



This document is scheduled to be published in the Federal Register on 01/04/2017 and available online at <https://federalregister.gov/d/2016-31315>, and on FDsys.gov

Billing Code: 3510–BX–P

DEPARTMENT OF COMMERCE

Docket No. 161102999-6999-01

Privacy Act of 1974, New System of Records

AGENCY: Office of the Secretary, U.S. Department of Commerce.

ACTION: Notice of a New Privacy Act System of Records: COMMERCE/DEPT-27, Investigation and Threat Management Records.

SUMMARY: The Department of Commerce (Department) is issuing this notice of its intent to establish a new system of records entitled “COMMERCE/DEPARTMENT–27, Investigation and Threat Management Records.” This action is being taken to update the Privacy Act notice and Department Notice to Amend All Privacy Act System of Records. We invite the public to comment on the items noted in this publication. This system allows the Department of Commerce to conduct investigations and analyses to identify and/or assess critical threats to the Department’s mission, operations, or activities; prevent or mitigate such threats from adversely affecting Department personnel, facilities, property, or assets through strategic and tactical approaches; and collaborate with other national security and law enforcement entities as appropriate.

DATES: To be considered, written comments must be submitted on or before [insert date 30 days from publication in the FEDERAL REGISTER]. Unless comments are received, the new system of records will become effective as proposed on [insert date 40 days from publication in the FEDERAL REGISTER]. If comments are received, the Department will publish a subsequent notice in the FEDERAL REGISTER within 10 days after the comment period closes,

stating that the current system of records will remain in effect until publication of a final action in the FEDERAL REGISTER.

ADDRESSES: You may submit written comments by any of the following methods:

Email: MHarman@doc.gov. Include “Privacy Act COMMERCE/DEPT–27, Investigation and Threat Management Records” in the subtext of the message.

Fax: (202) 482–4979, marked to the attention of Mr. Michael Harman.

Mail: Mr. Michael Harman, Office of Security, U.S. Department of Commerce, 1401 Constitution Ave. NW., Room 1067, Washington, DC 20230.

FOR FURTHER INFORMATION, CONTACT: Michael Harman, as noted in the ADDRESSES section above.

SUPPLEMENTARY INFORMATION: This notice announces the Department’s proposal for a new system of records being established under the Privacy Act of 1974 for Investigation and Threat Management Records. This new system of records is to account for the collection, maintenance, and use of information in connection with mission critical threats to the Department.

In a notice of proposed rulemaking, which is published separately in today’s **Federal Register**, the Department 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), (k)(1), (k)(2), and (k)(5). The Department is instituting this new system of records in accordance with the Privacy Act of 1974, as amended, Title 5 United States Code (U.S.C.) 552(e)(4) and (11); and Office of Management and Budget (OMB) Circular A–130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.

The system will be effective as proposed, on the date in the DATES section of this notice, unless comments are received which would require a contrary determination. If comments are received, the Department will publish a subsequent notice in the FEDERAL REGISTER within 10 days after the comment period closes, stating that the current system of records will remain in effect until publication of a final action in the FEDERAL REGISTER.

COMMERCE/DEPT-27

System Name:

Investigation and Threat Management Records.

Security Classification:

Unclassified, controlled unclassified information, for official use only, law enforcement sensitive, and classified.

System Locations:

Departmental Office of Security, OS, Herbert C. Hoover Building, Washington, DC 20230.

Office of Security, 551 John Carlyle Street, Alexandria, VA 22314.

Office of Security, 100 Bureau Drive, Gaithersburg, MD 20899.

Office of Security, 1315 East-West Highway, Silver Spring, MD 20910.

Office of Security, 325 Broadway St. Boulder, CO 80305.

Office of Security, 4600 Silver Hill Road, Suitland, MD 20746.

