4910-62

**DEPARTMENT OF HOMELAND SECURITY**

Office of the Secretary

[Docket No. DHS-2014-0038]

# Privacy Act of 1974; Department of Homeland Security Transportation Security Administration – 002 Transportation Security Threat Assessment System System of Records

**AGENCY**: Department of Homeland Security, Privacy Office.

**ACTION**: Notice to update an existing Privacy Act System of Records.

**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 – 002 Transportation Security Threat Assessment System of Records." This system of records allows the Department of Homeland Security/Transportation Security Administration to collect and maintain records related to security threat assessments, employment investigations, and evaluations that the Transportation Security Administration conducts on certain individuals for security purposes. For example, individuals who apply for a Transportation Worker Identification Credential or a Hazardous Materials Endorsement must undergo a security threat assessment, and records associated with the assessment are covered by this system.

TSA is making modifications to the "Purposes" section of the system of records to reflect the Department of Homeland Security's use of information to more readily and

effectively carry out the Department of Homeland Security's national security, law enforcement, immigration, and benefits missions. Also, two categories of records that were previously listed in the "Categories of individuals covered by the system" section are being moved to the "Categories of records" section. Finally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Portions of this system are exempt under 5 U.S.C. 552a(k)(1) and (k)(2) as reflected in the final rule published in the Federal Register on June 25, 2004.

This updated system will continue to 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 PUBLICATION IN THE FEDERAL REGISTER].

**ADDRESSES**: You may submit comments, identified by docket number DHS-2014-0038 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, DC 20528.

**INSTRUCTIONS**: All submissions received must include the agency name and docket number for this rulemaking. 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, Transportation Security Administration, TSA-36, 601 South 12th Street, Arlington, VA, 20598-6036, or TSAprivacy@dhs.gov. For privacy issues please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 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 Administration (TSA) proposes to update and reissue a current DHS system of records notice titled, "DHS/TSA – 002 Transportation Security Threat Assessment System of Records."

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. The Security Threat Assessment System contains records related to security threat assessments, employment investigations, and evaluations DHS/TSA conducts on certain individuals for security purposes. The information is collected to conduct security

threat assessments on individuals to ensure they do not pose, and are not suspected of posing, a threat to transportation or national security. For example, individuals who apply for a Transportation Worker Identification Credential or a Hazardous Materials Endorsement must undergo a security threat assessment and are covered by this system.

TSA is making the following modifications:

- TSA is updating the Purpose(s) section to reflect the use of information by DHS to more readily and effectively carry out DHS's national security, law enforcement, immigration, and benefits missions.
- TSA is updating the Categories of Records section to include two categories of records that were previously listed in the "Categories of individuals covered by the system" section. These categories are records concerning the following individuals: (i) known or suspected terrorists identified in the Terrorist Screening Database (TSDB) of the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC); individuals identified by DHS/TSA to be included in the TSDB because they pose a threat to civil aviation or national security; and individuals in classified and unclassified governmental terrorist, law enforcement, immigration, or intelligence databases, including databases maintained by the Department of Defense, National Counterterrorism Center, or FBI; and (ii) individuals who have been or seek to be distinguished from individuals on a watchlist through a redress process, or other means. This update reflects a conclusion that these categories are more appropriately categories of records used in this system, rather than categories of individuals maintained in this system.

Consistent with DHS's information-sharing mission, information stored in the DHS/TSA – 002 Transportation Security Threat Assessment System of Records 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, or foreign 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). In addition, to the extent a record contains information from other exempt systems of records, DHS/TSA will rely on the exemptions claimed for those systems as reflected in the final rule published on June 25, 2004, 69 FR 35536.

II. Privacy Act

The Privacy Act embodies fair information 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. The Privacy Act defines "individual" as a United States citizen or a lawful permanent resident. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Below is

the description of the DHS/TSA – 002 Transportation Security Threat Assessment System 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) – 002

**System name:**

DHS/TSA – 002 Transportation Security Threat Assessment System (T-STAS).

**Security classification:**

Classified, Sensitive.

**System location:**

Records are maintained at the Transportation Security Administration (TSA) Headquarters, 601 South 12th Street, Arlington, VA 20598 and TSA field offices. Records may also be maintained at the offices of TSA contractors.

**Categories of individuals covered by the system:**

Individuals who undergo a security threat assessment, employment investigation, or other evaluation performed for security purposes or in order to obtain access to the following: transportation infrastructure or assets, such as terminals, facilities, pipelines, railways, mass transit, vessels, aircraft, or vehicles; restricted airspace; passenger baggage; cargo; shipping venues; or other facilities or critical infrastructure over which DHS exercises authority; Sensitive Security Information or Classified information

provided in connection with transportation security matters; or transportation-related instruction or training (such as flight training). This includes, but is not limited to, the following individuals:

(a) Individuals who require or seek access to airports, or maritime or surface transportation facilities, or facilities over which DHS exercises authority.

