Privacy Impact Assessment
for the

Office of Intelligence & Analysis Trends and Patterns Branch

DHS/TSA/PIA-039

November 14, 2012

Contact Point
Joseph Salvator
Office of Intelligence & Analysis
Transportation Security Administration
Joseph.Salvator@dhs.gov

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

Abstract

The Transportation Security Administration (TSA), Trends and Patterns Branch (TPB) seeks to improve the ability to identify potential risks to transportation security by discovering and analyzing previously unknown links or patterns among individuals who undergo a TSA security threat assessment, aviation passengers identified as a match to a watch list, and passengers who do not present acceptable identification documents to access the sterile area of an airport whose identity is unverified. TSA is conducting this Privacy Impact Assessment (PIA) because the TPB will collect and use personally identifiable information (PII) to perform these functions.

Overview

TSA performs security threat assessments on workers within a variety of transportation sectors pursuant to its authorities under the Aviation and Transportation Security Act, 49 U.S.C. § 114. Privacy Impact Assessments (PIAs) have been conducted for those programs and can be found on the DHS website[1]. In general, those programs involve the collection of information from the worker that TSA uses to perform security threat assessments by matching biographical and, when applicable, biometric data against federal government databases in order to identify potential risks to transportation security. Under its Secure Flight program, TSA seeks to identify and prevent known or suspected terrorists or other individuals from gaining access to airports and airplanes where they may jeopardize the lives of passengers and others.[2] To identify those who present a threat to aviation security, the Secure Flight program compares passenger and non-traveler information to the No Fly and Selectee List components of the Terrorist Screening Center Database (TSDB)[3] and, when warranted by security considerations, other watch lists maintained by TSA or other federal agencies. When individuals attempt to enter the sterile area[4] but fail to present acceptable identification documents, TSA works with the individual to attempt to verify their identity. Those for whom TSA is unable to verify identity may be prevented from entering the sterile area.

The TSA Office of Intelligence and Analysis (OIA), Trends and Patterns Branch (TPB) seeks to improve the ability to identify potential risks to transportation security by searching for, discovering, and analyzing previously unknown links, trends, and/or patterns among the foregoing individuals. For example, the TPB may match information across the populations that indicate a previously unknown link between a transportation sector worker and an individual in the TSDB. Similarly, the TPB may identify that an individual failing to present acceptable identification is on a flight with one or more individuals in the TSDB. In both cases, TPB analysts might determine that further investigation or operational response is warranted and refer the information to appropriate officials for follow-up. TSA is conducting this PIA

[1] http://www.dhs.gov/files/publications/gc_1280763432440.shtm
[2] Secure Flight PIA and updates can be found at: http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[3] For additional information about the TSDB, see http://www.fbi.gov/about-us/nsb/tsc/tsc_faqs.
[4] A "sterile area" is a portion of airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator under 49 C.F.R. part 1544, or a foreign air carrier under 49 C.F.R. part 1546 through the screening of persons and property. 49 C.F.R. § 1540.5.

under the E-Government Act of 2002 because the TPB will collect and use personally identifiable information (PII) to perform these functions.

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 pursuant to 49 U.S.C. § 114(d). TSA is required to "receive, assess, and distribute intelligence information related to transportation security" as well as to "assess threats to transportation" pursuant to 49 U.S.C. § 114(f). TPB functions are directly related to TSA's statutory requirement to assess transportation security risks.

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

Transportation Security Threat Assessment System (TSTAS), DHS/TSA-002, 75 FR 28046, May 19, 2010; Secure Flight Records, DHS/TSA-019, 72 FR 63711, November 9, 2007; Transportation Security Enforcement Record System (TSERS), DHS/TSA-001, 75 FR 28042, May 19, 2010; and Transportation Security Intelligence Service Operations Files, DHS/TSA-011, 75 FR 11867, April 13, 2010.

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

Yes. The Authority to Operate (ATO) was granted on August 31, 2011.

