Privacy Impact Assessment
for
Threat Assessments for Access to Sensitive Security Information for Use in Litigation

December 28, 2006

Contact Point

Andrew Colsky
Sensitive Security Information (SSI) Office
Transportation Security Administration
SSI@dhs.gov

Reviewing Officials

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@dhs.gov

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
Privacy@DHS.gov

Overview

Transportation Security Administration (TSA) is implementing a process whereby a party seeking access to Sensitive Security Information (SSI) in a civil proceeding in a Federal court that demonstrates substantial need for relevant SSI in preparation of the party's case may request access to SSI. In order to determine if an individual representing the party may be granted access to SSI for this purpose, TSA will conduct a threat assessment that includes a fingerprint-based criminal history records check (CHRC) and a name-based check.

Introduction

Certain information has been identified in 49 C.F.R. Section 1520 defines certain information 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. Section 525(d) of the Department of Homeland Security Appropriations Act of 2007, P.L. 109-295, provides that in civil proceedings in the United States District Courts, where a party seeking access to SSI demonstrates both a substantial need for relevant SSI in the preparation of the party's case and an undue hardship to obtain equivalent information by other means, the party or party's counsel shall be designated as a covered person under 49 CFR Section 1520.7, provided that a) the overseeing judge enters an order protecting the SSI from unauthorized disclosure; b) the individual undergoes a threat assessment that includes a criminal history records check; and c) the provision of access to the specific SSI in question does not present a risk of harm to the nation. Additionally, court reporters that are required to record or transcribe testimony containing specific SSI and do not have a current clearance required for access to classified national security information as defined in Executive Order 12958 will need to undergo a threat assessment before access to SSI may be granted. The Aviation and Transportation Security Act (ATSA), P.L. 107-71, Section 114(f), authorizes TSA to perform security threat assessments.

To accomplish these threat assessments, TSA will require individuals seeking access to SSI for use in Federal civil court proceedings to provide their full name, date of birth, place of birth, citizenship information (including, if applicable, immigration status, alien registration number, passport number and country of issuance), home address, gender, employer name and address (if applicable), bar membership information (if applicable), Social Security Number (voluntary but recommended), and publicly available information about sanctions, if any, issued by a court or other judicial body against the party, the individual representing the party, or any of the individual's clients, while represented by the individual. Court reporters will be asked to provide additional information relating to their professional qualifications such as whether they are listed on the registry of the National Court Reporters Association Registry, if they currently hold a security clearance with the Federal government, have been denied a security clearance in the past, or have ever been disciplined for mishandling information. All of the above individuals will also be required to submit fingerprints on the FD 258 fingerprint card, which additionally collects race, height, weight, hair and eye color, required to conduct a Criminal History Records Check (CHRC). Individuals will be required to provide payment prior to the

processing of these threat assessments. Payments will be collected in a manner and form approved by TSA. TSA expects the collection of this personally identifiable information will be sufficient to conduct these threat assessments and reduce to the greatest extent possible the number of individuals falsely identified as positive matches to terrorist watch lists or law enforcement lists. Because this program entails a new collection of information about members of the public in an identifiable form, the E-Government Act of 2002 and the Homeland Security Act of 2002 requires that TSA conduct a Privacy Impact Assessment (PIA).

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

TSA will collect the full name (including any aliases), date of birth, place of birth, citizenship information (including, if applicable, immigration status, alien registration number, passport number and country of issuance), home address, gender, employer name and address (if applicable), bar membership information (if applicable), and Social Security Number (voluntary, but recommended) of individuals seeking access to SSI for use in Federal civil court proceedings. TSA will also collect publicly available information concerning citations or sanctions, if any, issued by a court or other judicial body against the party, the individual representing the party, or any of the individual's clients, while represented by the individual. It is possible that providing the required information will entail providing the names of the individual's clients who have been sanctioned in the past. Depending on the information provided, TSA may contact the sanctioning body for more publicly available information regarding any sanction or citation. Court reporters will be asked to provide additional information relating to their professional qualifications such as whether they are listed on the registry of the National Court Reporters Association Registry, if they currently hold a security clearance with the Federal government, have been denied a security clearance in the past, or have ever been disciplined for mishandling information.

