Privacy Impact Assessment

for the

Transportation Security Administration (TSA) Office of Intelligence and Analysis (OIA) Technology Infrastructure Modernization (TIM) Program

DHS/TSA/PIA-042

March 26, 2014

Contact Point

Royce West

TSA-OIA

Royce.West@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 Intelligence and Analysis (OIA) Technology Infrastructure Modernization (TIM) Program is an enterprise architecture designed to align TSA security threat assessment (STA) with credentialing activities for individuals. These individuals require access to transportation facilities, infrastructure, assets, Sensitive Security Information (SSI), or related security credentials or clearances. TIM integrates several vetting programs and systems and facilitates STA adjudication, credentialing, and redress processes. TIM accesses the same personally identifiable information (PII) that is already collected for the underlying STA programs.[1] TIM performs credentialing activities utilizing the PII that the underlying programs collect for the STAs. In light of this new information technology framework involving existing PII, TSA is conducting this Privacy Impact Assessment (PIA) pursuant to the privacy provisions of the E-Government Act of 2002.

Overview

TSA performs STAs and credentialing activities on a variety of individuals within the transportation sector pursuant to its authorities under the Aviation and Transportation Security Act.[2] STAs include checks against law enforcement, immigration, and intelligence databases, and may include a fingerprint-based criminal history records check (CHRC).[3] TSA enrolls fingerprints with the Federal Bureau of Investigation (FBI) for recurrent CHRCs. The FBI also checks fingerprints against its unsolved crimes database, but the results are not returned to TSA. TSA will also enroll fingerprints with the National Protection and Programs Directorate/Office of Biometric Identity Management's (NPPD/OBIM) Automated Biometric Identification System (IDENT)[4] biometric database. For certain programs, TSA may perform additional checks of commercial or public databases, such as checks of Dun & Bradstreet for indirect air carriers (IAC). More information on the STA to be performed for each program can be found in the PIA for the program.

TIM will consolidate multiple program-specific activities into a common secure vetting and credentialing architecture. TIM facilitates this automated interface by receiving data from various vetting infrastructures[5] associated with the individual programs that require STAs and/or credential processing. TIM provides a "person-centric" vetting model that allows TSA to query a

[1] PIAs associated with TSA vetting operations may be found at https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[2] 49 U.S.C. § 114.
[3] TSA conducts CHRCs pursuant to 49 C.F.R. Part 1542.209 to determine whether individuals seeking unescorted access to secure areas of certain transportation facilities have disqualifying offenses. Note: Not all vetting programs have the same disqualifying offenses. Additionally, certain programs do not require a CHRC. An example of disqualifying offenses may be found at 49 C.F.R. Part 1572.103.
[4] See the Privacy Impact Assessment for Automated Biometric Identification system (IDENT), DHS/NPPD/PIA-002 at http://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system-ident.
[5] These include, but are not limited to the following systems that serve as an architectural conduit to TIM: TSA Consolidated Screening Gateway (CSG), Transportation Vetting System (TVS), and the Universal Enrollment Service (UES) System.

consolidated system to view information related to a specific individual. For example, TSA may access a transportation worker's biographical and biometric information (when applicable), the type of STA completed, and the mode(s) of transportation and/or program(s) in which he or she works. By linking the STA to the person rather than to the program for which it was conducted, the STA becomes portable across programs and transportation modes.

Portability not only assists TSA in identifying potential security threats, but also assists the individual applicant by more seamlessly permitting confirmation of data supplied for multiple TSA programs. For example, the disposition of a criminal charge supplied in the application for one program would be available for review in the STA for a subsequent credential. It also assists when an applicant may have failed to supply required information, such as an alien registration number or contact information. TIM allows the individual to review the status of his or her STA, and make corrections or clarifications when necessary.

TIM is comprised of hardware platforms and software systems that are used to host applications that support certain STA/credentialing initiatives; see the Appendix for a list of these initiatives. TSA will leverage TIM to accommodate new STA/credentialing initiatives, and will update the Appendix as additional requirements and/or populations arise.

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]

Based on the specific STA/credentialing initiative, additional authorities are set forth in various transportation, aviation, domestic security regulations;[8] the Maritime Transportation Security Act of 2002 (MTSA);[9] and the Interim Final Rule for Security Threat assessment for Individuals Applying for a Hazardous Materials Endorsement (HME) for a Commercial License.[10]

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).[11]

---

[6] 49 U.S.C. § 114(d).
[7] 49 U.S.C. § 114(f).
[8] 6 U.S.C. § 469; 46 U.S.C. § 70105; 49 U.S.C. §§ 1542, 1544, 5103a, 44936, and 44939.
[9] Pub. L. 107-295, November 25, 2002.
[10] 69 FR 68720, November 24, 2004.
[11] 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.

