4310-RK-P

DEPARTMENT OF THE INTERIOR

Office of the Secretary

[XXXD4523WT DWT000000.000000 DS65101000]

Privacy Act of 1974, as Amended; Notice of a New System of Records

AGENCY: Department of the Interior.

ACTION: Notice of Creation of a New System of Records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of the Interior is issuing a public notice of its intent to create the Department of the Interior Insider Threat Program system of records. The Department of the Interior Office of Law Enforcement and Security will use the system to facilitate management of insider threat investigations and activities associated with counterintelligence complaints, inquiries and investigations; identify potential threats to Department of the Interior 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. This newly established system will be included in the Department of the Interior's inventory of record systems.

DATES: Comments must be received by [INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER.]. This new system will be effective [INSERT DATE 40 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Any person interested in commenting on this amendment may do so by: submitting comments in writing to the Departmental Privacy Act Officer, 1849 C Street NW, Mail Stop 5547 MIB, Washington, DC 20240; hand-delivering comments to the

Departmental Privacy Act Officer, 1849 C Street N.W., Mail Stop 5547 MIB, Washington, D.C. 20240 or e-mailing comments to *Privacy@ios.doi.gov*.

FOR FURTHER INFORMATION CONTACT: Chief, National Security Programs, Office of Law Enforcement and Security, Intelligence Division, 1849 C Street NW, MIB-3409, Washington, DC, 20240. Telephone: 202-208-6206.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of the Interior (DOI) has created a Department-wide system, known as the Insider Threat Program system of records, to manage insider threat matters within DOI. The Insider Threat Program was mandated by Presidential Executive Order 13587, issued October 7, 2011, which required 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 consistent with appropriate protections for privacy and civil liberties. Insider threats include attempted or actual espionage, subversion, sabotage, terrorism or extremist activities directed against the Department of the Interior 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; indicators of potential insider threats or other incidents that may indicate activities of an insider threat. The Insider Threat Program system may include information from any DOI bureau, office, program, record or source, and includes records from information security, personnel security, and systems security for both internal and external security threats.

In a notice of proposed rulemaking, which is published separately in the Federal Register, the Department of the Interior is proposing to exempt records maintained in this system from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

The system will be effective as proposed at the end of the comment period (the comment period will end 40 days after the publication of this notice in the Federal Register), unless comments are received which would require a contrary determination. DOI will publish a revised notice if changes are made based upon a review of the comments received.

II. Privacy Act

The Privacy Act of 1974, as amended, embodies fair information practice principles in a statutory framework governing the means by which Federal Agencies collect, maintain, use, and disseminate individuals' personal information. The Privacy Act applies to records about individuals that are maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particulars assigned to the individual. The Privacy Act defines an individual as a United States citizen or lawful permanent resident. As a matter of policy, DOI extends administrative Privacy Act protections to all individuals. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOI by complying with DOI Privacy Act regulations at 43 CFR part 2.

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 of each system to make agency recordkeeping practices transparent, notify individuals regarding the uses of their records, and assist individuals to more easily find such records within the agency. Below is the description of the Department of the Interior Insider Threat Program system of records.

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

III. Public Disclosure

Before including your address, phone number, e-mail address, or other personal identifying information in your comment, you should be aware that your entire comment – including your personal identifying information – may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Dated: August 26, 2014.

Teri Barnett,

DOI Privacy Act Officer.

SYSTEM NAME:

Insider Threat Program, DOI-50

SECURITY CLASSIFICATION:

Classified and unclassified.

SYSTEM LOCATION

Office of Law Enforcement and Security, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered in the system include current and former DOI employees, potential employees, and contractors; other officials or employees of Federal, state, tribal, territorial, and local law enforcement organizations; complainants, informants, suspects and witnesses; persons with access to DOI facilities and infrastructure; members of the general public, including individuals and/or groups of individuals involved with insider threat matters, complaints or incidents involving classified systems or classified information; individuals being investigated as potential insider threats; individuals identified as the result of an administrative, security or investigative function who could pose a threat to DOI operations, data, personnel, facilities and systems; and foreign visitors or foreign contacts that become involved in the Foreign Visitors Program, or insider threat matters.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system may contain information from DOI bureaus, offices, programs, databases, records or sources, including incident reports, investigatory records, personnel security records, facility access records, network security records, security violations, travel records, foreign visitor records, foreign contact reports, financial disclosure reports, personnel records, medical records, information on complainants, informants, suspects, and witnesses, and records involving potential insider threats or activities directed against

