9110-05-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2013-0040]

Privacy Act of 1974; Department of Homeland Security/Transportation Security Administration - DHS/TSA-021 TSA Pre✓™ Application Program System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records titled, "Department of Homeland Security/Transportation Security Administration - DHS/TSA-021 TSA Pre✓™ Application Program System of Records." This system of records allows the Department of Homeland Security/Transportation Security Administration to collect and maintain records on individuals who voluntarily submit information to the Transportation Security Administration for use by the agency to perform a security threat assessment. The security threat assessment will be used to identify persons who pose a low risk to transportation security and therefore may be eligible for expedited screening at participating U.S. airport security checkpoints. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking elsewhere in the **Federal Register** to exempt some records from this system of records from certain provisions of the Privacy Act. This newly established system will be included in the Department of Homeland Security's inventory of systems of records.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new 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-2013-0040 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: Jonathan R. Cantor, Acting 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 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, TSA Privacy Officer, TSA-036, 601 South 12th Street, Arlington ,VA 20598-6036; or email at TSAprivacy@dhs.gov. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting 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 Administration (TSA) proposes to establish a new DHS system of records titled, "DHS/TSA-021 TSA Pre✓™ Application Program System of Records."

TSA is establishing this new system of records to inform the public of the collection, maintenance, dissemination, and use of records on individuals who voluntarily submit personally identifiable information to the TSA Pre✓™ Application Program. TSA will use the information provided by applicants[1] to the Program to perform a security threat assessment to identify individuals who present a low risk to transportation security. This passenger prescreening enables TSA to determine the appropriate level of security screening the passenger will receive before the passenger receives a boarding pass.

TSA Pre✓™ Application Program. TSA Pre✓™ is a passenger prescreening initiative for low risk passengers who are eligible to receive expedited screening at participating U.S. airport security checkpoints.[2] TSA Pre✓™ is one of several expedited screening initiatives that TSA is implementing. TSA Pre✓™, as well as the larger set of expedited screening initiatives, enhance aviation security by permitting TSA to better focus its limited security resources on passengers who are more likely to pose a threat to

[1] Further information on information collection can be found in Intent To Request Approval From OMB of One New Public Collection of Information: TSA Pre✓™ Trusted Traveler Program; Republication, 78 FR 45256 (July 26, 2013)(republished for technical correction).

[2] Passengers who are eligible for expedited screening through a dedicated TSA Pre□™ lane typically will receive more limited physical screening, *e.g.,* will be able to leave on their shoes, light outerwear, and belt, to keep their laptop in its case, and to keep their 3-1-1 compliant liquids/gels bag in a carry-on. TSA Pre□™ lanes are available at 40 airports nationwide, with additional expansion planned. See *TSA Pre□™ Now Available at 40 Airports Nationwide: Expedited Screening Begins at Raleigh-Durham International Airport*, http://www.tsa.gov/press/releases/2013/03/28/tsa-pre%E2%9C%93%E2%84%A2-now-available-40-airports-nationwide-expedited-screening-begins.

civil aviation, while also facilitating and improving the commercial aviation travel experience for the public.

TSA is implementing the TSA Pre✓™ Application Program pursuant to its authority under section 109(a)(3) of the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71 (115 Stat. 597, 613, Nov. 19, 2001, codified at 49 U.S.C. 114 note). That section authorizes TSA to "[e]stablish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening."

Members of the public who apply to the TSA Pre✓™ Application Program will be required to pay a fee. Section 540 of the DHS Appropriations Act, 2006, Pub. L. 109-90 (119 Stat. 2064, 2088-89, Oct. 18, 2005), authorizes TSA to establish and collect a fee for any registered traveler program by publication of a notice in the Federal Register. The Department of Homeland Security is issuing a separate notice of the fee for the TSA Pre✓™ Application Program elsewhere in the **Federal Register**.

To apply to the TSA Pre✓™ Application Program, individuals will submit biographic and biometric information to TSA. TSA will use the information to conduct a security threat assessment of law enforcement, immigration, and intelligence databases, including a fingerprint-based criminal history records check conducted through the Federal Bureau of Investigation (FBI). The results will be used by TSA to decide if an individual poses a low risk to transportation or national security. TSA will provide individuals who meet the standards of the security threat assessment a Known Traveler

Number (KTN).[3]

The list of individuals approved under the TSA Pre✓™ Application Program, including their name, date of birth, gender, and KTN, will be provided to the TSA Secure Flight passenger prescreening system.[4] The Secure Flight system will not receive other applicant information that is maintained in the TSA Pre✓™ Application Program system of records.[5]

Eligibility for the TSA Pre✓™ Application Program is within the sole discretion of TSA, which will notify applicants who are denied eligibility in writing of the reasons for the denial. If initially deemed ineligible, applicants will have an opportunity to correct cases of misidentification or inaccurate criminal or immigration records. Consistent with 28 CFR 50.12 in cases involving criminal records, and before making a final eligibility decision, TSA will advise the applicant that the FBI criminal record discloses information that would disqualify him or her from the TSA Pre✓™ Application Program. Within 30 days after being advised that the criminal record received from the FBI discloses a disqualifying criminal offense, the applicant must notify TSA in writing of his or her intent to correct any information he or she believes to be inaccurate. The applicant must provide a certified revised record, or the appropriate court must forward a

[3] The Known Traveler Number is a component of Secure Flight Passenger Data (SFPD), both of which are defined in the Secure Flight regulations at 49 CFR 1560.3. *See also* the Secure Flight regulations at 49 CFR Part 1560.