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

Yes. Records retention schedules existing for the data inputs will be applied by the TPB. In addition, the work product generated by TPB analysts will be retained in accordance with existing approved records retention schedules (see section 5.1).

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.

TPB does not require any new information collection and thus does not implicate the PRA.

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 collects PII about persons who are applicants for, or holders of, credentials, or who seek access to transportation facilities, assets, or information. The specific identifying information collected is specified within each of the applicable program PIAs.[5] TPB will use the data to conduct supplemental analysis of individuals, and to establish links and patterns that may indicate a risk to transportation security. The data will be retained by the TPB for use in subsequent assessments of the individuals.

TPB analysts may reference a wide variety of other data as part of the manual review of links or patterns, including both PII and non-PII collected by TSA, other government agencies, and commercial and public sources. PII pertaining to members of the public may include such items as:

- Name
- Government issued identification numbers
- Physical description
- DOB
- Place of birth
- Gender
- Address
- Contact information
- Military status
- Watchlist status
- Results of law enforcement and immigration checks
- Employment information
- Date, place, and type of flight training or other instruction
- Flight information, including crew status on board
- Travel document information
- Level of access at an airport of other transportation facility, including termination or expiration of access
- Other information provided by federal, state, local, and tribal government agencies or private entities relevant to the assessment, investigation, or evaluation.
- Results of any analysis performed for security threat assessments and adjudications

TPB will also collect full name, gender, date of birth, and passport information (when available) for passengers and individuals seeking access to the sterile area through the Secure Flight system, and will collect information provided by the individual during the identity verification process for individuals who are unable to present acceptable identification documents at the checkpoint. PII from Secure Flight will be collected, used, or maintained by TPB only from members of the public identified as a match to a government watch list. Information collected as part of the identity verification process varies as

[5] PIAs for TSA vetting programs can be found at http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

necessary to respond to knowledge-based queries to verify the individual's identity. For example, home address information may develop further inquiries that will assist in verifying identity. Immigration information may be used to assist foreign nationals in verifying identity, for example when a foreign national's entry into the country is documented. TPB will collect information on individuals who are unable to verify identity for use in identifying potential threats to aviation.

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

As discussed above, TPB receives information from existing TSA programs[6] that collect information from the individual either directly or through an employer, transportation facility owner, airline, or reservation agent. TPB will also use information from TSA systems, other classified and non-classified government databases, as well as information available publicly and from commercial databases for use in discovering and analyzing links and patterns that may indicate a potential risk to transportation security. TPB will not search within the Secure Flight system but Secure Flight watch list matches will be reported to the TPB.

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

Commercial and publicly available information may be used by the TPB to research identified risks. It will enrich the data available for a full security threat assessment of individuals seeking or holding a credential that grants access to transportation facilities, assets, or Sensitive Security Information. For example, such data may establish that an address provided by an applicant for, or holder of, a credential to a transportation facility might be linked to individuals on government watch lists or that the address may be a fabrication. Other commercial and publicly available data sources provide non-PII data such as flight statistics available on the U.S. Department of Transportation Research and Innovative Technology Administration website.

2.4 Discuss how accuracy of the data is ensured.

TPB relies on the accuracy of the existing databases from which it will pull data. Once the data reaches TPB's analytic layer, its format may be modified and standardized but will not be changed in substance. For example, if one of the underlying databases feeds address information using a different format, TPB will alter the address format to permit rule-based searches. The original format of the data, however, will be logged and auditable.

---

[6] Applicable TSA vetting programs include, but are not limited to Hazardous Materials Endorsement, Airspace Waiver and Flight Authorizations for Certain Aviation Operations, Crew Vetting Program, Airport Access Authorization to Commercial Establishments Beyond the Screening Checkpoint, Airmen Certificate Vetting Program, TWIC, Federal Flight Deck Officer, Large Aircraft Security Program, Secure Flight, Air Cargo, STA for Airport Badge and Credential Holders, Maryland-Three Airports, Alien Flight Student Program.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that TPB will perform search functions that could previously only have been performed in separate searches within each individual database, allowing users more access to a larger amount of data.