the Department of the Interior and its personnel, facilities, and resources. These records may contain the following information: names, Social Security numbers, dates of birth, place of birth, security clearance, home addresses, work addresses, personal and official phone numbers, personal and official email addresses, other contact information, driver license numbers, vehicle identification numbers, license plate numbers, ethnicity and race, tribal identification numbers or other tribal enrollment data, work history, educational history, affiliations, information on family members, dependents, relatives and other personal associations, passport numbers, gender, fingerprints, hair and eye color, biometric data, and any other physical or distinguishing attributes of an individual. Investigation records and incident reports may include additional information such as photos, video, sketches, medical reports, and network use records, identification badge data, facility and access control records, email and text messages. Records may also include information concerning potential insider threat activity, counterintelligence complaints, investigative referrals, results of incident investigations, case number, forms, nondisclosure agreements, consent forms, documents, reports, and correspondence received, generated or maintained in the course of managing insider threat activities and conducting investigations related to the protection of DOI resources and information assets against potential insider threats.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458; Intelligence Authorization Act for FY 2010, Public Law 111-259; Title 28 U.S.C. 535, Investigation of Crimes Involving Government Officers and Employees; Limitations; Title 50 U.S.C. 402a, Coordination of Counterintelligence Activities; Executive Order

10450, Security Requirements for Government Employment, April 17, 1953; Executive Order 12333, United States Intelligence Activities (as amended); Executive Order 12829, National Industrial Security Program; Executive Order 12968, Access to Classified Information, August 2, 1995; Executive Order 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; Executive Order 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, January 16, 2009; Executive Order 13526, Classified National Security Information; Executive Order 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.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

The primary purpose of the Insider Threat Program system of records is to manage insider threat matters; facilitate insider threat investigations and activities associated with counterintelligence complaints, inquiries and investigations; identify potential threats to Department of the Interior 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.

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 DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

(1) (a) To any of the following entities or individuals, when the circumstances set forth in paragraph (b) are met:

(i) The U.S. Department of Justice (DOJ);

(ii) A court or an adjudicative or other administrative body;

(iii) A party in litigation before a court or an adjudicative or other administrative body; or

(iv) Any DOI employee acting in his or her individual capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee;

(b) When:

(i) One of the following is a party to the proceeding or has an interest in the proceeding:

(A) DOI or any component of DOI;

(B) Any other Federal agency appearing before the Office of Hearings and Appeals;

(C) Any DOI employee acting in his or her official capacity;

(D) Any DOI employee acting in his or her individual capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee;

(E) The United States, when DOJ determines that DOI is likely to be affected by the proceeding; and

(ii) DOI deems the disclosure to be:

(A) Relevant and necessary to the proceeding; and

(B) Compatible with the purpose for which the records were compiled.

(2) To a congressional office in response to a written inquiry that an individual covered by the system, or the heir of such individual if the covered individual is deceased, has made to the office, to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(3) To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible for which the records are collected or maintained, to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(4) To any criminal, civil, or regulatory law enforcement authority (whether Federal, State, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

(5) To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

(6) To Federal, State, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

(7) To representatives of the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

(8) To State and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

(9) To an expert, consultant, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

(10) To appropriate agencies, entities, and persons when:

(a) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; and

(b) The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interest, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and

(c) The disclosure is made to such agencies, entities and persons who are reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(11) To the Office of Management and Budget during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-

19.

(12) To the Department of the Treasury to recover debts owed to the United States.

(13) To the Department of Justice, the Federal Bureau of Investigation, the Department of Homeland Security, and other Federal, State and local law enforcement agencies for the purpose of referring potential insider threats and information exchange on insider threat activity.

(14) To agency contractors, grantees, or volunteers for DOI or other Federal Departments who have been engaged to assist the Government in the performance of a contract, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform the activity.

