9110-05-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2013-0079]

Privacy Act of 1974; Department of Homeland Security Transportation Security Administration - DHS/TSA-001 Transportation Security Enforcement Record System System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records Update.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled, "Department of Homeland Security/Transportation Security Administration - DHS/TSA-001 Transportation Security Enforcement Record System System of Records." This system of records allows the Department of Homeland Security/Transportation Security Administration to collect and maintain records related to the Transportation Security Administration'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. As a result of a biennial review of this system, records have been updated within the routine uses. Specifically, the statute citation in routine use P. has been corrected. This notice is being re-issued in its entirety

in order to have a single updated record available for public review. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This updated system will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2013-0079 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Peter Pietra, Privacy Officer, Privacy Policy and Compliance, TSA-36, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598-6036; e-mail: TSAPrivacy@dhs.gov. For privacy questions, please contact: Karen L. Neuman, (202)

343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS) Transportation Security Information (TSA) proposes to update and reissue a current DHS system of records titled, "DHS/TSA-001 Transportation Security Enforcement Record System (TSERS) System of Records."

As a result of a biennial review of this system, records have been updated within the routine uses. The statute citation in routine use P. has been corrected to 49 U.S.C. § 46301(h).

TSA's mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. To achieve this mission, TSA is required to develop and adapt its security programs to respond to evolving threats to transportation security.

Consistent with DHS' information-sharing mission, information stored in the DHS/TSA-001 TSERS 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, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Portions of this system are exempt under 5 U.S.C. §§ 552a(k)(1) and (k)(2). Portions of the system pertaining to investigations or prosecutions of violations of criminal law are exempt under 5 U.S.C. § 552a(j)(2). These exemptions are reflected in the final rule published on August 4, 2006 in 71 FR 44223.

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

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/TSA-001 TSERS System of Records.

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

System of Records:

Department of Homeland Security (DHS)/Transportation Security Administration (TSA) - 001

System name:

DHS/TSA-001 Transportation Security Enforcement Record System (TSERS)

Security classification:

Classified, sensitive.

System location:

Records are maintained at TSA Headquarters offices in Arlington, Virginia, and at various TSA field offices.

Categories of individuals covered by the system:

Owners, operators, and employees in all modes of transportation for which DHS/TSA has security-related duties; 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. Chapter 449, or other laws; individuals being investigated or prosecuted for violations of law; 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 of birth;
- Gender;
- Contact information (e.g., email addresses, phone numbers);
- Social Security Number
- Fingerprints or other biometric identifiers;
- Photographs or video; and
- Travel information or boarding passes.

Additionally, information related to the investigation or prosecution of any alleged violation; place of violation; Enforcement Investigative Reports (EIRs); 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.

Authority for maintenance of the system:

49 U.S.C. 114(d), 44901, 44903, 44916, 46101, 46301.

Purpose(s):

The records are created in order 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.

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

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

A. To the Department of Justice (DOJ), including U.S. Attorney Offices, 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 where 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. §§ 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

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

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS' efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other

assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate federal, state, tribal, local, territorial, 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, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To 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.

I. 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.

J. To a Federal, State, local, tribal, territorial, foreign, or international agency, where such agency has requested information relevant or necessary for the hiring or retention of an individual, or the issuance of a security clearance, license, contract, grant, or other benefit.

K. To a Federal, State, local, tribal, territorial, foreign, or international agency, if necessary to obtain information relevant to a DHS/TSA decision concerning the hiring or retention of an employee, the issuance of a security clearance, license, contract, 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 where 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, 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. § 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 where 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 Web site 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, where there exists a legitimate public interest in the disclosure of the information, or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy or a risk to transportation or national security.

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, where DHS/TSA determines that the information would assist in the enforcement of a civil or criminal law.

Disclosure to consumer reporting agencies:

Pursuant to 5 U.S.C. § 552a(b)(12), disclosures may be made from this system to consumer reporting agencies collecting on behalf of the United States Government.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records in this system are stored electronically or on paper. The records may be stored on magnetic disc, tape, digital media, microfiche, and roll microfilm.

Retrievability:

Records may be retrieved 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.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who also have a need-to-know for the performance of their official duties; using locks, alarm devices, and passwords; and

encrypting data communications. Strict control measures are enforced to ensure that access to classified and/or sensitive information in these records is also based on need to know. Electronic access is limited by computer security measures that are strictly enforced. TSA file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel.

Retention and disposal:

National Archives and Records Administration approval is pending for the records in this system. Paper records and information stored on electronic storage media are maintained within TSA for five years and then forwarded to Federal Records Center. Records are destroyed after ten years.

System Manager and address:

Information Systems Program Manager, Office of the Chief Counsel, TSA Headquarters, West Tower, 8th Floor, TSA-2, 601 S. 12th Street, Arlington, VA 20598.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/TSA will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the TSA FOIA Officer by e-mail at foia.tsa@dhs.gov or by mail at Transportation Security Administration, TSA-20, FOIA Office, 601 S. 12th Street, Arlington, VA 20598. If an individual believes more than one

component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 C.F.R. Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Records are obtained from 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.

Exemptions claimed for the system:

Portions of this system are exempt under 5 U.S.C. § 552a(k)(1) and (k)(2). Portions of the system pertaining to investigations or prosecutions of violations of criminal law are exempt under 5 U.S.C. § 552a(j)(2). These exemptions are reflected in the final rule published on August 4, 2006 in 71 FR 44223.

Dated: November 21, 2013.

Karen L. Neuman

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-29353 Filed 12/06/2013 at 8:45 am; Publication Date: 12/09/2013]