(b) Individuals who have or are seeking responsibility for screening individuals or carry-on baggage, and those persons serving as immediate supervisors and the next supervisory level to those individuals, other than employees of the DHS/TSA who perform or seek to perform these functions.

(c) Individuals who have or are seeking responsibility for screening checked baggage or cargo, and their immediate supervisors, and the next supervisory level to those individuals, other than employees of the DHS/TSA who perform or seek to perform these functions.

(d) Individuals who have or are seeking the authority to accept checked baggage for transport on behalf of an aircraft operator that is required to screen passengers.

(e) Pilots, copilots, flight engineers, flight navigators, and airline personnel authorized to fly in the cockpit, relief or deadheading crewmembers, cabin crew, and other flight crew for an aircraft operator or foreign air carrier that is required to adopt and carry out a security program.

(f) Flight crews and passengers who request waivers of temporary flight restrictions (TFR) or other restrictions pertaining to airspace.

(g) Other individuals who are connected to the transportation industry for whom DHS/TSA conducts security threat assessments to ensure transportation security.

(h) Individuals who have or are seeking unescorted access to cargo in the transportation system.

(i) Individuals who are owners, officers, or directors of an indirect air carrier or a business seeking to become an indirect air carrier.

(j) Aliens or other individuals designated by DHS/TSA who apply for flight training or recurrent training.

(k) Individuals transported on all-cargo aircraft, including aircraft operator or foreign air carrier employees and their family members and persons transported for the flight.

(l) Individuals seeking to become, or qualified as, known shippers or Certified Cargo Screening Program validators.

(m) Individuals who are owners, operators, or directors of any transportation mode facilities, services, or assets.

**Categories of records in the system:**

DHS/TSA's system may contain any, or all, of the following information regarding individuals covered by this system:

(a) Name (including aliases or variations of spelling).

(b) Gender.

(c) Current and historical contact information (including, but not limited to, address information, telephone number, and e-mail).

(d) Government-issued licensing or identification information (including, but not limited to, Social Security number; pilot certificate information, including number and country of issuance; current and past citizenship information; immigration status; alien registration numbers; visa information; and other licensing information for modes of transportation).

(e) Date and place of birth.

(f) Name and information, including contact information and identifying number (if any) of the airport, aircraft operator, indirect air carrier, maritime or land transportation operator, or other employer or entity that is employing the individual, submitting the individual's information, or sponsoring the individual's background check/threat assessment.

(g) Physical description, fingerprint and/or other biometric identifier, and photograph.

(h) Date, place, and type of flight training or other instruction.

(i) Control number or other unique identification number assigned to an individual or credential.

(j) Information necessary to assist in tracking submissions, payments, and transmission of records.

(k) Results of any analysis performed for security threat assessments and adjudications.

(l) Other data as required by Form FD 258 (fingerprint card) or other standard fingerprint cards used by the Federal Government.

(m) Information provided by individuals covered by this system in support of their application for an appeal or waiver.

(n) Flight information, including crew status on board.

(o) Travel document information (including, but not limited to, passport information, including number and country of issuance; and current and past citizenship information and immigration status, any alien registration numbers, and any visa information).

(p) Criminal history records.

(q) Data gathered from foreign governments or entities that is necessary to address security concerns in the aviation, maritime, or land transportation systems.

(r) Other information provided by federal, state, and local government agencies or private entities.

(s) The individual's level of access at an airport or other transportation facility, including termination or expiration of access.

(t) Military service history.

(u) Suitability testing and results of such testing.

(v) The individual’s status as a known or suspected terrorist identified in the Terrorist Screening Database (TSDB) of the Federal Bureau of Investigation’s (FBI) Terrorist Screening Center (TSC); an individual identified by DHS/TSA to the TSDB because he or she poses a threat to civil aviation or national security; and an individual in classified and unclassified governmental terrorist, law enforcement, immigration, or

intelligence databases, including databases maintained by the Department of Defense, National Counterterrorism Center, or Federal Bureau of Investigation.

(w) The individual who has or seeks to be distinguished from individuals on a watch list through a redress process, or other means.

**Authority for maintenance of the system:**

49 U.S.C. 114, 5103a, 40103(b)(3), 40113(a), 44903(b), 44936, 44939, and 46105.

**Purpose(s):**

The purposes of this system are:

(a) Performance of security threat assessments, employment investigations, and evaluations performed for security purposes that federal statutes and/or DHS/TSA regulations authorize for the individuals identified in "Categories of individuals covered by the system," above.

