DEPARTMENT OF TRANSPORTATION

Office of the Secretary

Docket No. OST-2018-0128

Privacy Act of 1974; Department of Transportation, Office of the Secretary of Transportation; DOT/ALL 26; Department of Transportation Insider Threat Program

AGENCY: Office of the Departmental Chief Information Officer, Office of the Secretary of Transportation, DOT.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Transportation (DOT) intends to establish a system of records titled, "DOT/ALL 26, Insider Threat Program." This system of records will allow DOT to administer an insider threat program, including identification of potential external foreign intelligence risks and insider threats, and to maintain information regarding counterintelligence or insider threat inquiries. This system will be included in the Department of Transportation's inventory of record systems.

DATES: Written comments should be submitted on or before [INSERT DATE 30 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER] The Department may publish an amended SORN in light of any comments received. This new system will take effect [INSERT DATE 30 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number OST-2018-0128 by any of the following methods:

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

- Mail: Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Ave. SE., West Building Ground Floor, Room W12–140, Washington, DC 20590–0001.
- Hand Delivery or Courier: West Building Ground Floor, Room W12–140, 1200 New Jersey Ave. SE., between 9 a.m. and 5 p.m. ET, Monday through Friday, except Federal Holidays.
- Fax: (202) 493–2251.

Instructions: You must include the agency name and docket number OST-2018-0128. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Privacy Act: Anyone is able to search the electronic form of all comments received in any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's system of records notice for dockets in the Federal Register notice published on January 17, 2008 (73 FR 3316-3317).

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* or to the street address listed above. Follow the online instructions for accessing the docket.

FOR FURTHER INFORMATION CONTACT: For questions, please contact: Claire W. Barrett, Departmental Chief Privacy Officer, Privacy Office, Department of Transportation, Washington, D.C. 20590; privacy@dot.gov; or (202) 366-8135.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the United States Department of Transportation (DOT) proposes to create a new DOT system of records titled, "DOT/ALL-26 Insider Threat Program." This system of records is created as a DOT/ALL system because records are maintained for this program by the Office of the Secretary (OST) and the Federal Aviation Administration (FAA), two DOT components. This system of records notice only applies to records maintained by the Office of the Secretary and the Federal Aviation Administration's Insider Threat Programs. There are no other components within DOT authorized to administer an insider threat program. The term "DOT Insider Threat Program" refers to the insider threat program administered by both OST and the FAA.

Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, directs Federal departments and agencies to establish insider threat programs consistent with guidance and standards developed by the National Insider Threat Task Force, which was established under section 6 of Executive Order 13587. The National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs were issued in November 2012. As described in Executive Order 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, insider threat programs are intended to deter and detect insider threats and mitigate the risks associated with an individual using his or her authorized access to Government information and facilities to do harm to the security of the United States. This insider threat may include espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of Government resources or capabilities. The DOT Insider Threat Program will adhere to Executive Order 13587 and the National Insider

Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, and will include protocols for reporting and responding to potential or suspected insider threat activity. The DOT Insider Threat Program applies to all DOT Operation Administrations and Secretarial Offices, and to all DOT employees who have access to classified systems (as defined in Executive Order 13587), as well as to controlled unclassified information or information systems, as determined by DOT. For the purposes of the DOT Insider Threat Program, Executive Order 12968 defines "employee" as "a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency," as determined by the Secretary of Transportation or, for the FAA, the FAA Administrator. This definition includes interns and students. A licensee, certificate holder (such an airman), or grantee who is not also a DOT employee is generally excluded from the DOT Insider Threat Program; however, such an individual may be included if a determination is made that the nature and extent of that individual's access to DOT personnel, facilities, equipment, systems, networks, operations, and information necessitates their inclusion.

Per DOT Order 1642.1, the Department's Defensive Counterintelligence and Insider Threat Program Manager within the Office of the Secretary oversees the collection, analysis, and reporting of information across DOT, including FAA, to support the identification and assessment of insider threats. Subject to this oversight, OST administers the DOT Insider Threat Program for all DOT Operating Administrations except the FAA, which administers the DOT Insider Threat Program for itself.

