Privacy Impact Assessment Update
for the
TSA Pre✓® Application Program

DHS/TSA/PIA-041(a)

January 22, 2016

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

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) operates its TSA Pre✓® Application Program to perform a security threat assessment on individuals who seek eligibility for expedited screening at participating U.S. airport security checkpoints. This PIA update covers two aspects of the program: 1) TSA will offer the ability to obtain a birth certificate certification through the National Association for Public Health Statistics and Information Systems (NAPHSIS); and 2) TSA will expand TSA Pre✓® Application Program capabilities by entering into agreements with private-sector entities for marketing, enrollment, identity assurance, and criminal records checks. As part of the latter expansion effort, TSA will share personally identifiable information collected by the TSA Pre✓® Application Program with DHS Science & Technology (S&T) Directorate to test the ability of the private sector to perform identity assurance and criminal history assessments.

Introduction

TSA Pre✓® is a passenger prescreening initiative that identifies lower 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 security resources on passengers who may be more likely to pose a threat to civil aviation, while also facilitating and improving the commercial aviation travel experience for the public.

TSA implemented the TSA Pre✓® Application Program pursuant to its authority under Section 109(a)(3) of the Aviation and Transportation Security Act (ATSA).[2] 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."

This PIA update covers two aspects of the program: 1) TSA will offer the ability to obtain a birth certificate certification through the National Association for Public Health Statistics and Information Systems (NAPHSIS); and 2) TSA will expand TSA Pre✓® Application Program capabilities by entering into agreements with private-sector entities for marketing, enrollment, identity assurance, and criminal records checks. As part of the latter

[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, keep their laptop in its case, and keep their 3-1-1 compliant liquids/gels bag in a carry-on. TSA Pre✓® lanes are available at more than 150 airports nationwide.
[2] Pub. L. 107-71 (115 Stat. 597, 613, Nov. 19, 2001, codified at 49 U.S.C. § 114 note).

expansion effort, TSA will share personally identifiable information (PII) collected by the TSA Pre✓® Application Program with DHS Science & Technology (S&T) Directorate to test the ability of the private sector to perform identity assurance and criminal history assessments. Unless otherwise noted, the information provided in previously published PIAs remains in effect. Individuals are encouraged to read all program PIAs to have an understanding of TSA's privacy assessment of the TSA Pre✓® Application Program.[3]

1) Birth Certificate Certification

Applicants to the TSA Pre✓® Application Program must provide documentation of their citizenship status. Applicants frequently are unable to enroll because they do not have a passport or birth certificate readily available to support their application.[4] NAPHSIS, an association of state agencies, operates the Electronic Verification of Vital Events (EVVE) system to check more than 250 million birth and death certificates in real time.[5] TSA will allow its TSA Pre✓® Application Program enrollment contractor to offer, as an optional service to applicants, the ability to access the EVVE system to obtain confirmation of their birth certificate. In addition to information collected for the TSA Pre✓® Application Program, applicants seeking to use EVVE will need to provide their mother's maiden name, which will be transmitted along with other required data, to the state authority that issues birth certificates for the state claimed by the applicant. NAPHSIS sees that a transaction has taken place for billing purposes, but does not access or retain the PII, which is encrypted while in transit.

2) TSA Pre✓® Application Program Expansion

TSA is seeking to expand the TSA Pre✓® Application Program by entering into agreements with one or more private-sector entities to provide marketing and enrollment services, and to perform identity assurance and criminal history assessments using commercial, publicly available, and public records data, and/or government records if available. Before operating under the agreement, DHS S&T will test the ability of the entity to perform identity assurance and criminal history assessments, with involvement and oversight from the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office. The private-sector entity will enter into a Cooperative Research and Development Agreement (CRADA) with S&T to complete the evaluation process. The entity will then use its systems to process a test dataset of PII collected by TSA from a subset of applicants who applied directly to TSA under the TSA Pre✓® Application Program. S&T will process and evaluate results, discuss outcomes, and provide results to TSA for consideration as part of the acquisition process. Prior to receiving

[3] Available at http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[4] Please visit www.tsa.gov for more information on how to apply for TSA Pre✓®, including what identity verification documents are required.

[5] Please visit www.naphsis.org/about-evve for more information on the EVVE system.

any PII, each entity entering into a CRADA must demonstrate its ability to purge from its systems and the systems data provider sources use, all the data S&T provides - including the TSA applicant data - during the evaluation, as well as the search histories and data generated by the entity during the evaluation. Confirmation of data destruction will be by written acknowledgement, verification of data logs, and other means as appropriate including inspection of contractor systems.