(b) To assist in the management and tracking of the status of security threat assessments, employment investigations, and evaluations performed for security purposes.

(c) To permit the retrieval of the results of security threat assessments, employment investigations, and evaluations performed for security purposes; including criminal history records checks and searches in other governmental, commercial, and private data systems, performed on the individuals covered by this system.

(d) To permit the retrieval of information from other terrorist-related, law enforcement, immigration and intelligence databases on the individuals covered by this system.

(e) To track the fees incurred, and payment of those fees, by the airport operators, aircraft operators, maritime and land transportation operators, flight students, and others, when appropriate, for services related to security threat assessments, employment investigations, and evaluations performed for security purposes.

(f) To facilitate the performance of security threat assessments and other investigations that DHS/TSA may conduct.

(g) To enable DHS to carry out DHS's national security, law enforcement, immigration, intelligence, or other homeland security functions.

**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. 522a(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. 522a(b)(3) as follows:

A. To the Department of Justice (DOJ), including offices of 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 or proceedings and one of the following is a party to the litigation or proceedings or has an interest in such litigation or proceedings:

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. 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's 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 government 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.

H. To the U.S. 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, endorsement, certificate, contract, grant, or other benefit.

I. To an appropriate federal, state, local, tribal, territorial, or foreign 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, or foreign agency, when such agency has requested information relevant to or necessary for the hiring or retention of an individual; or the issuance of a security clearance, license, endorsement, contract, grant, waiver, credential, or other benefit.

K. To a federal, state, local, tribal, territorial, or foreign agency, if necessary to obtain information relevant to a DHS/TSA decision concerning the initial or recurrent security threat assessment; the hiring or retention of an employee; the issuance of a security clearance, license, endorsement, contract, grant, waiver, credential, or other benefit; and to facilitate any associated payment and accounting.

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

M. To third parties during the course of a security threat assessment, employment investigation, or adjudication of a waiver or appeal request, to the extent necessary to obtain information pertinent to the assessment, investigation, or adjudication.

N. To airport operators, aircraft operators, 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, training, or the issuance of such credentials or clearances.

O. 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 when the Department requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

P. 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.

Q. 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 civil or criminal laws.

R. 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 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.

**Disclosure to consumer reporting agencies:**

None.

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

**Storage**:

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 or digital media.

**Retrievability**:

DHS/TSA may retrieve records by name, Social Security number, identifying number of the submitting or sponsoring entity, other case number assigned by DHS/TSA or other entity/agency, biometric, or a unique identification number, or any other identifying particular assigned or belonging to the individual.

**Safeguards**:

DHS/TSA safeguards records in this system in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. DHS/TSA limits access to the computer system containing the records in this system 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.

**Retention and disposal:**

In accordance with National Archives and Records Administration approved retention and disposal policy N1-560-06, for individuals who were not identified as possible security threat, records will be destroyed one year after DHS/TSA is notified that access based on security threat assessment is no longer valid; when an individual was identified as a possible security threat and subsequently cleared, records will be destroyed seven years after completion of the security threat assessment or one year after being notified that access based on the security threat assessment is no longer valid, whichever is longer; and when the individual is an actual match to a watchlist, records will be destroyed 99 years after the security threat assessment or seven years after DHS/TSA is notified the individual is deceased, whichever is shorter.

**System manager(s) and address:**

Assistant Director for Compliance, Office of Intelligence & Analysis, TSA-10, Transportation Security Administration, 601 South 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 and access to any record contained in the system of records, or seeking to contest its content, may submit a request in writing to the DHS/TSA's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts." 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, DC 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 CFR 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, or by calling 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;
- 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 procedure:**

See "Notification Procedure" above.

**Contesting record procedure:**

See "Notification Procedure" above.

**Record source categories:**

Records are obtained from individuals subject to a security threat assessment, employment investigation, or other security analysis; from aviation, maritime, and land transportation operators, flight schools, or other persons sponsoring the individual; and any other persons, including commercial entities that may have information that is relevant or necessary to the assessment or investigation. Information about individuals is also used or collected from domestic and international intelligence sources and other

governmental, private, and public databases. The sources of information in the criminal history records obtained from the Federal Bureau of Investigation are set forth in the Privacy Act system of records notice Department of Justice Federal Bureau of Investigation – 009 Fingerprint Identification Records System (64 FR 52347, September 28, 1999).

**Exemptions claimed for the system:**

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. § 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

Dated: July 28, 2014.

Karen L. Neuman,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2014-18699 Filed 08/08/2014 at 8:45 am; Publication Date:

08/11/2014]