The DOT Insider Threat Program will maintain information about employees who demonstrate indicia of potential insider threats. Indicia of potential insider threats may be identified to the DOT Insider Threat Program through referrals or the Insider Threat Program office's review/analysis of DOT information assets (together, referred to as "reports"). Reports of potential insider threats can come from a variety of sources, including other Federal agencies, DOT employees, and Insider Threat program staff. The DOT Insider Threat Program will review reports in accordance with established DOT and FAA Insider Threat Program management policy and procedures, as applicable. Based on this review, an appropriate authorized OST or FAA official will determine whether to proceed with an insider threat inquiry, refer the matter to appropriate law enforcement officials, close the matter, or take other appropriate action. Insider threat inquiries will be comprised primarily of existing DOT information assets including, but not limited to, records from information security, personnel security, and human resources; and may include information obtained from other Federal agencies or from publicly available resources (such as internet searches). The DOT Insider Threat Program records also will be used to track reports of indicia of potential insider threats, whether or not an inquiry was opened; the rationale for opening or not opening an inquiry; the disposition of all inquiries, and referrals to law enforcement (such as the DOT Office of the Inspector General or the Federal Bureau of Investigation); and to report on DOT's Insider Threat Program activities.

In addition to the General Routine Uses applicable to all DOT systems of records, the Department may disclose information from this system to third parties, only to the extent necessary and relevant to an insider threat inquiry conducted by DOT or FAA. The DOT also may disclose information from this system to other Federal agencies, when necessary and relevant to an insider threat inquiry conducted by that Federal agency. These routine uses are

compatible with the purposes for which the information was collected because individuals who have authorized access to classified or controlled unclassified information are aware that the Federal Government must take steps, such as sharing information with other Federal agencies, when necessary to obtain additional information relevant to the subject matter of an insider threat inquiry. It must also protect these assets from unauthorized access, use, and disclosure, including regularly evaluating/re-evaluating individuals' suitability for employment and for access to classified or sensitive but unclassified information and information systems.

This new system will be included in DOT's inventory of record systems.

II. Privacy Act

The Privacy Act (5 U.S.C. 552a) governs the means by which the Federal Government collects, maintains, and uses personally identifiable information (PII) in a System of Records. A ''System of Records'' is a group of any records under the control of a Federal agency from which information about individuals is retrieved by name or other personal identifier. The Privacy Act requires each agency to publish in the **Federal Register** a System of Records notice (SORN) identifying and describing each System of Records the agency maintains, including the purposes for which the agency uses PII in the system, the routine uses for which the agency discloses such information outside the agency, and how individuals to whom a Privacy Act record pertains can exercise their rights under the Privacy Act (e.g., to determine if the system contains information about them and to contest inaccurate information).

In a notice of proposed rulemaking, which will be published separately in the Federal Register, the Department is proposing exempting this system from certain provisions of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2).

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

SYSTEM NAME AND NUMBER:

Department of Transportation (DOT)/ALL – 26, Insider Threat Program

SECURITY CLASSIFICATION:

Most of the records in this system are unclassified or controlled unclassified information; however, the system also may include records that are classified.

SYSTEM LOCATION:

Records are maintained in the DOT, Office of the Secretary, and Federal Aviation Administration at their headquarters in Washington, D.C.

SYSTEM MANAGERS:

DOT, Office of Intelligence, Security and Emergency Response, 1200 New Jersey Ave, SE, Washington, D.C. 20590.