(15) To any criminal, civil, or regulatory authority (whether Federal, State, territorial, local, or tribal) for the purpose of providing background search information on individuals for legally authorized purposes, including but not limited to background checks on individuals residing in a home with a minor or individuals seeking employment opportunities requiring background checks.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Electronic records are maintained in password-protected systems that are compliant with the Federal Information Security Management Act, and paper records are

maintained in file cabinets. Access is limited to authorized personnel who have a need to access the records in the performance of their official duties.

RETRIEVABILITY:

Multiple fields allow retrieval of individual record information including first and last name, Social Security number, date of birth, phone number, and other types of information by key word search.

SAFEGUARDS:

The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security and privacy rules and policies. During normal hours of operation, paper records are maintained in locked filed cabinets under the control of authorized personnel. Computerized records systems follow the National Institute of Standards and Technology privacy and security standards as developed to comply with the Privacy Act of 1974 (Pub. L. 93–579), Paperwork Reduction Act of 1995 (Pub. L. 104–13), Federal Information Security Management Act of 2002 (Pub. L. 107–347), and the Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems. Computer servers in which electronic records are stored are located in secured Department of the Interior facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI network and information assets. Security controls include encryption, firewalls, audit logs, and network system security monitoring.

Electronic data is protected through user identification, passwords, database permissions and software controls. Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their

official duties, and each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior.

RETENTION AND DISPOSAL:

A records retention schedule for the Insider Threat Program has been developed and submitted to the National Archives and Records Administration (NARA) for approval. Pending approval by NARA, these records will be treated as permanent. The proposed records disposition is temporary, and records will be destroyed when no longer needed for agency business. Approved disposition methods include shredding or pulping paper records, and degaussing or erasing electronic records in accordance with 384 Department Manual 1 and NARA guidelines.

SYSTEM MANAGER AND ADDRESS:

Chief, National Security Programs, Office of Law Enforcement and Security, Intelligence Division, 1849 C Street NW, MIB-3409, Washington, DC, 20240.

NOTIFICATION PROCEDURES:

The Department of the Interior is proposing to exempt portions of this system from the notification procedures of the Privacy Act pursuant to sections (j)(2) and (k)(2). An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request envelope and letter should both be clearly marked "PRIVACY ACT INQUIRY." A request for notification must meet the requirements of 43 CFR 2.235.

RECORDS ACCESS PROCEDURES:

The Department of the Interior is proposing to exempt portions of this system from the access procedures of the Privacy Act pursuant to sections (j)(2) and (k)(2). An individual requesting records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request should describe the records sought as specifically as possible. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR ACCESS." A request for access must meet the requirements of 43 CFR 2.238.

CONTESTING RECORDS PROCEDURES:

The Department of the Interior is proposing to exempt portions of this system from the amendment procedures of the Privacy Act pursuant to sections (j)(2) and (k)(2). An individual requesting corrections or the removal of material from his or her records should send a signed, written request to the System Manager identified above. A request for corrections or removal must meet the requirements of 43 CFR 2.246.

RECORD SOURCE CATEGORIES:

Sources of information in the system include Department, bureau, office and program officials, employees, contractors, and other individuals who are associated with or represent the DOI; officials from other Federal, Tribal, State, and local government organizations; relevant DOI 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; and complainants, informants, suspects, and witnesses.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

This system contains classified and unclassified intelligence and law enforcement investigatory records related to counterintelligence and insider threat activities that are exempt from certain provisions of the Privacy Act, 5 U.S.C. 552a(j)(2) and (k)(2). Pursuant to the Privacy Act, 5 U.S.C. 552a(j)(2) and (k)(2), the Department of the Interior has exempted portions of this system from the following subsections of the Privacy Act: (c)(3), (c)(4), (d), (e)(1) through (e)(3), (e)(4)(G) through (e)(4)(I), (e)(5), (e)(8), (e)(12), (f), and (g). In accordance with 5 U.S.C. 553(b), (c) and (e), the Department of the Interior has promulgated rules, which have been published separately in today's Federal Register.

[FR Doc. 2014-20741 Filed 08/29/2014 at 8:45 am; Publication Date: 09/02/2014]