Privacy Impact Assessment
for

Vetting of Security Personnel Receiving International TSA Training Assistance

DHS/TSA/PIA-044

May 07, 2014

Contact Point
Lori Silcox
Section Chief
Transportation Security Administration
Lori.Silcox@tsa.dhs.gov

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

Abstract

The Transportation Security Administration (TSA), Office of Global Strategies conducts security training for foreign partners (foreign governments, air carriers, and private companies responsible for transportation security) in order to mitigate threats originating overseas and to reduce the risk of insider threats among those receiving training from TSA. TSA conducts a Security Threat Assessment (STA) for individuals who reside outside the United States who have been nominated by the foreign partner for TSA-funded, sponsored, or administered security-related training. These foreign partners are responsible for security measures at foreign transportation facilities and employ individuals to carry-out those security measures.

TSA is conducting this Privacy Impact Assessment (PIA) pursuant to the E-Government Act of 2002 because it will collect, maintain, and disseminate information in identifiable form on the individuals nominated for training.

Overview

TSA trains individuals who are responsible for security measures at foreign airports. The training includes effective ways to ensure secure facility access, establish security controls, and conduct risk management assessments. Additionally, foreign partners attend training on effective passenger and cargo screening techniques. TSA training provides foreign partners with advanced skills and supports efforts to mitigate global risk in the international transportation sector.

Under the program, TSA will conduct an STA on individuals nominated by foreign partners for training in TSA-funded, sponsored, or administered security-related training programs. Foreign partners initiate the training request by providing biographical information about their employee candidates to TSA including full name, date of birth, gender, place of birth, nationality, passport number, and passport issuing country. This information will be collected by the TSA Representative (TSAR) at the U.S. Embassy whose area of responsibility covers the specific country in which the candidates reside. TSAR sends the information to the TSA Office of Intelligence and Analysis (OIA) by encrypted email to conduct an STA consisting of checks against federal terrorism and law enforcement databases. TSA may request additional information, such as names and dates of birth of the candidate's parents, if needed to resolve potential and confirmed matches to a federal terrorism or law enforcement watch list.

The TSAR is responsible for notifying the foreign partner that individuals will or will not be permitted to attend TSA-sponsored training. The names of all potential and confirmed matches to a federal terrorism or law enforcement watch list will be shared with the Department of State (DoS) Regional Security Officer (RSO) and the Federal Bureau of Investigation (FBI) Legal Attaché (Legat) at the local U.S. Embassy so that an additional investigation may be conducted to assess the security risk.

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?

The Aviation and Transportation Security Act (ATSA)[1] grants TSA the responsibility for security in all modes of transportation. It also grants the TSA Administrator authority to "receive, assess, and distribute intelligence information related to transportation security" as well as to "assess threats to transportation."[2]

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

The DHS/TSA-002 Transportation Security Threat Assessment System (T-STAS) SORN applies to the information collected for this program.[3]

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, 2013.

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

Yes, Transportation Threat Assessment and Credentialing (TTAC), N1-560-06-6, approved by NARA on March 8, 2007.

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.

This program does not fall within the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

The TSAR at a U.S. Embassy will collect information including: full name, date of birth, gender, place of birth, nationality, passport number, and passport issuing country for all candidates. TSA may request additional information (such as names and dates of birth of the candidate's parents) to clarify data or to resolve potential and confirmed matches to a federal terrorism or law enforcement watch list.

[1] Pub. L. 107-71, November 19, 2001, 115 Stat. 597.
[2] See 49 U.S.C. § 114(f).
[3] 75 FR 28046, May 19, 2010.

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

Foreign partners will provide information about their employees, who are training candidates, to the TSAR at a U.S. Embassy prior to participation in TSA-sponsored training activities. TSAR sends the information by encrypted email to the TSA Office of Intelligence and Analysis (OIA) where the STA will be completed. TSA will use federal terrorism and law enforcement watch lists to conduct the STA.

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 accuracy of the information provided to it by the foreign partner and by the federal agencies whose databases are checked for the security threat assessment. Foreign partners certify that the data is true and accurate. Approved training candidates will show photo identification to enter the training facility but TSA does not collect the photograph.

2.5 Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that a candidate may be incorrectly identified as a potential or confirmed match to a federal terrorism or law enforcement watch list.

Mitigation: TSA reduces this risk by requesting data elements that should be sufficient to distinguish each candidate from those on the federal terrorism or law enforcement watch list. TSA further reduces the risk of misidentification by requesting that the foreign partner certify the accuracy of the information provided to TSA. TSA provides contact information to the foreign partner in case the information must be corrected after it has been submitted to TSA.

Privacy Risk: There may be a risk that TSA maintains erroneous information about candidates.

Mitigation: The risk is reduced by providing potential and confirmed federal terrorism or law enforcement watch list matches to the local U.S. Embassy RSO and Legat for local investigation. In cases of possible misidentification or inaccurate records, the RSO or Legat will inform the TSA Representative, who will work with the program to correct the erroneous information. Individuals are vetted prior to each TSA training event, thus mitigating the risk of erroneous information being maintained.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

TSA uses the information to conduct STAs on foreign partner candidates nominated for security training. The STA is conducted in order to reduce the potential that TSA will provide security training to an insider threat within the foreign partner's workforce. The STA consists of a check against federal terrorism and law enforcement 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 system?

No. The system does not use technologies to locate a predictive pattern or an anomaly.

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 personally identifiable information (PII) may be used inappropriately.

Mitigation: PII collected by TSA will be used 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 TSA program managers were involved in the drafting of this PIA. A local investigation by the RSO and Legat assists in reducing the risk that an individual is inappropriately denied training.

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.