Mitigation: Privacy concerns that might be associated with the discovery of possible threats to transportation will be mitigated by strictly controlling access to the TPB analytic subsystem to a limited number of OIA analysts with clearances. Privacy risks are further mitigated because TBP users already have access to the individual underlying databases; the search capability merely streamlines already existing processes and capabilities.

Privacy Risk: There is a risk of inaccurate information when it is collected from someone other than the individual, for example, from commercial or publicly available data.

Mitigation: Most of the information used by the TPB is collected from the individual, whether it is supplied by the applicant for a credential, the passenger identified as a watch list match through Secure Flight, or the passenger at the security checkpoint whose identity remains unverified. Commercial or publicly available data may identify a potential link to be researched.

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.

TPB will use the information collected to discover potential transportation security risks that might not have been apparent through watch list matching processes. TPB will also analyze potential transportation security risks that may be revealed by information on aviation passengers who have been identified as matches to watch lists or who have been denied access to the sterile area for failure to verify their identity. TPB accomplishes this by identifying matches of information elements across and within populations, which are then evaluated by analysts for significance. For example, if Secure Flight watch list matching reveals several individuals who are matches to a watch list scheduled for a single flight, TPB will refer this information within TSA or to an appropriate external agency such as the Terrorist Screening Center (TSC) for possible operational response.

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.

The TPB will use technology to identify subject-based links among individuals and seek matches to known activity patterns and anomalies that may indicate risks to transportation security.

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

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of disclosure of PII to individuals without authorized access.

Mitigation: TSA will secure personal information against unauthorized use through the use of a layered security approach involving procedural and information security safeguards. The data will be encrypted using National Institute of Science and Technology (NIST) and Federal Information Security Management Act (FISMA) standards and industry best practices when being transferred between secure workstations. Only TSA employees and contractors with proper security credentials and passwords will have access to this information to conduct the security threat assessment. Moreover, all TSA and assigned contractor staff receive DHS-mandated privacy training on the use and disclosure of PII.

Specific privacy safeguards include:

- Technical limitations on, and tracking of, data access and use;
- Use of secure telecommunications techniques; and
- Limitation of physical access to system databases and workstations.

Privacy Risk: There may be a risk that information used by TPB is not relevant to its mission.

Mitigation: TPB use of information is compatible with the purpose for which it was originally collected by TSA; that is, to further the mission of transportation security.

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 provides notice to individuals of the collection of the information by TSA and its use for security purposes. Notice is provided when the information is collected, as well as through the PIAs associated with each underlying program, and for some populations through formal rulemaking published in the Federal Register.

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

Individuals can decline to provide information to TSA but will not be able to complete the security risk assessment associated with the underlying program. Once the information is provided to TSA, there is no opportunity to consent, decline, or opt out of information being provided to the TPB.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals do not have notice that TPB will evaluate the risk to transportation posed by the individual.

Mitigation: The risk is mitigated by the fact that information used by the TPB comes from individuals who submit information to TSA for a security threat assessment, from passengers as part of the Secure Flight program who have been identified as matches to a watch list, or from passengers seeking access to the sterile area whose identity remains unverified. These individuals are provided notice that TSA will examine the information they submit to identify risk to transportation security. The TPB is a part of TSA that exists to identify potential risks to transportation security.

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.

TPB will retain records on individuals in accordance with the retention schedule for the systems that provide the underlying information. Records on transportation sector workers undergoing a TSA security threat assessment are retained as follows: 1) those who do not match a watch list will be retained for one year after the individual no longer requires access or a credential; 2) those identified as a possible match to a watch list will be retained for seven years; and 3) confirmed matches will be retained for 99 years. Information on individuals denied access to sterile areas of an airport due to the inability to verify their identity will be retained for three years. Information on individuals identified by Secure Flight as a match to a watch list will be retained for 99 years, while unconfirmed matches will be retained for seven years. Final analyst reports will be retained for thirty years.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the TPB retains data longer than necessary to accomplish its mission in accordance with source system record retention policies.