FAA, Assistant Administrator for Security and Hazardous Materials Safety, 800 Independence Avenue, SW., Washington, DC 20591.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 3381 (section 811 of the Intelligence Authorization Act for Fiscal Year 1995); Executive Order 10450, Security Requirements for Government Employment (April 17, 1953); Executive Order 12444; Executive Order 10865, Safeguarding Classified Information within Industry (Jan. 7, 1961); Executive Order 12829, National Industrial Security Program (Jan. 6, 1993); Executive Order 12968, Access to Classified Information (Aug. 2, 1995); Executive Order 13567, 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 (Jan. 16, 2009); Executive Order 13526, Classified National Security Information (Jan. 5, 2010); Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 7, 2011); 49 U.S.C. 40113, 49 USC 44701(a)(5).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to receive and respond to reports of potential insider threats, manage and track insider threat inquiries and law enforcement referrals, and identify potential insider threats to DOT information assets.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former DOT employees, including contractors, subcontractors, experts, consultants, licensees, certificate holders, grantees, interns, students, or any other category of person who acts on behalf of DOT and has authorized access to classified or controlled unclassified information, as determined by the Secretary of Transportation or Administrator of the Federal Aviation Administration.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in the system will include reports of indicia of insider threat activity, and information relevant and necessary to DOT's evaluation of those reports and the conduct of an insider threat inquiry. These records may include information obtained from DOT Operating Administrations, other Federal agencies, or publicly available sources, including, but not limited to, personnel security records, administrative adjudication records, regulatory records, incident reports, personnel records, network or building access records, identification media records, law

enforcement records, financial records, and travel records. Information derived from these record sources may include full name; former names/aliases; date and place of birth; social security number; hair and eye color; ethnicity and race; gender; biometric data; mother's maiden name; current and former home and work addresses, phone numbers, and email addresses; employment history; military history; education history; criminal history; court actions; credit reports; financial information, including financial disclosure filings; personnel security adjudications and eligibility decisions; spouse, cohabitant, or relative names, dates and places of birth, social security numbers, and citizenship information; foreign contacts and activities; travel records or briefings; polygraph examination reports; document control registries; facility access records; security violation files; and requests for access to classified information. This system also includes reports of indicia of potential insider threats and counterintelligence referrals, insider threat inquiry reports, and referrals to law enforcement.

RECORD SOURCE CATEGORIES:

Records are obtained from existing DOT record systems, publicly-available sources, Federal agencies, DOT employees, or individuals who are the subject of such 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 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 DOT as a routine use pursuant to 5 U.S.C. 552a(b)(3):

(1) To third parties only to the extent necessary and relevant to a DOT or FAA insider threat inquiry;

(2) To any Federal agency with responsibilities for activities related to counterintelligence or the detection of insider threats, for the purpose of conducting such activities;

DOT General Routine Uses

(3) To the appropriate agency, whether Federal, State, local, or foreign, charged with the responsibility of implementing, investigating, prosecuting, or enforcing a statute, regulation, rule or order, when a record in this system indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, including any records from this system relevant to the implementation, investigation, prosecution, or enforcement of the statute, regulation, rule, or order that was or may have been violated;

(4) 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 for DOT to obtain information relevant to a DOT decision concerning the hiring or retention or an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit;

(5) To a Federal agency, upon its request, in connection with the requesting Federal agency's hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation or an employee, 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 requested is relevant and necessary to the requesting agency's decision on the matter;

(6) To the Department of Justice, or any other Federal agency conducting litigation, when (a) DOT, (b) any DOT employee, in his/her official capacity, or in his/her individual capacity if the Department of Justice has agreed to represent the employee, or (c) the United States or any agency thereof, is a party to litigation or has an interest in litigation,

and DOT determines that the use of the records by the Department of Justice or other Federal agency conducting the litigation is relevant and necessary to the litigation; provided, however, that DOT determines, in each case, that disclosure of the records in the litigation is a use of the information contained in the records that is compatible with the purpose for which the records where collected.

(7) To parties in proceedings before any court or adjudicative or administrative body before which DOT appears when (a) DOT, (b) any DOT employee in his or her official capacity, or in his or her individual capacity where DOT has agreed to represent the employee, or (c) the United States or any agency thereof is a party to litigation or has an interest in the proceeding, and DOT determined that is relevant and necessary to the proceeding; provided, however, that DOT determines, in each case, that disclosure of the records in the proceeding is a use of the information contained in the records that is compatible with the purpose for which the records where collected.

(8) To the Office of Management and Budget (OMB) in connection with the review of privacy relief legislation as set forth in OMB Circular A-19 at any stage of the legislative coordination and clearance process set forth in that Circular.

(9) To the National Archives and Records Administration for an inspection under 44 U.S.C. 2904 and 2906.

