Privacy Impact Assessment
for the

Travel Protocol Office Program

DHS/TSA/PIA-043

March 26, 2014

Contact Point
Daryush Mazhari
Program Manager, Stakeholder Management Branch
Transportation Security Administration
Daryush.Mazhari@tsa.dhs.gov

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

Abstract

The Transportation Security Administration (TSA) established the Travel Protocol Office (TPO) to support and facilitate the movement of eligible travelers whose presence at a security screening checkpoint may distract other travelers and/or reduce the efficiency of the screening process. TSA plans to collect limited personally identifiable information (PII) on these individuals in order to facilitate airport transit and to conduct security screening operations. The TPO Program applies to commercial airports within the continental United States and its territories. Because this program entails collecting information about members of the public in identifiable form, the E-Government Act of 2002 requires that TSA conduct a Privacy Impact Assessment.

Overview

Pursuant to 49 U.S.C. § 114, TSA conducts security screening operations at airport security checkpoints. To alleviate distractions at the checkpoint for travelers, as well as any attendant loss of screening efficiency, TSA created the TPO to manage airport transit and security screening for certain travelers, including but not limited to Members of the U.S. Congress, accredited ambassadors to the United States, dignitaries, foreign ministers, political figures, and other eligible travelers that have special needs and/or request assistance. At the request of an airport, airline, or the unexpected arrival of an individual meeting the parameters of the program at a checkpoint, TSA may provide *ad hoc* security screening assistance in instances when an individual's presence could potentially cause distractions or disruptions to the screening process. Individuals traveling with eligible travelers will also receive airport security assistance.

To support and facilitate eligible traveler's transit and security screening, TSA receives advance notification via phone, email, or fax from the point of contact representing the individual, directly from the individual (including co-travelers) or airport/airline managers prior to the flight departure time. TSA Security Coordination Centers (SCC) or Customer Support Representatives (CSR) located at each airport may receive ad hoc requests directly from airports and airlines. The notification provides TSA with the individual's name, title, point of contact, phone number, travel information,[1] and the nationality of foreign dignitaries when applicable.

Once TSA receives the notification, TPO Program Administrators submit a Travel Support Request containing the individual's information to the TSA Federal Security Director (FSD) and/or the SCC at the departure airport. The FSD or his/her designee arranges to greet the requester at a specific location in order to accommodate the request. The FSD or his/her designee will notify the TPO after completion of the support and convey whether TSA encountered any matters of concern during transit and/or screening.

TSA will retain information regarding the request and travel for three years in a secure Microsoft Access database.

---

[1] Travel information includes: Airport, airline, flight number, and departure date/time.

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?

Pursuant to 49 U.S.C. § 114, TSA is responsible for security in all modes of transportation. TSA is also responsible for screening all passengers and property. 49 U.S.C. § 44901.

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

DHS/TSA-001 Transportation Security Enforcement Record System (TSERS) System of Records Notice (SORN).[2]

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

No. This program does not involve an IT system that prompts Federal Information Security Management Act (FISMA) requirements for the development of a system security plan. The data will reside in a password-protected Microsoft Access database, with user-level security features.

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

Yes. Per NARA Record Schedule N1-560-10-001, Item 5 (see Section 5.0).

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.

TSA determined that the information collected by the TPO Program meets the parameters of the Paperwork Reduction Act (PRA) requirement. TSA initiated the PRA submission process for the recently submitted form associated with the TPO Program.

Section 2.0 Characterization of the Information

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

TSA will collect the individual's name, title, point of contact, phone number, travel information, and the nationality of foreign dignitaries when applicable. Travel information includes airport, airline, flight number, and departure date and time.

---

[2] 78 FR 73868, December 19, 2013.

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

TSA will collect information from the point of contact representing the individual, directly from the individual, and from individuals traveling with eligible travelers.

TSA collects the information via phone, email, or fax prior to the flight departure time. TSA may also receive *ad hoc* requests via the SCC or CSR located at each airport.

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.

2.4 Discuss how accuracy of the data is ensured.

TSA maintains accuracy of the information by collecting a limited amount of data (name, title, point of contact information, travel information, and nationality when applicable) directly from a trusted representative, the individual (including co-travelers), or airport/airline managers.

2.5 <u>Privacy Impact Analysis</u>: Related to Characterization of the Information

<u>Privacy Risk:</u> There is a risk that travel information pertaining to a celebrity may be exposed.

<u>Mitigation:</u> TSA restricts access to the database to a limited number of employees. Misuse of official information will be grounds for disciplinary action.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

TSA uses the eligible traveler's name, title, point of contact information, travel information, and nationality when applicable in order to support and facilitate airport transit and to complete the security screening process to alleviate distractions at the checkpoint for travelers, as well as any attendant loss of screening efficiency. TSA submits the individual's information to the TSA FSD and/or the SCC at the departure airport in order to complete the support request.

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?

No.

3.4 <u>Privacy Impact Analysis</u>: Related to the Uses of Information

<u>Privacy Risk</u>: There is a risk that unauthorized individuals may access the data.

<u>Mitigation</u>: TSA mitigates this risk by limiting access to the database to TPO personnel that have a need to know the information in order to facilitate the traveler's airport transit and to complete the security screening process. This risk is further mitigated by limiting access to the TSA FSD and/or his or her designee.

<u>Privacy Risk</u>: There is a risk that PII obtained for airport transit and screening support may be used for unrelated purposes.