Categories of Individuals Covered by the System:

The categories of individuals covered by this system include Department employees, former employees, and prospective employees; political appointees; research associates and guest workers; interns and detailees to the Department; foreign nationals and locally employed staff working for or with Department employees, and are assigned to or salaried by other U.S.

government agencies in locations worldwide; employees of contractors used, or which may be used, by the Department; employees, principal Officers, and company information of contractors/businesses retained, or which may be retained by the Department, to include subcontractors; individuals who have access, had access, will require access, or attempt access to any Department owned or leased facility, communications equipment, or information technology system; employees of other U.S. government agencies, foreign officials, or members of the public who visit the Department or have or may have other associations with the Department; family members, dependents, relatives, and individuals with a personal association to Department employees, former employees, and prospective employees; principal Officers and employees of organizations, firms, or institutions which were recipients or beneficiaries, or prospective recipients or beneficiaries, of grants, loans, or loan guarantee programs of the Department; sub-grantees, lessees, licensees or other persons engaged in business with the Department; and nominees, members, and former members of public advisory committees, boards, trade missions and export councils that may be part of the Department or associated with Department function.

The system also includes current and former employees of the Department and such other persons and entities whose association with the Department relates or may relate to the alleged violations of the Department's policies, rules of conduct, or any other criminal or civil misconduct, which affects the integrity, facilities, information, or assets of or within the Department. The identities of individuals and the files associated with them may be: (1) Received by referral; or (2) Initiated at the discretion of the Investigations and Threat Management Division ("ITMD") in the conduct of assigned duties, and include all of the categories listed in the preceding paragraph, as well as the following: employees or contractors

of other U.S. government agencies, named and unnamed, who are working with or supporting the investigative or intelligence functions of the ITMD; individuals identified in U.S. visa, border, immigration and naturalization benefit data, including arrival and departure data, that are included in results seeking Department-related individuals; individuals identified by U.S. or foreign information or intelligence reporting that are included in results seeking Department-related individuals; individuals who are: witnesses; complainants; confidential or non-confidential informants; suspects; defendants; and parties who have been identified by the ITMD or by other agencies, constituent units of the Department, and members of the general public in connection with the authorized functions of the ITMD.

Categories of Records in the System:

Categories in this system include individual identifying records, which may include some or all of the following: names and aliases; phone numbers, addresses and other contact information; date and place of birth; Social Security number; driver license, vehicle identification, and license plate numbers; visa, passport, and citizenship records, data, and documents; physical characteristics, sex, gender, and ethnicity; education, employment and military service history; salary and duty station; human resource and personnel data; affiliations; travel history; tax and financial records; credit references and credit records; medical history; records related to drug and alcohol use; biometric data; license and permit records, data, and documents; criminal and arrest records; dates and purpose of visits to foreign countries; names of spouses, relatives, references, affiliations, and personal associates; activities; special access program requests; facility and computer access logs; clearance adjudication and investigation data; and security and suitability materials.

Investigative files may include additional information such as allegations and referrals received and method received; publically and privately obtained internet data and items posted to social networking sites; information from background investigations; incidents involving unauthorized access to classified national security information (“classified”); individual identifying records; facility access logs; information processing use and activity records; classified and unclassified intelligence reports; activities having a potential bearing on the security of Department operations domestic and abroad, to include those involving criminal or foreign intelligence activities; photographic images, videos, audio recordings, CDs, DVDs, tapes; email and text messages; letters, e-mails, memoranda, notes, forms, and reports; exhibits, evidence, statements, affidavits, and correspondence; subpoena and grand jury information; materials and information on subjects of inquiries or investigations conducted by or on behalf of other Federal agencies; activities other agencies believe may have a bearing on U.S. foreign policy interests; reports of policy, physical, information, or cyber security violations or infractions, and recommendations for remedial actions and mitigation; activities and records related to Department cyber infrastructure, intrusion and network defense; litigants in civil suits and criminal prosecutions of interest to the ITMD; other documentation pertaining to investigative or analytical efforts by the ITMD to identify threats to the Department’s personnel, property, facilities, and information; and all other data included in inquiries or investigations into possible illegal activity or violation conducted by the ITMD.

This system also includes investigation case control and management documents that serve as the basis for conducting investigations, such as documents requesting the investigation and documents used in case management control such as case inventories, lead sheets, other tasking documents, and transfer forms; intelligence requirements, analysis, and reporting; operational

records; articles, open source data, and other published information on individuals and events of interest to the ITMD.