Contractors selected by TSA to provide expansion services will collect applicant name, date of birth, gender, country of birth, country of citizenship, Social Security number (optional), home address, contact information, photograph, fingerprints and/or iris scan,[6] and valid original or certified copies of TSA-approved identity documents. Depending on how the contractor proposes to operate to maximize enrollment, the application process may include an on-line registration process to be completed with an in-person enrollment, or may consist of an entirely in-person process.

Identity Assurance

Contractors will use commercial, publicly available, and public records data, and may propose using government records if available to them, to confirm the individual's identity. One option for confirmation may include a Knowledge-Based Authentication (KBA) quiz for the applicant based on personal data associated with the claimed identity. For those contractors using a KBA quiz, questions will be developed in real-time and their difficulty will dynamically adjust to a level at which only an individual with authentic personal knowledge can accurately answer. The data will only be used to validate an applicant's identity, and will not be used by contractors for any purposes other than for the TSA Pre✓® Application Program. An applicant may be denied at this step of the process if there is not enough information to establish identity or administer a KBA, or if the applicant fails the KBA. The KBA may be administered twice within 24 hours and no more than three times before the applicant will be required to establish his or her identity through personal appearance at a physical location.

Applicants directed to or enrolling at a physical location will provide original or certified copies of TSA-approved identity documents to further verify identity and provide biometrics.

Criminal Record Assessment

If the applicant's identity is confirmed, the contractor will perform a criminal history check using commercial, publicly available, and public records data, and/or government records

[6] Photograph, fingerprints, and/or iris scan will be used to verify the individual's identity when he or she is physically present at a TSA checkpoint, following successful enrollment in the TSA Pre✓® Application Program, except when the individual has expressly authorized by opting-in to other uses by the contractor.

if available, against the automatic disqualifying offenses used for the TSA Pre✓® Application Program. Because the TSA Pre✓® Application Program is voluntary, TSA may also direct that a significant overall criminal history be used as a disqualifier, even if the individual does not have convictions for a disqualifying offense. Applicants deemed ineligible based on their criminal records will be notified by the private sector entity of the disqualifying offense(s) and the reporting jurisdiction(s) so that the individual can seek to correct the record for reconsideration. If the individual is ultimately denied based upon criminal history, then the Contractor shall provide the denial information to TSA so that TSA may include them on a list of passengers who are ineligible for TSA Pre✓® expedited screening.

TSA Security Threat Assessment (STA)

Applicants who have passed the identity and criminal history prescreening processes will have their application transmitted to TSA for checks against Government databases and watch lists associated with security and immigration to determine eligibility, as well as a check against the TSA Pre✓® Passenger Disqualifying Protocol (PDP) list and a list of TSA Pre✓® Application Program applicants who have previously been determined as ineligible. TSA will retain the PII provided by the applicant, including fingerprints or other biometrics, but will not collect the commercial, publicly available, or public records data used by the private-sector entities for identity assurance.[7] TSA will receive criminal history records identified by the contractor. Biometrics will be linked to the applicant's identity and are expected to be used at the TSA checkpoint to confirm that the individual on the day of travel is, in fact, the same person who enrolled in the TSA Pre✓® Application Program. In addition, fingerprints will be enrolled in DHS National Protection and Programs Directorate/Office of Biometrics Identity Management (NPPD/OBIM) Automatic Biometric Identification System (IDENT) information technology platform for recurrent immigration, law enforcement, and intelligence checks, including checks against latent prints associated with unsolved crimes.

TSA will make the final determination on whether an applicant is accepted or denied for the TSA Pre✓® Application Program and will notify the applicant of his or her eligibility or ineligibility and any correction of record procedures. Eligibility for the TSA Pre✓® Application Program is within the sole discretion of TSA. Applicants will have an opportunity to correct cases of misidentification or inaccurate records for the TSA STA. With respect to immigration records, within 60 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 and correct any information believed to be inaccurate. TSA will review any information submitted and make a final decision. If a corrected record is not received by TSA,

[7] TSA may inspect underlying records for contract compliance purposes.

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.

TSA will issue a Known Traveler Number (KTN) to approved enrollees and provide status of the approval process (*e.g.*, in-process or complete) to private sector entities for customer service purposes. 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.

