9110-05

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2018-0017]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security, Transportation Security Administration.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/Transportation Security Administration-001 Transportation Security Enforcement Record System System of Records." This system of records allows DHS/Transportation Security Administration (TSA) to collect and maintain records related to the TSA's screening of passengers and property, as well as records related to the investigation or enforcement of transportation security laws, regulations, directives, or Federal, State, local, or international law. For example, records relating to an investigation of a security incident that occurred during passenger or property screening would be covered by this system. DHS is updating this system of records notice to cover records relating to the TSA Insider Threat program, modify the category of individuals and category of records, reflect an approved records retention schedule for records covered by this system, and modify two existing routine uses. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. The existing Privacy Act exemptions for this system of records will continue to apply.

This modified system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. This modified system will be effective upon publication. New or modified routine uses for this modified system of records 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-2018-0017 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: Philip S. Kaplan, 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 DHS-2018-0017. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Peter Pietra, TSAPrivacy@tsa.dhs.gov, Privacy Officer, Transportation Security Administration, 701 South 12th Street, Arlington, VA 20598-6036. For privacy questions, please contact: Philip S. Kaplan, Privacy@hq.dhs.gov, (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. sec. 552a, DHS/TSA proposes to modify and reissue a current DHS system of records notice (SORN) titled, "DHS/TSA-001 Transportation Security Enforcement Record System System of Records."

This modification more clearly identifies that this SORN contains records relating to the TSA Insider Threat program. In furtherance of TSA's responsibility for security in all modes of transportation and to ensure the adequacy of security measures at airports and other transportation facilities pursuant to its establishing legislation, the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71, 49 U.S.C. sec. 114(d) and (f), provides authority for TSA to establish its Insider Threat program in order to deter, detect, and mitigate insider threats to TSA's personnel, operations, information, critical infrastructure, and transportation sectors subject to TSA authorities. For purposes of this TSA system of records, "insider threats" are, or present themselves to be, current or former transportation sector workers (including both TSA and private sector personnel) and individuals employed or otherwise engaged in providing services requiring authorized access to transportation facilities, assets, or infrastructure who intend to cause harm to the transportation domain.

This system of records is being modified to: cover records relating to the TSA's Insider Threat program; include a new category of individuals and category of records; reflect an approved records retention schedules for records covered by this system; and change existing routine uses. The category of individuals covered under this SORN will

be modified to reflect that the system may contain information on both current and former owners, operators, and employees in all modes of transportation for which DHS/TSA has security-related duties; and will also cover individuals who have access to Sensitive Security Information (SSI) and are "covered persons" under the Sensitive Security Information regulation, 49 CFR Part 1520.7. The category of records in this SORN will be modified to include place of birth; Government-issued identification; citizenship; results of any law enforcement, criminal history record, or open source checks; employment information and work history; and security and access clearances and background investigation information. This SORN also reflects that the applicable records retention schedules are approved by the National Archives and Records Administration (NARA). This SORN modifies routine uses "E" and "F" to be in conformity with Office of Management and Budget Memorandum M-17-12. This SORN also combines two previous routines uses into one routine use "K" regarding the sharing of information relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual or issuance of a credential or clearance. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Consistent with DHS's information sharing mission, information covered by DHS/TSA-001 Transportation Security Enforcement Record System 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, TSA may share information with appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies consistent with any

applicable laws, rules, regulations, and information sharing and access agreements or arrangements, and as permitted pursuant to an applicable Privacy Act authorized disclosure, including routine uses set forth in this system of records notice.

As stated above, this modified system of records will rely on an existing rule for exempting TSA from certain provisions of the Privacy Act pursuant to 5 U.S.C. secs. 552a(j)(2), (k)(1), and (k)(2). These exemptions are reflected in the final rule published on August 4, 2006, in 71 FR 44223. This modified system will be included in DHS's 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. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/TSA-001 Transportation Security Enforcement Record System System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS 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 Homeland Security (DHS) Transportation Security Administration (TSA)-001 Transportation Security Enforcement Record System System of Records.

SECURITY CLASSIFICATION: Classified, sensitive.

SYSTEM LOCATION: Records are maintained at the TSA Headquarters offices, 601 South 12th Street, Arlington, Virginia,20598 and at various TSA field offices.