Records related to the Department's Insider Threat Program regarding the unauthorized disclosure of sensitive and classified information may include all categories mentioned above, and unclassified and classified insider threat inquiries, investigations and activities; counterintelligence complaints, inquiries and investigations; potential threats to Department resources and information assets; incoming referrals; referrals to internal and external partners; indicator data sets from Department bureaus and operating units; analytical thresholds, triggers, and analysis of records; statistical reports; information collected through information technology records, information assurance, enterprise audit, or continuous evaluation; Department component information and reporting about potential insider threats regarding personnel user names and aliases, levels of network access, audit data, logs and information regarding Department electronic devices; all other documents, reports, and correspondence received, generated or maintained in the course of managing insider threat activities and conducting investigations; and other unclassified and classified insider threat requirements per Executive Order 13587.

Other classified and unclassified files which may not be related to investigative functions and may include legal guidance; U.S. and foreign information and intelligence assessments and reporting; particularly sensitive or protected information, including information held by special access programs, intelligence, law enforcement, inspector general, or other sources or programs; vulnerability, risk, and threat information and assessments; Department acquisition and supply chain risk management information; ITMD budgetary and program management files and metrics; training materials; final versions and drafts of regulations, policies, and laws; employee

travel schedules and foreign travel briefings; other briefing and debriefing statements; certifications pertaining to qualifications for employment, including but not limited to education, firearms, first aid, and CPR; deputation records; Freedom of Information Act and Privacy Act requests, and congressional inquiries to the Office of Security; executive correspondence; hiring actions; contractual agreements and information; nondisclosure agreements; performance evaluations and disciplinary files; payroll data; travel authorization and voucher reports; and documentation related to security controls, internal procedures, and policies.

Authority for Maintenance of the System:

15 U.S.C. 1501 et. seq.; 28 U.S.C. 533–535; 44 U.S.C. 3101 (Records Management); 5 U.S.C. 301 (Departmental Regulations); 5 U.S.C. 7311 (Suitability, Security, and Conduct); 5 U.S.C. 7531-33 (Adverse Actions, Suspension and Removal, and Effect on Other Statutes); 18 U.S.C. (Crimes and Criminal Procedures); Executive Order 10450 (Security Requirements for Government Employment); Executive Order 13526 and its predecessor orders (Classified National Security Information); Executive Order 12968 (Access to Classified Information); HSPD-12, 8/27/04 (Homeland Security Presidential Directive); Executive Order 13356, 8/27/04 (Strengthening the Sharing of Terrorism Information to Protect Americans); Executive Order 13587 (Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information); Public Law 108-458 (Intelligence Reform and Terrorism Prevention Act of 2004); Intelligence Authorization Act for FY 2010, Public Law 111–259; Title 50 U.S.C. 402a, Coordination of Counterintelligence Activities; Executive Order 12829 (National Industrial Security Program); Committee for National Security System Directive 505 (Supply Chain Risk Management); Presidential Memorandum

National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

Purposes:

This system is used by authorized personnel to maintain records that reflect and support the ITMD mission, including various law enforcement and intelligence functions related to identifying, assessing, and/or managing the Department's mission critical security threats.

Threats to the Department's mission include those posed by influential criminal activity; foreign intelligence and security services and non-state actors; terrorism; and extremist groups or unstable persons. Threats also include significant events that may require the Department to take emergency action, such as geopolitical crises, natural disasters, and pandemics.

This system will: manage all matters relating to the storage, facilitation and enabling of documentation of activities associated with proactive and reactive assessments, complaints, inquiries, and investigations; process and house information and intelligence; identify risks, vulnerabilities, and threats to Department and information assets and activities; and track referrals of potential interest to internal and external partners. It will provide a basis for the development and recommendation of solutions to deter, detect, and/or mitigate potential risks, vulnerabilities, and threats identified; provide statistical reports of ITMD actions; and meet other reporting requirements.

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

1. In the event that a system of records maintained by the Department to carry out its functions indicates a violation or potential violation of law or contract, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute or

contract, or rule, regulation, or order issued pursuant thereto, or the necessity to protect an interest of the Department, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, state, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute or contract, or rule, regulation or order issued pursuant thereto, or protecting the interest of the Department.

