Privacy Impact Assessment
for the

TSA Pre✓™ Application Program

DHS/TSA/PIA-041

September 4, 2013

Contact Point
Hao-Y Froemling
Transportation Security Administration
Office of Intelligence & Analysis
Haoy.Froemling@tsa.dhs.gov

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) will conduct security threat assessments on individuals who apply to TSA for enrollment into the TSA Pre✓™ Application Program. TSA Pre✓™ Application Program participants are eligible to receive expedited screening at participating airport security checkpoints. TSA is conducting this Privacy Impact Assessment (PIA) pursuant to the E-Government Act of 2002 because personally identifiable information (PII) will be collected for the conduct of the security threat assessment.

Overview

TSA Pre✓™ is a passenger prescreening initiative that identifies low risk passengers who are eligible to receive expedited screening at participating U.S. airport security checkpoints.[1] TSA Pre✓™ enhances aviation security by permitting TSA to better focus its limited security resources on passengers who are more likely to pose a threat to 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." By way of background, TSA has provided, or expects to provide, expedited screening to several populations participating in TSA Pre✓™, including such groups as U.S. Customs and Border Protection (CBP) Global Entry and NEXUS,[2] certain frequent flyers,[3] members of the U.S. Armed Forces, certain holders of federal security clearances, Members of Congress, Federal judges, Medal of Honor recipients, and other populations for whom TSA has performed a security threat assessment, such as certain

[1] 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.

[2] For additional information about CBP's Trusted Traveler programs, please see DHS/CBP/PIA-002 – Global Enrollment System (GES), (January 10, 2013), *available at* http://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[3] Certain frequent travelers from Alaska Airlines, American Airlines, Delta Air Lines, United Airlines, US Airways and certain members of CBP's Trusted Traveler programs, including Global Entry, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and NEXUS who are U.S. citizens are eligible for expedited screening when they are booked on a participating airline. *See* TSA Pre✓™ Expedited Screening, *available at* http://www.tsa.gov/tsa-pre%E2%9C%93%E2%84%A2.

transportation sector workers who possess a Hazardous Materials Endorsement or Transportation Worker Identification Credential.

In an effort to expand the availability of TSA Pre✓™ to other populations, TSA will now conduct security threat assessments on individuals (beyond the populations listed above) who voluntarily apply to TSA for participation in the TSA Pre✓™ Application Program. The assessment will include checks against law enforcement, immigration, and intelligence databases, including a fingerprint-based criminal history records check (CHRC) conducted through the Federal Bureau of Investigation (FBI).[4] The results will be used by TSA to decide if an individual poses a sufficiently low risk to transportation or national security to be issued a Known Traveler Number (KTN).[5] Fingerprints are expected to be enrolled with the FBI for recurrent CHRCs. The FBI will also check fingerprints against its unsolved crimes database, but the result will not be returned to TSA. TSA expects that, in the future, fingerprints will also be enrolled with the National Protection and Programs Directorate/Office of Biometrics Identity Management NPPD/OBIM (formally known as NPPD/US-VISIT) Automatic Biometric Identification System (IDENT) biometric database.[6]

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.[7] The Secure Flight system will not receive other applicant information that is maintained in the TSA Pre✓™ Application Program system of records.[8]

Eligibility for the TSA Pre✓™ Application Program is within the sole discretion of TSA, which will notify individuals 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

---

[4] Convictions and findings of not guilty by reason of insanity are considered disqualifying.
[5] 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.
[6] See the Privacy Impact Assessment for Automated Biometric Identification System (IDENT), DHS/NPPD/PIA-002, at http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_usvisit_ident_appendixj_jan2013.pdf.
[7] 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.
[8] That 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). That system only covers individuals who apply to TSA for enrollment in the TSA Pre✓™ Application Program.

the appropriate court must forward a 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 TSA Pre✓™ Application 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)[9] 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, except that watch list matches will receive screening appropriate for their watch list status.

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 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.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

TSA is responsible for security in all modes of transportation, including civil aviation security and screening of passenger air transportation. 49 U.S.C. § 114. TSA is authorized to establish Application programs to provide expedited screening to members of such programs. 49 U.S.C. § 114 (note).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

[9] 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.