SYSTEM MANAGER(S): Information Systems Program Manager, IT_System_owner@tsa.dhs.gov, Office of Information Technology, TSA Headquarters, TSA-11, 601 South 12th Street, Arlington, VA 20598.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 49 U.S.C. sec. 114(d), 44901, 44903, 44916, 46101, and 46301.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to maintain an enforcement and inspections system for all modes of transportation for which TSA has security-related duties and to maintain records related to the investigation or prosecution of violations or potential violations of Federal, State, local, or international criminal law. They may be used, generally, to identify, review, analyze, investigate, and prosecute violations or potential violations of transportation security laws, regulations, and directives or other laws as well as to identify and address potential threats to transportation security. They may also be used to record the details of TSA security-related activity, such as passenger or property screening.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Current and former owners, operators, and employees, including TSA personnel, in all modes of transportation for which DHS/TSA has security-related duties; individuals reported or investigated as insider threat risks (that is, individuals who are, or present themselves to be, current or former transportation sector workers (including both TSA and private sector personnel) and individuals employed or otherwise engaged in providing services requiring authorized access to transportation facilities, assets, or infrastructure who intend to cause harm to the transportation domain); individuals who have access to SSI and are "covered persons" under the Sensitive Security Information regulation, 49 CFR Part 1520; witnesses and other third parties who provide information; individuals undergoing screening of their person (including identity verification) or property; individuals against whom investigative, administrative, or civil or criminal enforcement action has been initiated for violation of certain TSA regulations or security directives, relevant provisions of 49 U.S.C. sec. 449, or other laws; and individuals who communicate security incidents, potential security incidents, or otherwise suspicious activities.

CATEGORIES OF RECORDS IN THE SYSTEM: Information related to the screening of property and the security screening and identity verification of individuals, including identification media and identifying information such as:

- Individual's name;
- Address;
- Date and place of birth;
- Gender;
- Contact information (e.g., email addresses, phone numbers);

- Social Security number;
- Government-issued identification (e.g., Passport information, Driver's License number, Alien Registration number);
- Citizenship;
- Fingerprints or other biometric identifiers;
- Physical description, photographs or video;
- Travel information or boarding passes;
- Results of any law enforcement, criminal history record, intelligence, immigration, public records or open source checks;
- Military status (branch, traveling on orders);
- Employment information and work history;
- Security and access clearances and background investigations information.
- TSA Information technology network activity information; and
- Information from other agencies (e.g., FBI, Financial Crimes Enforcement Network (FinCEN)).

Additionally, information related to the investigation or prosecution of any alleged violation; place of violation; Enforcement Investigative Reports (EIR); security incident reports, screening reports, suspicious-activity reports, and other incident or investigative reports; statements of alleged violators, witnesses, and other third parties who provide information; proposed penalty; investigators' analyses and work papers; enforcement actions taken; findings; documentation of physical evidence; correspondence of TSA employees and others in enforcement cases; pleadings and other court filings; legal

opinions and attorney work papers; and information obtained from various law enforcement or prosecuting authorities relating to the enforcement of laws or regulations.

RECORD SOURCE CATEGORIES: Records are obtained from the alleged violator, TSA employees or contractors, witnesses to the alleged violation or events surrounding the alleged violation, other third parties who provided information regarding the alleged violation, State and local agencies, and other Federal agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 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. sec. 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/her official capacity;

3. Any employee or former employee of DHS in his/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 pursuant to records management inspections being conducted under the authority of 44 U.S.C. sec. 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 there has been a breach of this system of records; and (2) DHS has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, harm to DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity when DHS determines that information from this system of records is reasonably necessary to assist another Federal recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. 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.

H. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, 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.

I. To the United States Department of Transportation, its operating administrations, or the appropriate State or local agency, when relevant or necessary to:

1. Ensure safety and security in any mode of transportation;

2. Enforce safety- and security-related regulations and requirements;

3. Assess and distribute intelligence or law enforcement information related to transportation security;

4. Assess and respond to threats to transportation;

5. Oversee the implementation and ensure the adequacy of security measures at airports and other transportation facilities;

6. Plan and coordinate any actions or activities that may affect transportation safety and security or the operations of transportation operators; or

7. Issue, maintain, or renew a license, certificate, contract, grant, or other benefit.

J. To the appropriate Federal, State, local, tribal, territorial, foreign, or international agency, regarding individuals who pose, or are suspected of posing, a risk to transportation or national security.