<u>Mitigation</u>: By limiting the information to the individual's name, title, point of contact information, travel information, and nationality when applicable, TSA mitigates the risk that TPO personnel may use the information for unrelated purposes. The limited PII reduces the ability of TSA personnel to use the information for other programs and/or systems.

Section 4.0 Notice

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

In response to a request for screening assistance, TSA will provide a Privacy Act statement directly to the individual (including co-travelers), representatives submitting information on their behalf or to airport/airline managers via email, fax, or upon arrival at the screening location. The publication of this PIA also serves as notice by providing awareness of how TSA will use, disseminate, and retain the information.

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

By providing the requested information, individuals consent to the use of the information in order to facilitate their movement through the airport and/or the security screening process. Individuals have the opportunity to decline to participate in this program and undergo normal airport transit and security screening procedures.

4.3 <u>Privacy Impact Analysis</u>: Related to Notice

<u>Privacy Risk</u>: Although this is a voluntary program, there is a risk that the individual does not know exactly how TSA will use his or her information in order to facilitate airport transit and to complete the security screening process.

Mitigation: TSA mitigates this risk by providing a Privacy Act statement to the traveler at the time of information collection or for *ad hoc* support, upon arrival for security screening. TSA further mitigates this risk by publishing this PIA, which provides awareness of how TSA will use, disseminate, and retain the information.

Section 5.0 Data Retention by the project

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

TSA will retain this information for three years.

TSA retains this information for TPO staffing purposes and in order to obtain metrics. For example, TSA obtains the number of eligible travelers, dates of travel, and departure airport in order to assess the programs performance and to monitor eligible traveler support trends. In addition, TSA uses the information to address incidents in which TSA employees handle eligible travelers inappropriately. The information is also retained in accordance with the approved NARA retention schedule established for customer service requests and response documentation.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the TPO retains data longer than necessary to accomplish its mission.

Mitigation: This risk is mitigated by the fact that the retention schedule is consistent with the approved NARA records retention schedule for TSA customer service requests and response documentation. Use of the information for statistical analysis and staffing purposes is consistent with accomplishing the purposes of this program.

Section 6.0 Information Sharing

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.

In the normal course, TSA does not share information outside of DHS except to the extent needed for coordination with the point of contact for the individual traveling.

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

As noted, PII is typically not disclosed outside TSA since the screening function is performed by TSA. Routine use S allows DHS to disclose information with 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.

6.3　　Does the project place limitations on re-dissemination?

The TPO Program shares travel information in order to facilitate travel by the individual, which may require re-dissemination of the information by the individual's representative or airport facility operators. TSA does not limit re-dissemination of travel information by recipients, except to the extent that details of movement through the airport may constitute Sensitive Security Information (SSI) pursuant to regulations involving non-disclosure of security information. Re-dissemination of SSI is limited by the SSI regulation, Protection of Sensitive Information.[3]

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

In the normal course, TSA does not disclose information outside of the Department except as required to facilitate travel by the individual.

6.5　　Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: TSA mitigates this privacy risk by limiting access to the information to individuals responsible for coordinating travel by the individual. Misuse of official information is grounds for discipline.

Section 7.0 Redress

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

Individuals have the opportunity to access their information directly from the TPO Program Administrator or the representative or airport/airline manager that submitted the information on their behalf.

Pursuant to the Privacy Act, individuals may request access to their data by contacting the TSA Freedom of Information Act (FOIA) Office, at Transportation Security Administration, TSA-20, 601 South 12th Street, Arlington, VA 20598-6020. Although access to portions of the system may be limited pursuant to exemptions asserted under 5 U.S.C. § 552a (k)(1), (k)(2), and (j)(2) for the systems of record under which the TPO Program operates, individuals may access information that they submitted to TSA, such as: name, gender, date of birth, and flight information.

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

Individuals may have an opportunity to correct their information when it is being collected by the representative or airport/airline manager submitting it on their behalf or by contacting a TPO Program Administrator; otherwise, they may submit a Privacy Act request as described in 7.1.

---

[3] 49 CFR 1520.

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

This PIA serves as notice to the individual about how to correct their information once obtained by the TPO. In addition, TSA provides notice to individuals via the DHS/TSA-001, TSERS SORN.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that redress options related to the TPO Program are limited.

Mitigation: Redress limitations within the TPO Program are mitigated by the fact that the program does not make operational decisions on individuals. The TPO Program is principally a program designed to manage airport transit and security screening for individuals whose presence at the checkpoint may distract other travelers and/or reduce the efficiency of the screening process. Individuals have an opportunity to correct their information when it is being collected by the representative or airport/airline manager submitting it on their behalf or by contacting a TPO Program Administrator; otherwise, they may submit a Privacy Act request as described in 7.1.

Section 8.0 Auditing and Accountability

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

TPO Program Administrators and Information System Security Officers conduct biannual manual audits of the database to verify data accuracy, monitor system security, and to ensure that all users adhere to established policies and/or procedures.

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

All TSA employees and contractors are required to complete annual mandatory privacy training provided by DHS that emphasizes sensitive PII handling safeguards. In addition, TPO Program Administrators provide specific database usage and information technology security training to all users.

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

TPO Program Administrators restrict access to the database to TPO employees. As TPO users arrive and/or depart the office, a system administrator activates/deactivates accounts. Transportation Security Officers detailed to the TPO must undergo a stringent interview process and receive specific database usage and information technology security training.

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?

Only TSA personnel will use the TPO Program database. New users and new access will be controlled in accordance with sections 8.2 and 8.3, and will be reviewed annually for compliance with this PIA.

Responsible Officials

Daryush Mazhari
Program Manager, Stakeholder Management Branch
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security