[4] See the Privacy Impact Assessment for the Secure Flight Program, DHS/TSA/PIA-018(e), at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight_update018(e).pdf. *See also* the Secure Flight SORN, DHS/TSA 019, https://www.federalregister.gov/articles/2012/11/19/2012-28058/privacy-act-of-1974-system-of-records-secure-flight-records. The Secure Flight SORN is being updated for other reasons.

[5] This System of Records Notice does not cover all individuals who may be eligible for TSA Pre✓™ expedited screening through some other means (for example, U.S. Customs and Border Protection Global Entry members, Members of the Armed Forces). This system only covers individuals who apply to TSA for enrollment in the TSA Pre✓™ Application Program.

certified true copy of the information, prior to TSA approving eligibility of the applicant for the TSA Pre✓™ Application Program. With respect to immigration records, within 30 days after being advised that the immigration records indicate that the applicant is ineligible for the TSA Pre✓™ Application Program, the applicant must notify TSA in writing of his or her intent to correct any information believed to be inaccurate. TSA will review any information submitted and make a final decision. If neither notification nor a corrected record is received by TSA, TSA may make a final determination to deny eligibility. Individuals whom TSA determines are ineligible for the program will continue to be screened at airport security checkpoints according to TSA standard screening protocols.

To be eligible for expedited screening in a TSA Pre✓™ lane, the passenger will provide his or her KTN to the airline when making flight reservations. When the airline sends the passenger's Secure Flight Passenger Data (SFPD)[6] that includes a KTN to the Secure Flight passenger prescreening system, TSA will compare that information against the TSA Pre✓™ Application Program list (as well as watch lists) in Secure Flight before issuing an appropriate boarding pass printing instruction. If the passenger's identifying information matches the entry on the TSA Pre✓™ Application Program list, the passenger will be eligible for expedited screening.

Enrollment into the TSA Pre✓™ Application Program, and use of the associated KTN, does not guarantee that an individual always will receive expedited screening at airport security checkpoints. The Program retains a component of randomness to

[6] SFPD consists of name, gender, date of birth, passport information (if available), redress number (if available), Known Traveler number (if available), reservation control number, record sequence number, record type, passenger update indicator, traveler reference number, and itinerary information.

maintain the element of unpredictability for security purposes. Accordingly, persons who have been enrolled in the TSA Pre✓™ Application Program may be randomly selected for standard physical screening on occasion. In addition, although the number of TSA Pre✓™ lanes at U.S. airports is increasing, TSA Pre✓™ is not yet available for all airports, all airlines or all flights.

DHS Information Sharing. Consistent with DHS's information-sharing mission, TSA may share information stored in the DHS/TSA-021 TSA Pre✓™ Application Program system of records 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, or foreign government agencies consistent with the routine uses set forth in this system of records notice.

Notice of Proposed Rulemaking. DHS is issuing a notice of proposed rulemaking to accompany this SORN elsewhere in the **Federal Register** to exempt some records from this system of records (*see* "Exemptions claimed for the system") from certain provisions of the Privacy Act. This newly established system will be included in DHS's inventory of record systems which can be found at www.DHS.gov/privacy.

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. 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-021 TSA Pre✓™ Application Program 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) DHS/TSA-021

System name:

DHS/TSA-021 TSA Pre✓™ Application Program

Security classification:

Classified, unclassified, Sensitive Security Information.

System location:

Records will be maintained at the Transportation Security Administration (TSA), 601 South 12th Street, Arlington, VA 20598, and at TSA facilities in Annapolis Junction, Maryland, and Colorado Springs, Colorado. Records also may be maintained at other authorized TSA or DHS facilities, or by TSA contractors or other parties that perform functions under this program.

Categories of individuals covered by the system:

Individuals who apply to, or participate in the TSA Pre✓™ Application Program.