DHS/TSA-021 TSA Pre✓™ Application Program System of Records applies to the information and is being published simultaneously with this PIA.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. Authority to Operate (ATO) the information system was granted on June 27, 2011.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. See section 5.0 below.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Paperwork Reduction Act compliance is in process and an OMB Control Number will be provided for the information.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

TSA will collect the following information from applicants:

- full legal name and any aliases;
- current residential address;
- mailing address if different than residential address;
- previous residential address;
- date of birth;
- Social Security number (voluntary, but recommended[10]);
- gender;
- physical description (height; weight; eye color; hair color);

[10] Although TSA does not require submission of a Social Security number, failure to provide it may result in delays in processing the application or may prevent completion of the assessment.

- fingerprints;
- photograph;
- city, state, and country of birth; and
- immigration status and an alien registration number for both naturalized citizens and aliens (if applicable).

TSA will also retain the results of its assessment and supporting information.

2.2 What are the sources of the information and how is the information collected for the project?

TSA will collect information directly from the individual applicant, and from federal agencies whose databases will be checked for the security threat assessment.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. TSA does not use commercial data or publicly available data in order to accomplish the security threat assessment.

2.4 Discuss how accuracy of the data is ensured.

TSA relies on the accuracy of the information provided to it by the individual applicant and by the federal agencies whose databases are checked for the security threat assessment.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that because an applicant submits limited or inaccurate PII to TSA, an individual may be incorrectly identified as a match to a watch list.

Mitigation: TSA seeks to reduce the potential for misidentification by requiring data elements that should be sufficient to distinguish each affected individual from individuals whose information is included in the Terrorist Screening Data Base (TSDB). TSA will further mitigate the risk of misidentification by requiring the individual applicant to certify the accuracy, to the best of his or her knowledge, of the PII submitted to TSA.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

TSA will use the collected PII to conduct security threat assessments to determine whether the individual is eligible, and remains eligible, for participation in the TSA Pre✓™ Application Program. TSA expects to conduct recurrent checks against law enforcement, immigration, and intelligence databases.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

TSA shares information within DHS in the course of conducting security threat assessments. This sharing includes U.S. Citizenship and Immigration Services for immigration checks, and may in the future include enrolling fingerprints and certain associated biographic information with the NPPD/OBIM IDENT system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that PII may be used inappropriately.

Mitigation: TSA routinely performs security threat assessments on millions of individuals; therefore, the risk that the information for this population will be used inappropriately is small. PII collected by TSA will be used only in accordance with the described uses by integrating administrative, technical, and physical security controls that place limitations on the collection of PII, and protect PII against unauthorized disclosure, use, modification, or destruction.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

TSA will provide a Privacy Act Statement to individuals regarding the information collected for security threat assessments at the point of collection. The Privacy Act Statement will describe the

authority for the collection of the information, the purpose for the collection of information, whether provision of the information is voluntary, and any consequences of failing to provide the requested information.

In addition, TSA provides notice by issuing this PIA and in the associated Privacy Act SORN.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The TSA Pre✓™ Application Program is completely voluntary. However, if individuals choose to apply and are enrolled, then they cannot limit uses or decline to provide mandatory information. Individuals may elect not to provide voluntary information; however, doing so may delay the processing of their application or prevent its completion.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: The risk that an individual may not know how his or her information is used.

Mitigation: The risk is mitigated by information provided by TSA at the time of application and this PIA.

Section 5.0 Data Retention by the Project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The length of time TSA will retain information on an individual is based on each individual's vetting result. Information will be retained as described below:

- Information pertaining to an individual who is not a potential match to a watch list will be retained for one year after the individual has notified TSA that the individual no longer is participating, or seeking to participate, in the TSA Pre✓™ Application Program.
- Information pertaining to an individual who may originally have appeared to be a match to a watch list, but who was subsequently determined not to be a match, will be retained for seven years after completion of matching, or one year after the individual has notified TSA that he or she no longer is participating, or seeking to participate, in the TSA Pre✓™ Application Program, whichever is later.
- Information pertaining to an individual who is determined to be a positive match to a watch list will be retained for 99 years after completion of matching activity,[11] or seven years after TSA learns that the individual is deceased, whichever is earlier.

