Privacy Impact Assessment

for the

Security Threat Assessment for Conditional Access to Sensitive Security Information

DHS/TSA/PIA-045

August 5, 2014

Contact Point

Inga Dawson

TSA-OLE

Inga.Dawson@tsa.dhs.gov

Reviewing Official

Karen L. Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717

Abstract

The Transportation Security Administration (TSA) occasionally discloses Sensitive Security Information (SSI)[1] to individuals so that they can assist with the design, implementation, or review of TSA security programs, techniques, or technology, or when needed to understand TSA functions. TSA may conclude that the individuals must undergo a security threat assessment (STA) as a condition of being granted access to the SSI. This Privacy Impact Assessment (PIA) is conducted pursuant to the privacy provisions of the E-Government Act of 2002[2] because TSA will collect, maintain, and disseminate information in identifiable form on members of the public in order to conduct the STA.

Overview

Among the authorities transferred to TSA at its creation from the Department of Transportation was the authority governing the protection of certain information related to transportation security.[3] By law, and subsequent implementing regulations, certain information has been identified as constituting SSI, the public release of which would be detrimental to the security of transportation. Individuals may only access SSI if they are a covered person with a need to know as defined by the regulation.[4] The TSA Administrator may authorize a conditional disclosure of specified records that constitute SSI, subject to limitations and restrictions that render the disclosure not detrimental to transportation security.[5] On occasion, TSA may have a need for assistance or advice on its security programs, techniques, or technologies from individuals who might not fall within an existing category of covered person, or may want to provide SSI to individuals so they understand TSA functions. As one of the conditions for granting access to the specified SSI, TSA may require that the individuals undergo a STA consisting of a check against federal terrorism watch lists. For example, TSA may share SSI with civil rights advocacy groups in order to assess concerns with racial profiling.

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's general operating authorities for security in all modes of transportation are set forth in Title 49 of the United States Code.[6] In addition, TSA is authorized to receive, assess, and distribute intelligence information related to transportation security, as well as assess threats and develop policies, strategies, and plans for dealing with threats to transportation security.[7]

---

[1] 49 U.S.C. § 114(r).
[2] http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.
[3] 49 U.S.C. §§ 114(d), 40119.
[4] 49 C.F.R. parts 1520.7 and 1520.11.
[5] 49 C.F.R. part 1520.15(e).
[6] 49 U.S.C. § 114(d).
[7] 49 U.S.C. § 114(f).

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

DHS/TSA-002, Transportation Security Threat Assessment System (T-STAS).[8]

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

Yes. TSA issued an Authority to Operate (ATO) to the Technology Infrastructure Modernization (TIM) system[9] on March 12, 2014.

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.

The collection of information is exempt from the PRA pursuant to 5 CFR 1320.3(h)(1).

Section 2.0 Characterization of the Information

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

TSA will collect full name, date of birth, and gender to conduct the STA. In the event that there is a possible match to a watch list, TSA may seek other identifying information to resolve the possible match. The information collected may vary from person to person depending on the information in the matching database.

TSA will maintain the results of the STA, which includes derogatory information, and information provided by individuals during the resolution of any possible watch list match.

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

TSA collects the name, gender, and date of birth directly from the individuals identified by TSA for conditional release of SSI. The information is collected by email or by phone from the individual since the number of individuals is typically very small and permits a manual process.

---

[8] May 19, 2010, 75 FR 28046. See DHS/TSA-002 T-STAS SORN at http://www.gpo.gov/fdsys/pkg/FR-2010-05-19/html/2010-11919.htm.

[9] For more information about the TIM system, see DHS/TSA/PIA-042 TSA OIA TIM Program PIA at http://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-oia-technology-infrastructure-modernization-program-03-26-14.pdf.

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 relies on the individual submitting the information to ensure the accuracy of the data. An individual has an opportunity to review and correct errors before submitting information to TSA.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that an applicant may be incorrectly identified as a match to information contained in intelligence databases.

Mitigation: TSA reduces this risk by requiring data elements that should be sufficient to distinguish most applicants from individuals who are identified as a match to information contained in intelligence databases. TSA further reduces the risk by working with the individual to resolve any potential error in identification.

Privacy Risk: There is a risk that the individual collecting applicant information may mishandle the information.

Mitigation: TSA reduces this risk by emphasizing data security practices, and requires annual training on handling of Personally Identifiable Information (PII).

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

TSA uses PII to perform a STA on individuals who otherwise are not covered persons under the SSI regulation, but who require access to SSI in order to provide assistance or advice on TSA security programs, techniques, or technologies. TSA will conduct checks against terrorism databases as part of the STA.