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) 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.

See Appendix.

Section 2.0 Characterization of the Information

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

TIM manages information collected in existing STA vetting programs as described in each program's respective PIA. TIM processes individual information against relevant databases and resolves potential matches. Checks are performed on a recurring basis to ensure that updates to the relevant databases are captured daily or upon receipt of new information. For more detailed information on the PII collected and maintained by each program, please see the applicable PIA.

TIM maintains the results of the STA, which includes derogatory information, and information provided by individuals during the resolution of any Preliminary Determination of Ineligibility (PDI), Preliminary Determination of Ineligibility with Immediate Suspension (PDIIS), or Final Determination of Ineligibility (FDI). TSA will issue the PDI to the individual in order to permit the individual to challenge the preliminary result or, as is often the case, provide missing information. The PDIIS will be issued if the preliminary results of the STA are sufficiently derogatory to warrant immediate suspension of the individual's credential or access to a facility. The FDI will be issued if the time limitations for the redress process pass without action by the individual or once redress measures have been completed. TIM may collect and maintain the following information collected pursuant to the cited STA programs and/or any new programs or populations:

- Full legal name; any applicable suffix; and any other names used previously;
- Social Security Number (SSN) – Providing the SSN is voluntary, however, failure to provide it may delay or prevent completion of the STA;
- Fingerprints used to obtain a CHRC and for enrollment in IDENT for immigration

checks;

- Photograph (if applicable);
- Day time phone number; and e-mail address if available;
- Date of birth;
- Gender;
- Height, weight, hair color, and eye color;
- City, state, and country of birth, and country of citizenship;
- Date, place, and type of flight training or other instruction;
- Current and previous mailing address; current residential address if it differs from the current mailing address;
- Information necessary to assist in tracking submissions and payments;
- Federal Aviation Administration (FAA) operating certificate number of the applicant, if applicable;
- Results of any analysis performed for STAs and adjudications;
- Information provided by the individual to assist in resolving any adjudication issue;
- Immigration status and if applicable, the date of naturalization, the type of visa, the visa number, and the date on which it expires. Each individual must present documentary evidence specified by TSA that he or she is lawfully present in the United States, including proof of U.S. citizenship, if claiming U.S. citizenship;
- If applicable, the alien registration number and/or the number assigned to the individual on the U.S. Customs and Border Protection Arrival-Departure Record,[12] Form I–94, if issued;
- If the individual is a commercial driver licensed in Canada and does not hold a Free and Secure Trade (FAST) for Commercial Vehicles, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), or NEXUS card,[13] his or her Canadian passport number;

[12] See DHS/NPPD/PIA-005 Arrival and Departure Information System (ADIS) PIA at http://www.dhs.gov/privacy.

[13] Information about the U.S. Customs and Border Protection (CBP) trusted traveler programs may be found at http://www.cbp.gov/travel/trusted-traveler-programs, or see DHS/CBP/PIA-002 Global Enrollment System (GES) PIA, January 10, 2013, at http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_cbp_ges_jan2013.pdf.

- Current employer(s), employer address, phone number, and fax. If the individual's current employer is a U.S. military service, include the branch of the service. In the case of an individual who is self-employed or employed by several operators, the individual must provide the name, address, telephone number, and fax number of the primary transportation facility where the individual requires or may require unescorted access, if known;

- The individual's level of access at an airport or other transportation facility, including access termination and/or expiration dates;

- If available, passport number, city of issuance, date of issuance, and date of expiration;

- If applicable, Department of State (DoS) Consular Report of Birth Abroad;

- If applicable, whether the individual has previously completed a TSA STA, and if so the date and program for which it was completed;

- Previously issued government license, credential, or certificate number; and

- If applicable, whether the individual currently holds a federal security clearance, and if so, the type of clearance, date of and agency for which the clearance was performed.

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

TSA collects biographical and biometric information directly from individuals seeking an STA and/or a credential, or from facilities regulated by DHS, enrollment centers, or designated service providers authorized to provide the information on behalf of the individual. Because the populations are so numerous and dispersed, TSA provides several means for information collection. All of the collection means require the applicant to take or authorize action to submit information to TSA. Enrollment information may be provided to TIM through enrollment providers, directly input by the individual at an enrollment center, or directly transmitted by entities authorized by the individual to submit information. Information used by TIM during the STA (for example, watch lists or criminal history records) is supplied by law enforcement, immigration, and intelligence agencies.

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

Yes. TSA uses Dun & Bradstreet to verify the existence and legitimacy of an Indirect Air Carrier (IAC) as a business entity. Commercial databases, such as Lexis-Nexis or CLEAR, and public records may be used to perform identity verification functions or resolve criminal

history or immigration issues (e.g., to obtain a final disposition of charges).