2. A record from this system of records may be disclosed, as a routine use, to a federal, state or local agency maintaining civil, criminal or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Department decision concerning the assignment, hiring or retention of an individual, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

3. A record from this system of records may be disclosed, as a routine use, to a federal, state, local, or international agency, in response to its request, in connection with the assignment, hiring or retention of an individual, the issuance of a security clearance, the reporting of an investigation of an individual, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

4. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

5. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual when the individual has requested assistance from the Member with respect to the subject matter of the record.
6. A record in this system of records which contains medical information may be disclosed, as a routine use, to the medical advisor of any individual submitting a request for access to the record under the Act and 15 CFR part 4, subpart b, if, in the sole judgment of the Department, disclosure could have an adverse effect upon the individual, under the provision of 5 U.S.C. 552a(f)(3) and implementing regulations at 15 CFR 4.26.
7. A record in this system of records may be disclosed, as a routine use, to the Office of Management and Budget in connection with the review of private relief legislation as set forth in OMB Circular No. A-19 at any stage of the legislative coordination and clearance process as set forth in that Circular.
8. A record in this system of records may be disclosed, as a routine use, to the Department of Justice in connection with determining whether disclosure thereof is required by the Freedom of Information Act (5 U.S.C. 552).
9. A record in this system of records may be disclosed, as a routine use, to a contractor of the Department having need for the information in the performance of the contract, but not operating a system of records within the meaning of 5 U.S.C. 552a(m).
10. A record in this system may be transferred, as a routine use, to the Office of Personnel Management: for personnel research purposes; as a data source for management information; for the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained; or for related manpower studies.

11. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services Administration (GSA), or his designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e. GSA or Department) directive. Such disclosure shall not be used to make determinations about individuals.

12. A record in this system of records may be disclosed to appropriate agencies, entities and persons when: (1) it is suspected or determined 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 whether systems or programs (whether maintained by the Department 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 the Department's efforts to respond to the suspected or confirmed compromise and to prevent, minimize, or remedy such harm.

13. A record in this system of records may be disclosed to any other agency or department of the Federal Government pursuant to statutory intelligence responsibilities.

14. A record in this system of records may be disclosed to any Federal, state, municipal, foreign or international law enforcement or other relevant agency or organization for law enforcement or counterterrorism purposes: threat alerts and analyses, protective intelligence and counterintelligence information, information relevant for screening purposes, and other law

enforcement and terrorism-related information as needed by appropriate agencies of the Federal government, states, or municipalities, or foreign or international governments or agencies.

15. A record in this system of records may be disclosed to any Federal agency following a response to its subpoena or to a prosecution request that such record be released for the purpose of its introduction to a grand jury.

16. A record from this system of records may be disclosed, as a routine use, to representatives of the Department of Justice (DOJ) or of any other agency that is responsible for representing Department interests in connection with judicial, administrative or other proceedings. This includes circumstances in which (1) the ITMD; (2) any employee of the ITMD in his or her official capacity; (3) any employee of the ITMD in his or her individual capacity, where DOJ has agreed to represent or is considering a request to represent the employee; or (4) the United States or any of its components, is a party to pending or potential litigation or has an interest in such litigation; in which the Department or the ITMD is likely to be affected by the litigation, or in which the Department or the ITMD determines that the use of such records by the DOJ is relevant and necessary to the litigation; provided, however, that in each case, the Department or the ITMD determines that disclosure of records to the DOJ or representative is a use of the information that is compatible with the purpose for which the records were collected.

17. Records may also be disclosed to representatives of DOJ and other U.S. Government entities, to the extent necessary, to obtain their advice on any matter relevant to an ITMD investigation.

18. A record in this system of records may be disclosed, as a routine use, to any source from which additional information is requested, either private or governmental, to the extent necessary to solicit information relevant to any investigation or inquiry.

19. A record in this system of records may be disclosed, as a routine use, to representatives of the Office of Personnel Management, the Office of Special Counsel, the Merit Systems Protection Board, the Federal Labor Relations Authority, the Equal Employment Opportunity Commission, the Office of Government Ethics, and other Federal agencies in connection with their efforts to carry out their responsibilities to conduct examinations, investigations, and/or settlement efforts, in connection with administrative grievances, complaints, claims, or appeals filed by an employee, and such other functions promulgated in 5 U.S.C. 1205-06.

20. A record in this system of records may be disclosed, as a routine use, to the Departments of the Treasury and Justice in circumstances in which ITMD seeks to obtain, or has in fact obtained, an ex parte court order to obtain tax return information from the Internal Revenue Service.

21. A record in this system of records may be disclosed, as a routine use, to appropriate Congressional Committees in furtherance of their respective oversight functions.