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 Privacy Impact Analysis: Related to the Uses of Information

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

Mitigation: 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. System users receive privacy training, and system managers were involved in the drafting of this PIA.

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.

A TSA representative who has sponsored the conditional release of SSI will notify the individual that the PII is being collected for purposes of conducting a STA for access to SSI. In addition, TSA provides notice by issuing this PIA.

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

Individuals may decline to provide information to conduct the STA, but will be denied access to the SSI if they choose to do so, and may be unable to assist TSA with its security programs, techniques, or technology.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not know how their information is used.

Mitigation: TSA reduces this risk by providing information when the individual is contacted regarding providing TSA with assistance, as well as this PIA and the DHS/TSA-002 T-STAS SORN. Moreover, the population covered by this PIA is comprised of individuals who have agreed to assist TSA and generally can be expected to understand the purpose of providing 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 information on an individual 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 TSA is notified or has knowledge that any credential, access, or privilege granted based upon a STA is no longer valid.

- 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 the STA or one year after TSA is notified or has knowledge that any credential, access, or privilege granted based upon a STA is no longer valid, whichever is longer.
- 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,[10] or seven years after TSA learns that the individual is deceased, whichever is earlier.

5.2 Privacy Impact Analysis: Related to Retention

TSA has not identified any significant unique privacy risks associated with the retention schedule.

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 normal agency operations involving this population, TSA does not expect to share information outside of DHS, except to the extent that there is a need to share with the Federal Bureau of Investigation (FBI) and Terrorist Screening Center (TSC) in order to conduct the STA.

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

External sharing is compatible with the purpose of the system, which is to conduct a STA on regulated populations or others seeking access to security information.

DHS/TSA-002, T-STAS System of Records, Routine Use K permits DHS to share information with a federal, state, local, tribal, territorial, foreign, or international agency, if necessary to obtain information relevant to a DHS/TSA decision concerning an initial or recurrent STA; the hiring or retention of an employee; the issuance of a security clearance, license, endorsement, contract, grant, waiver, credential, or other benefits; and to facilitate any associated payment and accounting.

6.3 Does the project place limitations on re-dissemination?

TSA does not place limitations on re-dissemination of information by the TSC except to the extent match information is SSI pursuant to regulations involving non-disclosure of security information.[11] Re-dissemination of SSI is limited by the SSI regulation, Protection of Sensitive

[10] See JUSTICE/FBI-019 Terrorist Screening Records System (TSRS) at http://www.fbi.gov/foia/privacy-act/72-fr-47073.
[11] 49 U.S.C. § 114(r), November 19, 2001.

Information.[12] SSI information may only be shared with covered persons with a need to know as defined by 49 C.F.R. part 1520.11.

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

Disclosures may be recorded manually within investigative files or 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 this privacy risk by sharing externally in accordance with published routine uses under the T-STAS SORN. Further, TSA has entered into an MOU with the FBI and TSC governing the conditions of sharing information related to STA programs.

Section 7.0 Redress

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

An individual may request access to his or her 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. A request may also be submitted by fax at 571-227-1406 or by email at FOIA.TSA@dhs.gov. Please refer to the TSA FOIA web site (http://www.tsa.gov/research/foia/index) for more information. 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 seek to correct information through a Privacy Act request as described in Section 7.1 of this PIA.

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 the STA result. 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 may not have the opportunity to correct, access, or amend inaccurate information maintained by TSA.

[12] 49 CFR Part 1520, May 18, 2004.

Mitigation: Individuals are provided with the opportunity to access, correct, or amend inaccurate information about them through the redress procedures described above. In addition, individuals may seek access to TSA records by submitting a request under the Privacy Act or under FOIA, though some aspects of their record may be exempt from access.

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?

This project involves collecting limited information from a very small population of individuals who have agreed to assist TSA with the design, implementation, or review of TSA security programs, techniques, or technology. It is expected that information will be collected manually and transmitted for the STA. TSA system administrators, security administrators, IT specialists, vetting operators, and analysts have access to the STA system in order to perform their duties in managing, upgrading, and using the system. Role-based system 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. 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.

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

All TSA employees are required to complete the annual DHS privacy training. In addition, security training is required, which raises the level of awareness and understanding for protecting PII.

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 to the Program Manager/System Owner, who grants access and designates a system administrator to provide access to approved individuals. Access to any part of the system is approved specifically for, and limited only to, users who have an official need to know the information for the performance of their duties associated with the STA process. 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?

TSA does not anticipate that information collected for this project will implicate such information sharing, uses, or access, but to the extent it does, they are controlled in accordance with Sections 8.1 (uses) and 8.3 (access), and will be reviewed for compliance with this PIA.

Responsible Officials

Inga Dawson
TSA-OLE
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security