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 or during the process for resolving PDI or PDIIS. If an individual believes that he or she received a PDI or PDIIS based on incorrect information submitted to or obtained by TSA, that individual can seek redress as detailed in the letter notifying the individual and in Section 7.2.

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 mitigates this risk by requiring data elements that should be sufficient to distinguish an applicant from individuals whose information is included in a derogatory data set or who are identified as a match to information contained in intelligence databases. TSA will further mitigate the risk of misidentification by requiring the applicant to certify the accuracy, to the best of his or her knowledge, of the PII submitted to TSA. TSA further mitigates this risk by providing the individual redress through the PDI or PDIIS process as described above.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The PII TSA has collected for its STA programs are used to vet individuals undergoing an STA for transportation security purposes. Typically this covers individuals who require access to transportation facilities, infrastructure, assets, SSI, or related benefits or credentials. TSA expects to conduct recurrent checks against law enforcement, immigration, and intelligence databases.

TIM provides a person-centric view of applicants, and thus TSA may be able to identify potential security risks that would otherwise not be readily apparent. For example, TIM will identify individuals that may attempt to conceal their true identity behind multiple names or aliases. It will also identify whether an individual has applied for multiple credentials. Rejection for one credential is not, by itself, grounds for rejection for another credential. TIM provides the capability for TSA to identify links among applicants, such as whether multiple unrelated applicants share a common or false address.

TIM will also improve the STA process through enhanced monitoring of an application's status by generating statistical information, and identifying whether an applicant is entitled to a reduced fee for a credential. It is not uncommon for an applicant to have omitted immigration information, a contact address, phone number, or email address. For an applicant that has submitted PII for multiple programs, TIM provides the capability to supply and/or correct missing information from a previous data submission. From a customer service standpoint, TIM

centralizes all support transactions and will provide the applicant with the opportunity to review the status of his or her 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, TIM does not use technology that predicts patterns. It does, however, provide a capability to identify links across its populations, and thus identify anomalies such as multiple identities or links among applicants.

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

TSA shares information within DHS in order to conduct STAs. This sharing includes U.S. Citizenship and Immigration Services for immigration checks, and with the OBIM IDENT system for recurrent immigration and law enforcement checks. DHS NPPD may submit STAs on individuals participating in the Chemical Facility Anti-Terrorism Standards (CFATS) Program.[14]

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. Additionally, there is a risk that anomalies discovered during the STA process may result in an inappropriate decision that impacts the individual.

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. TSA mitigates the risk that anomalies may result in an inappropriate decision by providing a secondary review of the anomaly using available data sets to ensure the accuracy of information obtained during the vetting process.

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.

The individual receives a Privacy Act Statement regarding the information obtained for STAs and credentialing activities at the point of collection. The Privacy Act Statement describes the authority for the collection of the information, the purpose for the collection of information, whether provision of the information is voluntary, and any consequences of failing to provide the requested information.

[14] http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-nppd-cfats.pdf

In addition, TSA provides notice by issuing 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?

Individuals may opt-out of undergoing a STA and/or submitting certain required data for a credential application, but if they choose to do so, they will not have access to transportation facilities, assets, or information. Individuals may elect not to provide voluntary information; however, doing so may delay the processing of their STA or credential application or prevent completion.

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: The risk is mitigated by information provided by TSA at the time of application through the Privacy Act Statement, as well as this PIA and the DHS/TSA-002 T-STAS SORN.

Section 5.0 Data Retention by the Project

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

TIM 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 an 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 an 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,[15] or seven years after TSA learns that the individual is deceased, whichever is earlier.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the TSA will retain more data than is necessary or will retain data for periods of time longer than those approved.

Mitigation: TSA mitigates excess data retention by limiting the data collection to the amount required to conduct STAs and/or credential activities with a high level of confidence. TSA

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

maintains information in accordance with NARA-approved record retention schedules and all employees are required to take records management training. 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

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 governments, 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.

TSA will share information with the FBI and the Terrorist Screening Center (TSC) as part of normal operations to conduct STAs. TSA will disclose the STA results to the individual applicants associated with the PDI, PDISS, and the FDI. In instances when TSA issues a PDIIS or a FDI, TSA will disclose the outcome with facility operators, owners, and employers. TSA will share STA results with the state in which an individual is authorized to hold an HME.