(10) To another agency or instrumentality of any government jurisdiction for use in law enforcement activities, either civil or criminal, or to expose fraudulent claims; however, this routine use only permits the disclosure of names pursuant to a computer matching program that otherwise complies with the requirements of the Privacy Act.

(11) To the Attorney General of the United States, or his/her designee, information indicating that a person meets any of the disqualifications for receipt, possession, shipment, or transport of a firearm under the Brady Handgun Violence Prevention Act. In case of a dispute concerning the validity of the information provided by DOT to the Attorney General (or designee), it shall be a routine use of the information in this system to make any disclosures of such information to the National Background Check System, established by the Brady Handgun Violence Prevention Act, as may be necessary to resolve such dispute.

(12) To appropriate agencies, entities, and persons, when (1) DOT suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DOT 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 DOT or not) that rely on the compromised information; and (3) the disclosure made to such agencies, entities, or persons is reasonably necessary to assist in connection with DOT's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(13) To the Office of Government Information Services (OGIS) for the purpose of resolving disputes between requesters seeking information under the Freedom of Information Act (FOIA) and DOT, or OGIS' review of DOT's policies, procedures, and compliance with FOIA.

(14) To DOT's contractors and their agents, DOT's experts, consultants, and others performing or working on a contract, service, cooperative agreement, or other assignment

for DOT, when necessary to accomplish an agency function related to this system of records.

(15) To an agency, organization, or individual for the purpose of performing an audit or oversight related to this system or records, provided that DOT determines the records are necessary and relevant to the audit or oversight activity. This routine use does not apply to intra-agency sharing authorized under Section (b)(1) of the Privacy Act.

(16) To a Federal, State, local, tribal, foreign government, or multinational agency, either in response to a request or upon DOT's initiative, terrorism information (6 U.S.C. 485(a)(5), homeland security information (6 U.S.C. 482(f)(1), or law enforcement information (Guideline 2, report attached to White House Memorandum, "Information Sharing Environment," Nov. 22, 2006), when DOT finds that disclosure of the record is necessary and relevant to detect, prevent, disrupt, preempt, or mitigate the effects of terrorist activities against the territory, people, and interests of the United States, as contemplated by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-456, and Executive Order 13388 (Oct. 25, 2005).

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS

Records in this system are stored electronically and/or on paper in secure facilities.

POLICIES AND PRACTICES FOR RETREIVEAL OF RECORDS:

Records may be retrieved by individual's name or DOT- or FAA-assigned case number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records in this system are covered by National Archives and Records Administration Schedule 5.6, items 230 and 240. Records determined to be associated with an insider threat or to have potential to be associated with an insider threat are destroyed 25 years after the date the threat was discovered, but a longer retention is authorized if required for business use. User attributed data collected to monitor user activities on a network to enable insider threat programs and activities to support authorized inquiries and investigations, is destroyed five years after an inquiry was opened, but a longer retention period is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DOT 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 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.

RECORD ACCESS PROCEDURES:

Individual seeking access to records in this system of records should follow the procedures described in the section "Notification procedure" below.

CONTESTING RECORD PROCEDURES:

Individuals seeking amendment to the records in this system of records should follow the procedures described in the section "Notification procedure" below.

NOTIFICATION PROCEDURES:

The Secretary of Transportation has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it may contain classified information, and

includes allegations and inquiries about potential unauthorized disclosure of classified or controlled unclassified information in violation of federal law. However, DOT/FAA will consider individual requests to determine whether or not the information requested may be released. Thus, individuals who seek notification of and access to any record contained in this system, or who seek to contest its content, may submit a request for such information to the DOT or FAA. Individuals seeking access to records in this system maintained by the DOT Insider Threat Program should submit a request to the DOT or FAA System Manager identified at the address listed under "System Manager and Address," above.

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 49 CFR Part 10. 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. 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.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

This system contains classified and unclassified records that are exempt from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2): (c)(3), (d), (e)(1), (e)(4)(G)-(I), and (f).

HISTORY

This is a new system of records.

Claire W. Barrett

Departmental Chief Privacy Officer

[FR Doc. 2018-21441 Filed: 10/2/2018 8:45 am; Publication Date: 10/3/2018]