the records are part of an on-going investigation in which case they may be retained until completion of the investigation. This period is based on the statute of limitations for most types of misuse or fraud possible using E-Verify (under 18 U.S.C. 3291, the statute of limitations for false statements or misuse regarding passports, citizenship, or naturalization documents).

SYSTEM MANAGER AND ADDRESS:

Chief, Verification Division, U.S. Citizenship and Immigration Services, Washington, DC 20529.

NOTIFICATION PROCEDURE:

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 USCIS Verification Division 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, SW., 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 1–866–431–0486. In addition you should provide the following:

- An explanation of 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 this bulleted 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 several sources including: (A) Information collected from employers about their employees relating to employment eligibility verification; (B) Information collected from E-Verify users used to provide account access and monitoring; (C) Information collected from federal databases as listed in the Category of Records section above; and (D) Information created by E-Verify, including its monitoring and compliance activities.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–11972 Filed 5–18–10; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2010–0013]

Privacy Act of 1974: System of Records; Department of Homeland Security Transportation Security Administration—001, Transportation Security Enforcement Record System, System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice to alter 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 an existing Department of Homeland Security system of records notice titled, Transportation Security Administration 001 Transportation Security Enforcement Record System previously published on December 10, 2004. As a result of the biennial review of this system, modifications are being made to the system of records' categories of individuals, categories of records, routine uses, record source categories, retention and disposal, notification procedures, and system manager and address. The Department of Homeland Security Transportation Security Administration—001 Transportation Security Enforcement Record System covers records related to the Transportation Security Administration's screening of passengers and property and enforcement actions involving all modes of transportation regulated by the Transportation Security Administration. Information in this system also includes 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.

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.

This system will continue to be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before June 18, 2010. The system will be effective June 18, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS–2010–0013 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Mary Ellen Callahan, 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 go to *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: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with this requirement and 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 DHS/TSA system of records notice titled, DHS/TSA–001 Transportation Security Enforcement Record System (69 FR 71828, December 10, 2004.)

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. In accordance with the biennial review of this system, the following modifications are being made:

- The categories of individuals section is updated from "passengers undergoing screening" to "individuals undergoing screening." This change clarifies that individuals other than passengers may be subject to screening, such as individuals who escort minors or the elderly into the sterile area.
- The categories of records section has been updated to State that records may relate to any individual, not just to a passenger, who undergoes screening and to an individual whose identity must be verified against the Federal watch lists.
- DHS/TSA is updating the system of records to incorporate five DHS standard routines uses. One routine use will allow release of information to appropriate agencies, entities, and persons when DHS/TSA suspects or has confirmed that the security or confidentiality of an information system of records has been compromised. Another routine use permits the release of information to the media when there exists a legitimate public interest in disclosing information. Release under this routine use will require the approval of the DHS Chief Privacy Officer in consultation with counsel. Another routine use allows the release of information to a court, magistrate, administrative tribunal or opposing counsel or parties where a Federal agency is a party or has an interest in the litigation or administrative proceeding. The fourth routine use allows DHS/TSA to release information to a former employee when it is necessary to consult with the former employee regarding a matter that is within that person's former area of responsibility. The fifth routine use allows DHS/TSA to release information to appropriate entities where it would assist in the enforcement of civil or criminal laws.
- Additionally, DHS/TSA is revising a current routine use adding indirect air carriers and other facility operators as a potential recipient of information from these systems 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.
- DHS/TSA is also revising a current routine use by adding indirect air carriers and other facility operators as potential recipients of information 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.
- Finally, DHS/TSA is adding a routine use to allow DHS/TSA to publish final agency and Administrative Law Judge decisions in civil enforcement and other administrative matters.
- The record source categories are updated to reflect the use of commercial and public record databases and Web sites to obtain information regarding the identity of individuals who attempt to gain access to the sterile areas of the airport and for whom identity needs to be verified or individuals who are being vetted to qualify as Federal flight deck officers.
- The retention and disposal sections are updated to reflect the records retention schedules approved by the National Archives and Records Administration (NARA).
- The notification section was changed to reflect that inquiries regarding whether the applicable system contains records about an individual should be directed to TSA's Freedom of Information Act (FOIA) Office.
- The system manager was revised to reflect the current system manager of the system.

Consistent with the Privacy Act, information stored in TSERS may be shared with other DHS components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions 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.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates 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 United States 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. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency recordkeeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the Transportation Security Administration 001 Transportation Security Enforcement Record 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

DHS/TSA—001

SYSTEM NAME:

Transportation Security Administration Transportation Security Enforcement Record System (TSERS).

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.

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 name, address, gender, date of birth, contact information, fingerprints and/or other biometric identifiers, photographs or video, or travel information or boarding passes; 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 and 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 United States Attorney Offices) or other Federal agency in anticipation of, or conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is 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 current or former employee of DHS in his/her official capacity, or

3. Any current 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, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS/TSA collected the records.

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, or other Federal government agencies, pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual 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 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 DHS or another agency or entity) or harm to the individual that rely upon the compromised information;

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 provide 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, international, or foreign agency, including law enforcement, 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. The issuance, maintenance, or renewal of 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 40 U.S.C. 610101(b).

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 are maintained on paper and in computer-accessible storage media. Records are also stored on microfiche and roll microfilm.

RETRIEVABILITY:

Records are 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; 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 22202–4220.

NOTIFICATION PROCEDURE:

To determine whether this system contains records relating to you, write to the System Manager identified above.

RECORD ACCESS PROCEDURE:

Same as "Notification Procedures" above. Provide your full name and a description of information that you seek, including the time frame during which the record(s) may have been generated. Individuals requesting access must comply with the Department of Homeland Security Privacy Act regulations on verification of identity (6 CFR 5.21(d)).

CONTESTING RECORD PROCEDURES:

Same as "Notification Procedure," and "Record Access Procedures" above.

RECORD SOURCE CATEGORIES:

Information contained in this system is 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.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–11917 Filed 5–18–10; 8:45 am]

BILLING CODE 4410–62–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2010–0014]

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

AGENCY: Privacy Office, DHS.

ACTION: Notice to alter 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 the Department of Homeland Security Transportation Security Administration—002 Transportation Security Threat Assessment System of Records, November 8, 2005, to reflect necessary programmatic changes. As a result of the biennial review of this system, modifications are being made to the system of records' categories of individuals, categories of records, routine uses, data retention and disposal, and notification procedures. The Department of Homeland Security Transportation Security Administration—002 Transportation Security Threat Assessment System System of Records contains records related to security threat assessments, employment investigations, and evaluations 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.

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 June 18, 2010. This amended system will be effective June 18, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS–2010–0014 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Mary Ellen Callahan, 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 go to *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Peter Pietra (*TSAprivacy@dhs.gov*), Privacy Officer, Transportation Security Administration, TSA–36, 601 South 12th Street, Arlington, VA 20598–6036 or *TSAprivacy@dhs.gov*. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. 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 DHS/TSA system of records notice titled, DHS/TSA—002 Transportation Security Threat Assessment System of Records (70 FR 33383, November 8, 2005).

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. In accordance with the biennial review of this system, the following modifications are being made:

- The categories of individuals section is updated to expressly include individuals who seek maritime or surface transportation facility access badges or credentials as well as individuals who undergo a security threat assessment unassociated with a