K. To federal, state, local, tribal, territorial, foreign, or international agencies, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or the issuance, grant, renewal, suspension, or revocation of a security clearance, license, contract, grant, or other benefit; or to the extent necessary to obtain information relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit.

L. To international and foreign governmental authorities in accordance with law and formal or informal international agreement.

M. To third parties during the course of an investigation into any matter before DHS/TSA to the extent necessary to obtain information pertinent to the investigation.

N. To airport operators, aircraft operators, and maritime and surface transportation operators, indirect air carriers, and other facility operators about individuals who are their employees, job applicants, or contractors, or persons to whom they issue identification credentials or grant clearances to secured areas in transportation facilities when relevant to such employment, application, contract, or the issuance of such credentials or clearances.

O. To any agency or instrumentality charged under applicable law with the protection of the public health or safety under circumstances in which the public health or safety is at risk.

P. With respect to members of the armed forces who may have violated transportation security or safety requirements and laws, to disclose the individual's identifying information and details of their travel on the date of the incident in question to the appropriate branch of the armed forces to the extent necessary to determine whether the individual was performing official duties at the time of the incident. Members of the armed forces include active duty and reserve members, and members of the National Guard. This routine use is intended to permit TSA to determine whether the potential violation must be referred to the appropriate branch of the armed forces for action pursuant to 49 U.S.C. sec. 46301(h).

Q. To the DOJ, U.S. Attorney's Office, or other Federal agencies for further collection action on any delinquent debt when circumstances warrant.

R. To a debt collection agency for the purpose of debt collection.

S. To airport operators, aircraft operators, air carriers, maritime, and surface transportation operators, indirect air carriers, or other facility operators when appropriate to address a threat or potential threat to transportation security or national security, or when required for administrative purposes related to the effective and efficient administration of transportation security laws.

T. To a former employee of DHS, in accordance with applicable regulations, for purposes of responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority; or facilitating communications with a former

employee that may be necessary for personnel-related or other official purposes where the Department requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

U. To a court, magistrate, or administrative tribunal when a Federal agency is a party to the litigation or administrative proceeding in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in connection with criminal law proceedings.

V. To the public, on the TSA website at www.tsa.gov, final agency and Administrative Law Judge decisions in criminal enforcement and other administrative matters, except that personal information about individuals will be deleted if release of that information would constitute an unwarranted invasion of privacy, including but not limited to medical information.

W. 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's 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 a clearly unwarranted invasion of personal privacy.

X. To the appropriate Federal, State, local, tribal, territorial, foreign, or international agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, order, license, or treaty, when DHS/TSA determines that the information would assist in the enforcement of a civil or criminal law.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/TSA 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.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/TSA retrieves records by name, address, Social Security number, administrative action or legal enforcement numbers, or other assigned identifier of the individual on whom the records are maintained.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Retention and disposal varies depending on the type of record. Passenger, baggage, and cargo screening incident reports that are not referred for investigation are maintained for three years from the end of the fiscal year in which they were created, in accordance with NARA authority, N1-560-12-002. Security incident reports are cut off at the end of involvement and destroyed four years after cut-off (N1-560-03-6). Items that are referred for investigation within TSA or to an outside agency are destroyed 25 years after the case is closed (N1-560-03-6). Insider Threat information and inquiry records are destroyed no sooner than five years after an inquiry is opened and 25 years after a case is closed, in accordance with NARA authority DAA-GRS-2017-0006.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/TSA safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. TSA 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.

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/TSA will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of 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 and the TSA Freedom of Information Act (FOIA) Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts Information." 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 FOIA Officer, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under FOIA.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify your identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign his/her request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for

notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief FOIA Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believes the Department would have information on him/her;
- Identify which component(s) of the Department the individual believes may have the information about him/her;
- Specify when the individual believes 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 an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second 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 the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any

documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES: See "Record Access Procedures."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(j)(2), has exempted portions of this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(3), (e)(4)(G), (H), and (I); and (f). Portions of the system pertaining to investigations or prosecutions of violations of criminal law are exempt under 5 U.S.C. sec. 552a(j)(2). Further, the Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(k)(1) and (k)(2), has exempted portions of this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (H), and (I); and (f).

HISTORY: 78 FR 73868 (Dec. 9, 2013); 75 FR 28042 (May 19, 2010); 71 FR 44223 (Aug. 4, 2006).

Philip S. Kaplan,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2018-18558 Filed: 8/27/2018 8:45 am; Publication Date: 8/28/2018]