22. A record in this system of records may be disclosed, as a routine use, to student volunteers, individuals working under a personal services contract, and other workers who technically do not have the status of Federal employees, when they are performing work for the Department of Commerce and/or its agencies, as authorized by law, as needed to perform their assigned Agency functions.

Disclosure to consumer reporting agencies:

Not applicable.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of

Records in the System:

Storage:

Records in this system are on paper and/or in digital or other electronic form. Paper records are stored in secure rooms and storage cabinets or safes, and electronic records are stored as electronic/digital media and stored in secure file-servers within controlled environments. Both paper and electronic/digital records are accessed only by authorized personnel.

Retrievability:

Electronic searches may be performed by search criteria that include case numbers, names of individuals or organizations, Department-assigned identifier, and other key word search variations. Paper records are retrieved by indices cross-referenced to file numbers or other identifiers.

Safeguards:

Paper records are kept in locked cabinets located in secure rooms in guarded buildings, and used only by authorized screened personnel. Access to computerized files is password-protected and under the direct supervision of the system manager and is available only within the secure, access controlled rooms by authorized personnel.

Retention and Disposal:

Retention of the records varies depending upon the specific kind of record involved. The records are retired or destroyed in accordance with current published records schedules of the Department of Commerce and as approved by the National Archives and Records Administration.

System Manager(s) and Address:

The ITMD and Departmental Classified System Owners, depending on type of record, located at the Herbert C. Hoover Building, Washington, DC 20230.

Notification Procedure:

An individual requesting notification of existence of records on himself or herself should send a signed, written inquiry to the Deputy Chief FOIA Officer and Department Privacy Act Officer, Room 52010, U.S. Department of Commerce, 1401 Constitution Avenue NW., Washington, DC 20230.

Record Access Procedures:

An individual requesting access to records on himself or herself should send a signed, written inquiry to the same address as stated in the Notification Procedure section above. The request letter should be clearly marked, “PRIVACY ACT REQUEST.” The written inquiry must be signed and notarized or submitted with certification of identity under penalty of perjury.

Requesters should specify the record contents being sought.

Contesting Record Procedures:

An individual requesting corrections or contesting information contained in his or her records must send a signed, written request inquiry to the same address as stated in the Notification Procedure section above. Requesters should reasonably identify the records, specify the information they are contesting and state the corrective action sought and the reasons for the correction with supporting justification showing how the record is incomplete, untimely, inaccurate, or irrelevant. The Department’s rules for access, for contesting contents, and for appealing initial determination by the individual concerned appear in 15 CFR part 4, Appendix B.

Record Source Categories:

Subject individuals; other Department of Commerce operating units; OPM, FBI and other Federal, state and local agencies; individuals and organizations that have pertinent knowledge about the subject; and those authorized by the individual to furnish information.

These records may contain information obtained from the individual; persons having knowledge of the individual; persons having knowledge of incidents or other matters of investigative interest to the Department; other U.S. law enforcement agencies and court systems; pertinent records of other Federal, state, or local agencies or foreign governments; pertinent records of private firms or organizations; the intelligence community; and other public sources. The records also contain information obtained from interviews, review of records, and other authorized investigative techniques.

System Exemptions from Certain Provisions of the Act:

Pursuant to 5 U.S.C. 552a(j)(2), all information about an individual in the record which meets the criteria stated in 5 U.S.C. 552a(j)(2) are exempted from the notice, access and contest requirements of the agency regulations and from all parts of 5 U.S.C. 552a except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i). Pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and (k)(5) on condition that the 5 U.S.C. 552a(j)(2) exemption is held to be invalid, all investigatory material in the record which meets the criteria stated in 5 U.S.C. 552a(k)(1), (k)(2) and (k)(5) are exempted from the notice, access, and contest requirements (under 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f)) of the agency regulations because of the necessity to exempt this information and material in order to accomplish the law enforcement function of the agency, to prevent disclosure of classified information as required by Executive Order 13526, to assure the protection of the President, to prevent subjects of investigation from frustrating the investigatory process, to prevent the disclosure of investigative techniques, to fulfill commitments made to protect the confidentiality of information, and to avoid endangering these sources and law enforcement personnel.

Michael J. Toland
Department of Commerce
Deputy Chief FOIA Officer
Department Privacy Act Officer

[FR Doc. 2016-31315 Filed: 12/30/2016 4:15 pm; Publication Date: 1/4/2017]