To be eligible for expedited screening in a TSA Pre✓® lane, the passenger will need to provide his or her KTN to the airline when making flight reservations. When the airline sends the passenger's Secure Flight Passenger Data (SFPD) 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 may 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✓® expedited screening is not yet available for all airports, all times, all airlines, or all flights.

Reason for the PIA Update

TSA is updating the PIA to reflect: 1) the use of EVVE to verify birth certificates for those applicants who opt to use that system; and 2) the expansion of application options for the TSA Pre✓® Application Program through the private sector. This PIA update also reflects that as part of the expansion effort, TSA will provide PII collected from a subset of applicants for the TSA Pre✓® Application Program to DHS S&T in order to test the capability of private-sector entities to perform identity assurance and criminal history checks.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

No change.

Characterization of the Information

Individuals who use EVVE to verify their birth certificate will provide their full name, gender, date of birth, state of birth, and mother's maiden name to the enrollment provider. EVVE will transmit the information to the state of birth and return a confirmation of birth certificate from that state. EVVE does not retain a record of the transaction. TSA's enrollment provider will retain the applicant's information and confirmation of birth certificate.

For TSA Pre✓® Application Program expansion, contractors will submit information to TSA from all applicants except those whose identity is unable to be validated. TSA will not receive the commercial, publicly available, or public record data used for identity assurance. TSA will receive criminal history information from applicants whose identity is validated. TSA and its contractors will collect the same information collected from individuals who apply directly to the existing TSA Pre✓® Application Program, including:

- full legal name and any aliases;
- residential address;
- mailing address if different than residential address;
- date of birth;
- Social Security number (voluntary, but recommended[8]);
- gender;
- photograph, fingerprints, and/or iris scan;
- city, state, and country of birth; and
- citizenship information, including immigration status and alien registration number (if applicable).

[8] 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.

For purposes of testing private sector capability to verify identity and perform a criminal history check, TSA will provide to DHS S&T the PII from a subset of individuals who have applied to the TSA Pre✓® Application Program, as well as criminal history records.

Uses of the Information

Information provided to TSA's enrollment contractor for EVVE to confirm their birth certificate will be used to confirm citizenship status.

TSA will use PII collected by the contractor 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. TSA expects to use the biometric to verify the identity of the individual presenting themselves at the TSA checkpoint when they travel. Further, biometrics enrolled in the DHS National Protection and Programs Directorate/Office of Biometrics Identity Management (NPPD/OBIM) Automatic Biometric Identification System (IDENT) IT platform will be recurrently checked for immigration, law enforcement, and intelligence purposes, including checks against latent prints associated with unsolved crimes.

As part of the TSA Pre✓® Application Program expansion effort, TSA will use PII for a subset of the applicants to the TSA Pre✓® Application Program for testing the capability of private sector entities to perform identity verification and criminal history assessments.

Privacy Risk: There is a risk that the contractor will come to an erroneous conclusion on identity or criminal history.

Mitigation: The risk is mitigated by providing the basis for the conclusion so that the individual can seek to correct his or her record by providing additional documentation to the private-sector entity, or the individual can separately apply directly to TSA with supporting identity documentation and with information on the alleged criminal offense. The individual can also choose to apply directly to TSA where a finger-print based CHRC will be conducted.

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 watch list. TSA will further mitigate the risk of misidentification through the identity verification performed by the private-sector entity under its agreement with TSA.

Privacy Risk: There is a risk associated with the use by DHS S&T of PII collected for the TSA Pre✓® Application Program for testing the capabilities of private-sector entities entering into agreements with TSA to expand enrollment options for the program.

Mitigation: The risk is mitigated by limiting the use of the information to testing the capabilities of the entities; no operational use will be made of any individual's test result, though TSA may investigate if the test reveals a fraudulent identity or criminal disqualifier. Further, the entities must purge the information after the test.

Privacy Risk: There is a risk that an individual may be implicated in an unsolved crime by the check against latent fingerprints that were collected at a crime scene.

Mitigation: Notice of the check against latent prints is provided in this PIA and in the Privacy Statement provided to the individual before enrolling. Individuals consent to provide their fingerprints.

Notice

TSA has updated its Privacy Notice to TSA Pre✓® Application Program applicants to expressly highlight that information may be shared with contractors and others performing or working on a contract, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to the system of records. While previously published to the public as a routine use in the TSA Pre✓® Application Program system of records notice published in September 2013, TSA provides additional notice in the Privacy Notice that applicants receive when enrolling.