Mitigation: This risk is mitigated by the fact that reports and query results will be maintained under the same schedule as the source systems. Retention of query results relating to security threats is aligned with the purpose and mission of TSA, and permitting the underlying system to delete information when it is no longer needed by that system protects PII by reducing the proliferation of the data.

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 individuals suspected of posing a risk to transportation security may be shared outside DHS. In the ordinary course, such sharing will be with the Federal Bureau of Investigation (FBI) for investigation or operational response. TSA may also share information with transportation facility and asset owners and operators, and state or local law enforcement. Sharing outside DHS will be pursuant to the Privacy Act and routine uses published in the applicable system of records notice Transportation Security Threat Assessment System (TSTAS), DHS/TSA-002, 75 FR 28046, May 19, 2010; Secure Flight Records, DHS/TSA-019, 72 FR 63711, November 9, 2007; Transportation Security Enforcement Record System (TSERS), DHS/TSA-001, 75 FR 28042, May 19, 2010; and Transportation Security Intelligence Service Operations Files, DHS/TSA-011, 75 FR 11867, April 13, 2010.

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

The external sharing described in 6.1 is compatible with routine uses G, I, and N in system of record notice DHS/TSA-002; routine uses 5, 1, and 3 in DHS/TSA-019; routine uses G, I, and N in DHS/TSA-001; and routine uses G, R, and S in DHS/TSA-011.

6.3 Does the project place limitations on re-dissemination?

Yes. Information shared externally is Sensitive Security Information and must be handled and protected in accordance with 49 U.S.C. § 114(r) and 49 CFR Part 1520.

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

Disclosures outside the agency by TPB are recorded both manually within investigative files and automatically in an output report. All reports will be logged and searchable.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be disclosed beyond what would have been contemplated in the underlying systems.

Mitigation: This privacy risk is mitigated by implementing appropriate IT security and access controls, limiting the number of authorized users of the system, and by limiting the sharing of information to those who have an official need to know and then only in accordance with DHS information sharing policies and procedures.

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) for the Transportation Security Threat Assessment System (TSTAS), DHS/TSA 002 system of record.

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 data when it is being collected by the TSA program that supplies data used by the TPB; otherwise, they may submit a Privacy Act request as described in 7.1. An individual may also correct or update his or her information through the program that initially collected the information (*e.g.,* Transportation Worker Identification Credential (TWIC), Hazmat Endorsement, etc.).

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

The TPB has no direct interaction with any individual and other than the procedures discussed in 7.2 of this PIA, does not notify individuals about procedures to correct information, instead relying on source program processes and procedures to provide the necessary notifications.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals cannot correct erroneous information about themselves.

Mitigation: TPB relies on the accuracy of the information collected by the underlying systems that supply information to TPB. Those systems collect information from the individual involved and provide an opportunity to ensure accurate data submission to the programs for which the security threat

assessment is performed, when the individual is matched by Secure Flight to a watch list, or when the individual is unable to verify their identity at an airport checkpoint.

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?

All TPB system user access can be analyzed and audited by the system owner and Information System Security Officer to ensure that data and reports are accessed only by individuals with a need-to-know and for authorized purposes. 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 (OLC) courses covering privacy. In addition, system-specific training is provided to users in the proper and secure use of the applications.

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 to the administrators of the TPB system in writing and individual access is granted by an authorizing official. Access to any part of the TPB 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?

The TPB system will be used only by internal users. New uses and new access will be controlled in accordance with sections 8.2 and 8.3, and will be reviewed for compliance with this PIA. An annual review will be conducted by the TSA Privacy Office.

Responsible Officials

Joseph Salvator
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