Categories of records in the system:

This 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, telephone number, and e-mail address);

(d) Date and place of birth;

(e) Physical description, fingerprint and/or other biometric identifier, including photograph;

(f) Control number, Social Security Number (SSN), or other unique identification number assigned to an individual;

(g) Information necessary to assist in tracking submissions, payments, and transmission of records;

(h) Other data as required by Form FD-258 (fingerprint card) or other standard fingerprint cards used by the federal government;

(i) Information provided by individuals covered by this system in support of their application, such as driver's license, passport or other documents used to verify identity, confirm immigration status, or other eligibility requirements;

(j) Criminal history records;

(k) Records obtained from the Terrorist Screening Center of known or suspected terrorists in the Terrorist Screening Database; and records regarding individuals

identified on classified and unclassified governmental watch lists used or maintained by TSA;

(l) Records containing the matching analyses and results of comparisons of individuals to the TSDB and other classified and unclassified governmental databases, such as law enforcement, immigration, or intelligence databases, and individuals who have been distinguished from individuals on a watch list through a redress process or other means;

(m) Other information provided by federal, state, local, tribal, territorial, and foreign government agencies or other entities relevant to the security threat assessment and adjudication of the application;

(n) Results of any analysis performed for security threat assessments and adjudications; and

(o) Communications between TSA and applicants regarding the results of the security threat assessments and adjudications.

Authority for maintenance of the system:

Section 109(a)(3) of the Aviation and Transportation Security Act, Pub. L. 107-71 (Nov. 19, 2001, codified at 49 U.S.C. 114 note).

Purpose(s):

The purpose of the TSA Pre✓™ Application Program is to:

(a) perform security threat assessments and to identify individuals who are a low risk to transportation or national security and are therefore eligible to receive expedited security screening;

(b) assist in the management and tracking of the status of security threat assessments

of individuals who apply to the TSA Pre✓™ Application Program;

(c) permit the retrieval of the results of security threat assessments, including criminal history records checks and searches in other governmental data systems, performed on the individuals covered by this system;

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

(e) track the fees incurred, and payment of those fees, when appropriate, for services related to security threat assessments.

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 agencies conducting litigation or in proceedings before any court, or 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. 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 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, including 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 TSC in order to:

1. determine whether an individual is a positive identity match to an individual identified as a known or suspected terrorist in the watch list;

2. allow redress for passenger complaints;

3. facilitate an operational response, if one is deemed appropriate, for individuals who are a positive identity match to an individual identified as a KST in the watch list;

4. provide information and analysis about terrorist encounters and KST associates to appropriate domestic and foreign government agencies and officials for counterterrorism purposes; and

5. perform technical implementation functions necessary for the TSA Pre✓™ Application Program.

I. To the appropriate federal, state, local, tribal, territorial, foreign governments, or other appropriate authority, regarding or to identify individuals who pose, or are under reasonable suspicion of posing, a risk to transportation or national security.

J. To foreign governmental and international authorities, in accordance with law and formal or informal agreements.

K. 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 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:

The records in this system are stored in secure facilities on paper and in computer-accessible storage, and may be retained in hard copy format in secure file folders or safes.

Retrievability:

Records may be retrieved by the individual's name, SSN, 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:

Records in this system are safeguarded 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. 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.

Retention and disposal:

TSA intends to use existing information technology infrastructure and systems, and other established processes to collect information and conduct the security threat assessment for the TSA Pre□™ Application Program. In accordance with NARA approved retention and disposal policy N1-560-06-006, records for individuals who:

A. were not identified as a possible security threat will be destroyed one year after DHS/TSA is notified that access based on security threat assessment is no longer is valid;

B. were identified as a possible security threat and subsequently cleared will be destroyed seven years after completion of the security threat assessment or one year after being notified that access to the TSA Pre✓™ Application Program based on the security threat assessment is no longer is valid, whichever is later; and

C. were an actual match to a watchlist or otherwise identified as a potential or actual threat to transportation security will be destroyed 99 years after the security threat assessment or seven years after DHS/TSA is notified the individual is deceased, whichever is earlier.

System Manager and address:

TSA Pre✓™ Application Program Manager, Transportation Security Administration, TSA-19, 601 South 12th Street, Arlington, VA 20598-6019.

Notification procedure:

The Secretary of Homeland Security has exempted certain records from this system from the notification, access, and amendment procedures of the Privacy Act because it may contain records or information related to law enforcement or national security purposes. 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 FOIA Officer. Written requests may be submitted to DHS/TSA FOIA Officer, Freedom of Information Act Office, Transportation Security Administration, TSA-20, 601 South 12th Street, Arlington, VA 20598-6020; or to foia.tsa@dhs.gov. If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Acting Chief Privacy Officer and Acting 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 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 either must 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 Acting Chief Privacy Officer and Acting Chief Freedom of Information Act Officer, http://www.dhs.gov 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.

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:

Information contained in this system may be obtained from TSA Pre✓™ Application Program applicants, the TSC, law enforcement, immigration, and

intelligence agency record systems, other government databases, and other DHS systems. 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 entitled Department of Justice Federal Bureau of Investigation–009 Fingerprint Identification Records System (72 FR 3410, January 1, 2007).

Exemptions claimed for the system:

Portions of this system will be exempted from 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f) pursuant to 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, TSA will rely on the exemptions claimed for those systems. TSA will publish a notice of proposed rulemaking for exemptions to accompany this system of records notice.

Dated: September 4, 2013.

Jonathan R. Cantor,

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-21979 Filed 09/09/2013 at 8:45 am; Publication Date: 09/10/2013]