[11] See JUSTICE/FBI-019 Terrorist Screening Records System (TSRS) at http://www.fbi.gov/foia/privacy-act/72-fr-

The FBI will retain fingerprint records in accordance with its own record schedule, which can be found at www.archives.gov.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information is retained for longer than necessary.

Mitigation: TSA will retain these records in accordance with the records retention schedule approved by NARA. The retention schedule was developed to provide flexibility to accommodate recurrent vetting during the time that the individual has access to the TSA Pre✓™ Application Program.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information on matches and potential matches to a watch list will normally be shared with the Terrorist Screening Center (TSC) to confirm the match analysis and for operational response. Information is provided to TSC via password-protected e-mail.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

DHS/TSA-021 TSA Pre✓™ Application Program System of Records, Routine Use I permits disclosure "to the appropriate federal, state, local, tribal, territorial, or foreign governments, or other appropriate authority, regarding or to identify individuals who pose, or are suspected of posing, a risk to transportation or national security." This is compatible with the collection of information for purposes of conducting security threat assessments since the TSC is the agency that maintains the TSDB and may coordinate an operational response if appropriate.

6.3 Does the project place limitations on re-dissemination?

No, TSA does not place limitations on re-dissemination of information by the TSC except to the extent match information is Sensitive Security Information (SSI) pursuant to 49 U.S.C. § 114(r). Re-dissemination of SSI is limited by the SSI regulation, 49 CFR Part 1520.

47073.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures to the TSC are recorded both manually within investigative files and automatically in an output report.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be inappropriately shared.

Mitigation: TSA may share this information in accordance with the Privacy Act. TSA mitigates attendant privacy risk by sharing externally only in accordance with published routine uses under the Privacy Act. Further, TSA has entered into an MOU with the FBI and TSC governing the conditions of sharing information.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals may request access to their data under the Privacy Act by contacting the TSA Headquarters Freedom of Information Act (FOIA) Office, at FOIA Officer, Transportation Security Administration, TSA-20, Arlington, VA 20598-6020. Access may be limited pursuant to exemptions asserted under 5 U.S.C. § 552a(k)(1) and (k)(2).

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may submit a Privacy Act request as described in section 7.1. In addition, individuals denied eligibility for enrollment into the TSA Pre✓™ Application Program will be advised of the basis for the denial and may submit information to correct missing or incorrect information (for example, if the CHRC reveals an arrest for a disqualifying crime, but there is no disposition information, the individual will be advised to submit disposition information to TSA).

7.3 How does the project notify individuals about the procedures for correcting their information?

TSA will provide information on the procedures for correcting information with its eligibility determination, and this PIA provides notice on how to correct information held by TSA. In addition, the TSA website provides information on how to submit a Privacy Act request.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not have an opportunity to correct, access, or amend their records maintained by TSA.

Mitigation: Individuals have an opportunity to check their data when it is submitted to TSA. In addition, individuals may seek access to TSA records by submitting a request under the Privacy Act, though some aspects of their record may be exempt from access.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

System administrators, security administrators, IT specialists, vetting operators, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Role-based access controls are employed to limit the access of information by different users and administrators based on the need to know the information for the performance of their official duties. TSA also employs processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA security officers. Program management was involved in the conduct and approval of this PIA.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All users are required to complete TSA-mandated Online Learning Center courses covering privacy. In addition, security training is provided, which helps to raise the level of awareness for protecting PII being processed. All IT security training is reported as required in the Federal Information Security Management Act of 2002, Pub. L. 107-347.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

All access requests are submitted in writing and individual access is granted by an authorizing official. Access to any part of the system is approved specifically for, and limited only to, users who have an official need for the information in the performance of their duties. External storage and communication devices are not permitted to interact with the system. All access to, and activity within,

the system are tracked by auditable logs. Audits will be conducted in accordance with TSA Information Security guidelines.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

New information sharing, uses, or access will be controlled in accordance with sections 8.2 and 8.3, and will be reviewed for compliance with this PIA.

Responsible Officials

Hao-Y Froemling
Transportation Security Administration
Office of Intelligence & Analysis
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security