TSA does not provide a candidate direct notice prior to the collection of information. TSA requests the information from the foreign partner because the foreign partner has requested that its employee attend the training as part of his or her official duties. TSA provides notice through the issuance of this PIA, and the T-STAS SORN.

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

None, except to the extent the foreign partner permits its employee to opt-out.

4.3 Privacy Impact Analysis: Related to Notice.

Privacy Risk: There is a risk that a training candidate may not know how his or her information is used.

Mitigation: Candidates are nominated by the foreign partner to attend training as part of their employment or official duties. TSA informs the foreign partner of the use of the employee information. It is not known whether the foreign partner will notify the individual, nor does TSA control the foreign partner's employment relationship.

Section 5.0 Data Retention by the project

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

The program operates within the NARA-approved schedule TTAC, N1-560-06-6 (March 8, 2007). The length of time TSA will retain information on a candidate is based on each candidate's vetting result as described below:

- Information pertaining to a candidate who is not a potential match to a federal terrorism or law enforcement watch list will be retained for one year after TSA is notified or has knowledge that any credential, access, or privilege granted based upon an STA is no longer valid;
- Information pertaining to a candidate who may originally have appeared to be a match to a federal terrorism or law enforcement 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 an STA is no longer valid, whichever is longer;
- Information pertaining to a candidate who is determined to be a positive match to a federal terrorism or law enforcement watch list will be retained for 99 years after completion of matching activity,[4] or seven years after TSA learns that the candidate is deceased, whichever is earlier.

Candidates are recurrently vetted during the retention period.

The TSAR will maintain the list of approved training candidates until training is completed, at which time the list will be destroyed.

5.2 Privacy Impact Analysis: Related to Retention

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

Mitigation: TSA reduces the risk by maintaining information in accordance with NARA-approved record retention schedule. Information on individuals who are not a match to a watch list may be

[4] See JUSTICE/FBI-019 Terrorist Screening Records System (TSRS) at http://www.fbi.gov/foia/privacy-act/72-fr-47073.

deleted as soon as a year after the STA. TSA's data collection and retention practices relating to security threats are aligned with its purpose and mission, and are implemented accordingly.

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.

This information is only shared outside of DHS in the case of potential or confirmed matches to a federal terrorism or law enforcement watch list. If there is a potential or confirmed match, the information will be shared with the RSO and Legat at the local U.S. Embassy to carry out an additional investigation to identify and assess security risks.

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

DHS/TSA-002, T-STAS System of Records, Routine Use I permits disclosure "to the appropriate Federal, State, local, tribal, territorial, foreign, or international agency regarding candidates who pose, or are suspected of posing, a risk to transportation or national security." This routine use is compatible with the program's collection of information to conduct STAs, communicate vetting results, and coordinate an operational response if an individual is a potential or confirmed to be a match to a watch list.

6.3 Does the project place limitations on re-dissemination?

No, TSA does not place limitations on re-dissemination of information except to the extent that match information is Sensitive Security Information (SSI) involving limitations on the disclosure of security information.[5] Re-dissemination of SSI is limited by the SSI regulation, Protection of Sensitive Information.[6]

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

Disclosures to the RSO and the Legat at the local U.S. Embassy will be reflected in the analysis on the individual maintained by OIA.

6.5 Privacy Impact Analysis: Related to Information Sharing.

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

Mitigation: The risk is reduced by sharing this information in accordance with the Privacy Act for purposes of identifying known security risks prior to providing security training. In the ordinary

[5] 49 U.S.C. § 114(r), November 19, 2001.
[6] 49 CFR Part 1520, May 18, 2004.

course, sharing is expected to be limited to the RSO and Legat and with the foreign partner who provided the individual's information to TSA.

Section 7.0 Redress

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

In addition to the information provided to the foreign partner, the TSA website provides information on how to submit a Privacy Act request and Freedom of Information Act request. The individual may request access to his or her data by contacting the TSA Headquarters Freedom of Information Act (FOIA) Office, at FOIA Officer, Transportation Security Administration, TSA-20, Arlington, VA 20598-6020 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?

Inaccurate or erroneous information provided to TSA by the foreign partner must be corrected by the foreign partner.

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

The program does not directly notify training candidates about procedures for correcting their information. The program works directly through each foreign partner because it is the entity requesting that an employee receive TSA sponsored training.

7.4 Privacy Impact Analysis: Related to Redress.

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

Mitigation: In addition to the information provided to the foreign partner, the TSA website provides information on how to submit a Privacy Act request, though some aspects of the records may be exempt from disclosure. Moreover, if the individual is identified as a potential or confirmed match to a federal watch list, the TSAR contacts the foreign partner to obtain additional information, and an additional investigation will be conducted by the RSO and Legat.

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?

TSA performs an annual review with the program manager to ensure that information is used in accordance with this PIA. In addition, this PIA was conducted in consultation with program managers to ensure it reflects program information use.

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

All DHS/TSA users and assigned contractors receive DHS privacy training on appropriate handling and disclosure of PII. TSA monitors compliance with DHS's annual privacy training requirements for the proper handling of information.

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

A TSA Operations Directive (OD) is in place, which outlines the vetting process, roles and responsibilities, and specifically identifies who may access the candidate's information and for what purposes.

Only the Technical Solutions Division (TSD) and the Transportation Security Vetting Branch (TSVB) of OIA will have electronic access to the vetting database. Access to any part of that database vetting 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 communications 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 the 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 are controlled in accordance with Sections 8.2 and 8.3 above, and are reviewed by the program manager, appropriate program leadership, component Privacy Officer, and counsel and sent to DHS for formal review as needed.

Responsible Officials

Lori Silcox
Transportation Security Administration
International Aviation Development
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