the United States, after consultation with the Chief Privacy Officer and the General Counsel.

R. To a Federal agency or entity that has information relevant to an allegation or investigation regarding an insider threat for purposes of obtaining guidance, additional information, or advice from such federal agency or entity regarding the handling of an insider threat matter, or to a federal agency or entity that was consulted during the processing of the allegation or investigation but that did not ultimately have relevant information.

S. To a former DHS employee, DHS contractor, or individual sponsored by DHS for a security clearance for purposes of responding to an official inquiry

by Federal, State, local, tribal, or territorial government agencies or professional licensing authorities; or facilitating communications with a former employee that may be relevant and necessary for personnel-related or other official purposes when DHS requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

T. 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' 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/ALL-038 Insider Threat Program system of records 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.

Retrievability:

DHS may retrieve records by first and last name, Social Security number, date of birth, phone number, other unique individual identifiers, and other types of information by key word search.

Safeguards:

DHS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS 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.

Retention and disposal:

DHS is working with NARA to develop the appropriate retention schedule based on the information below. For persons DHS determines to be insider threats, information in the Insider Threat Program system of records that is related to a particular insider threat is maintained for twenty-five years from the date when the insider threat was discovered. For persons DHS determines are not insider threats, the information will be destroyed three years after notification of death, or five years after (1) the individual no longer has an active security clearance held by DHS, (2) separation or transfer of employment, or (3) the individual's contract relationship with DHS expires; whichever is applicable.

System Manager and address:

Chief, Insider Threat Operations Center (202-447-5010), Office of the Chief Security Officer, Department of Homeland Security, 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, DHS 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 Chief Privacy 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, 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 (FOIA) Officer, <http://www.dhs.gov/foia> or 1-866-431-0486. In addition, you should:

- Explain 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 the above 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 Department officials, employees, contractors, and other individuals who are associated with or represent DHS; officials from other foreign, Federal, tribal, State, and local government organizations; non-government, commercial, public, and private agencies and organizations; relevant DHS records, databases, and files, including personnel security files, facility access records, security incidents or violation files, network security records, investigatory records, visitor records, travel records, foreign visitor or contact reports, and financial disclosure reports; media, including periodicals, newspapers, and broadcast transcripts; intelligence source documents; publicly available information, including publicly available social media; and complainants, informants, suspects, and witnesses.

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: 5 U.S.C. 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), (e)(12); (f); (g)(1); and (h). 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, 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from

which they originated and claims any additional exemptions set forth here.

Dated: February 18, 2016.

Karen L. Neuman,
Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2016-03924 Filed: 2/25/2016 8:45 am; Publication Date: 2/26/2016]