TSA may also disseminate information to other third parties involved in the STA process that have a need to know the information in the performance of official duties, including contractors operating enrollment centers, designated service providers performing vetting operations on TSA's behalf, and manufacturers of credentials. TSA and DoS will share information while processing STAs and/or credential applications when consulates are used by individuals located overseas. TSA will share information on persons who pose, or are suspected of posing, a risk to national or transportation security with law enforcement, immigration, or intelligence agencies. TSA also shares information with FAA for FAA Airman Certificate STAs. Finally, TSA may share information outside of DHS in accordance with the routine uses set forth in the DHS/TSA-002 T-STAS SORN.

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 an STA on regulated populations. Sharing of results with facility operators and others including law enforcement is compatible with that purpose.

DHS/TSA-002, T-STAS System of Records, Routine Use H permits DHS to share information with the Department of Transportation, its operating administrations, or the appropriate state or local agency when relevant or necessary to ensure safety and security in any mode of transportation; enforce safety and security related regulations and requirements; assess and distribute intelligence or law enforcement information related to transportation security; assess and respond to threats to transportation; oversee the implementation and ensure the adequacy of security measures at airports and other transportation facilities; plan and coordinate any actions or

activities that may affect transportation safety and security or the operations of transportation operators; or the issuance, maintenance, or renewal of a license, endorsement, certificate, contract, grant, or other benefits.

Routine Use I permits DHS to share information with an appropriate federal, state, local, tribal, territorial, foreign, or international agency regarding individuals who pose, or are suspected of posing, a risk to transportation or national security.

Routine Use J permits DHS to share information with a federal, state, local, tribal, territorial, foreign, or international agency, where such agency has requested information relevant or necessary for the hiring or retention of an individual; or the issuance of a security clearance, license, endorsement, contract, grant, waiver, credential, or other benefits.

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.

Routine Use M permits DHS to share information with third parties during the course of an STA, employment investigation, or adjudication of a waiver or appeal request, to the extent necessary to obtain information pertinent to the assessment, investigation, or adjudication.

Routine Use N permits DHS to share information with airport operators, aircraft operators, maritime and surface transportation operators, IACs and other facility operators about individuals who are their employees, job applicants or contractors, or persons to whom they issue identification credentials or grant clearances to secured areas in transportation facilities when relevant to such employment, application, contract, training or the issuance of such credentials or clearances.

6.3 Does the project place limitations on re-dissemination?

Information shared with state and local agencies, and with employers, operators, and owners of transportation facilities or assets is typically limited to the result of the STA, which must be disseminated for operational purposes, including issuance of a credential (such as the HME issued by the State licensing authority) and permitting access to facilities or assets.

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.[16] Re-dissemination of SSI is limited by the SSI regulation, Protection of Sensitive Information [17]

[16] 49 U.S.C. § 114(r), November 19, 2001.
[17] 49 CFR Part 1520, May 18, 2004.

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. In addition, TIM maintains an electronic log of all data sharing transactions.

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 only 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).

Additionally, if an individual seeks to appeal his or her STA, he or she may request the records upon which TSA's determination was based. Instructions detailing how to request the records are included in the individual's eligibility determination notification. Also pursuant to exemptions under 5 U.S.C. § 552a(k)(1) and (k)(2), classified or otherwise restricted materials may not be provided to the individual.

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

Procedures to correct inaccurate or erroneous information vary by program. Please review the applicable program PIA for more information. In addition, 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 provides information on the procedures for correcting information with eligibility determination on the TSA website, through this PIA. 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 commercial data brokers and submitted to TSA.

Mitigation: TSA does not make decisions regarding an individual based solely on commercial data. 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?

TSA system administrators, security administrators, IT specialists, vetting operators, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Role-based 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. TSA also employs processes to enforce separation of duties, to prevent unauthorized disclosure, or to prevent modification of information. 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. Finally, TIM's 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 privacy courses. In addition, security training is provided, which helps to raise the level of awareness and requirements for protecting PII. All IT security training is reported as required in the Federal Information Security Management Act of 2002.[18]

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 TIM 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

[18] Pub. L. 107-347.

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?

New information sharing, uses, or access will be controlled in accordance with Sections 8.2 and 8.3, and will be reviewed for compliance with this PIA.

Responsible Officials

Royce West
TSA-OIA
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

Appendix: TSA Programs that Require Security Threat Assessments (STAs)

- Alien Flight Student Program (AFSP) OMB 1652-0021
- Aviation Worker (AW) OMB 1652-0002
- Certified Cargo Screening Program (CCSP) OMB 1652-0053
- Chemical Facility Anti-Terrorism Standards (CFATS) OMB 1670 0015
- General Aviation (GA) OMB 1652-0035
- GA OMB 1652-0054
- Hazardous Materials Endorsement (HTAP) OMB 1652-0027
- Indirect Air Cargo (IAC) OMB 1652-0040
- Transportation Workers Identification Credential (TWIC) OMB 1652-0047
- TSA Pre√ Application Program OMB 1652-0059