Private-sector entities, under agreement with TSA, will issue an appropriate Privacy Act statement to individuals seeking to enroll in the TSA Pre✓® Application Program.

Privacy Risk: There is a risk that private-sector entities under agreement with TSA will use applicant information for other purposes.

Mitigation: The risk is mitigated by prohibiting other uses of applicant information unless expressly authorized by the applicant through an opt-in procedure.

Privacy Risk: There is a risk that individuals who provided PII to a private-sector entity will believe that they are applying directly to TSA, and will not understand that redress for the identity assurance and criminal history assessments performed by the entity is only available through the entity.

Mitigation: The risk is mitigated by the availability of the TSA Contact Center, which acts as a central point of inquiry to TSA that can appropriately direct a redress request. In addition, the entity must directly advise the individual of redress options.

Privacy Risk: There is a risk that individuals who provided PII to TSA in order to apply for the TSA Pre✓® Application Program would not have anticipated that their PII would be used in order to test the capability of commercial entities to perform identity assurance and criminal history assessments for the program.

Mitigation: TSA has amended its Privacy Notice for enrollment in the TSA Pre✓® Application Program to expressly reflect that information may be shared with contractors. TSA will only use information for testing from individuals who applied subsequent to that change in the Privacy Notice. The information is used for a very limited test purpose associated with the TSA Pre✓® Application Program.

Data Retention by the Project

TSA will receive and retain information on individuals identified by contractors as being disqualified based on their criminal history, and will place such individuals on a list of passengers who are ineligible for TSA Pre✓® expedited screening. Individuals may be retained on the list of TSA Pre✓® ineligible passengers permanently or may come off the list if their disqualifying crime is one that is time-limited (for example, some offenses may not be disqualifying if the application is more than 7 years after conviction).

DHS S&T will retain the PII provided by TSA and the results from identity assurance and criminal history assessments for purposes of the testing, and will delete these data once evaluation of the test is complete.[9]

Privacy Risk: There is a risk that test data may be retained longer than necessary.

Mitigation: The risk is mitigated by DHS S&T maintaining information in accordance with a NARA-approved retention schedule. Entities participating in the test will only be tested after executing a CRADA and Statement of Work that mandates that the commercial entity document their ability, in addition to any of their subcontractors or data sources, to purge all TSA provided records and entity search histories and results when testing is complete or as directed by TSA.

Information Sharing

TSA will provide PII to DHS S&T so that it can perform testing functions on behalf of TSA for the TSA Pre✓® Application Program expansion.

[9]See http://www.dhs.gov/publication/dhs-st-pia%E2%80%93027-st-test-data.

Privacy Risk: There is a privacy risk that individuals will not understand that their PII may be shared within DHS and to the contractors.

Mitigation: The risk is mitigated by the publication of this PIA, and by using only information collected from individuals who enrolled with the Privacy Notice language expressly identifying the sharing of information with contractors. TSA and DHS S&T also mitigate this risk by using the PII only for purposes of the test. There will be no impact to the individual from any result of the test, though TSA will investigate if the test reveals that an identity is not assured or that a criminal history may exist. Test data will be destroyed following completion of the test evaluation. DHS S&T privacy protections for test data are described in its own PIA.

For those applicants who opt to use the EVVE system to certify their birth certificate, TSA's enrollment provider will share information with NAPHSIS and the state that the applicant claims issued their birth certificate.

Redress

Individuals who opt to use the EVVE system to obtain their birth certificate confirmation, but for whom no confirmation is obtained, may provide an official birth certificate through other means or prove citizenship through a passport.

Individuals who are unable to establish their identity through the contractor process may choose to apply directly to the TSA Pre✓® Application Program with supporting documentation for their identity. Applicants deemed ineligible based on a criminal offense will be notified by the private-sector entity of the disqualifying offense and the reporting jurisdiction so that the individual can seek to correct the record for reconsideration. There is no waiver or appeal process for criminal disqualifiers in the TSA Pre✓® Application Program.

Privacy Risk: There is a risk that individuals will be unable to correct, access, or amend records maintained by private-sector entities.

Mitigation: This is a risk that cannot be mitigated by this program. TSA cannot mandate that private-sector entities correct records they obtain from other sources. TSA does, however, mandate that those entities identify the crime and reporting jurisdiction so that the individual can correct any errors.

Auditing and Accountability

No change.

Responsible Official

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

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security