The individuals seeking access to SSI will also be required to submit fingerprints on the FD 258 card, which additionally collects race, height, weight, hair and eye color. These individuals will be required to provide payment to cover the costs of these threat assessments prior to processing; payment will be collected in a manner and form approved by TSA.

TSA also collects certain information as a result of the checks performed against terrorist threat, criminal history, and immigration databases. If the individual has a criminal record, a copy of that record will be collected. For other databases, the result of the check will be collected. As discussed below in section 7, other information may be collected in connection with the redress, appeal, or waiver process.

1.2 From whom is information collected?

TSA will collect the information from individuals, including experts retained by either party, seeking access to SSI for use in Federal civil court proceedings. Access may only be granted to a limited number of persons per litigation, as designated by TSA. Information may also be collected from court reporters that will be required to record or transcribe testimony containing specific SSI and do not have a current clearance required for access to national security information as defined in Executive Order 12958.

1.3 Why is the information being collected?

The purpose of collecting this information is to perform a threat assessment to ensure that granting a specific individual access to particular SSI for use in a civil proceeding in a Federal court does not pose a risk of harm to the nation. The threat assessment includes (1) a fingerprint-based CHRC; (2) a name-based check to determine whether the individual poses or is suspected of posing a threat to transportation or national security, including checks against terrorism, immigration or other databases TSA maintains or uses; and (3) a professional responsibility check (if applicable).

1.4 How is the information collected?

Individuals seeking access to SSI in civil proceedings in Federal civil court proceedings will be required to submit a questionnaire and certification with personally identifiable information and fingerprints at a physical location designated by TSA, such as a government office or a TSA contractor location. The information will be sent to a TSA contractor, who will format the fingerprints and biometric data in order to send it to TSA for a threat assessment.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

Under ATSA §114(f), TSA has broad authority to carry out transportation security responsibilities, including assessing threats to transportation security. It also authorizes TSA to develop policies, strategies, and plans for dealing with threats to transportation security. Section 525(d) of the Department of Homeland Security Appropriations Act of 2007 states that in civil proceedings in the U. S. District Courts individuals who can demonstrate a substantial need of relevant SSI in preparation of the party's case may be granted limited access to SSI, upon successful completion of a criminal history check and a threat assessment.

1.6 Privacy Impact Analysis

The incorrect identification of an individual as a security threat (false positives) is one of the privacy risks associated with this collection. TSA seeks to reduce the potential for misidentification by requesting sufficient items of information in order to distinguish the individual from others that may have the same name. TSA's privacy challenge is to mitigate the risk of

false positives while ensuring that access to SSI is not granted to individuals where such access would present a risk of harm to the nation. It is critical that false positives be kept to a minimum, since they could result in the delay or denial of access to SSI that may affect a civil proceeding in Federal court.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

TSA will use the information to conduct threat assessments which will include (1) a fingerprint-based CHRC; (2) a name-based check to determine whether the individual poses or is suspected of posing a threat to transportation or national security, including checks against terrorism, immigration or other databases TSA maintains or uses; and (3) a professional responsibility check (if applicable) for the purpose of identifying those situations in which providing SSI access to a particular individual would present a risk of harm to the nation. The results of the threat assessment will be used by TSA to make a final determination on whether the individual may be granted access to SSI.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The information will be obtained directly from the individual. TSA expects that individuals will submit accurate information and will require a sworn certification attesting to the accuracy of the information.

2.4 Privacy Impact Analysis

The risk of collecting inaccurate information is minimal because the individual seeking access to SSI has a strong interest in submitting accurate information. The impact of collecting inaccurate information is mitigated because individuals who feel they have been wrongly identified as a security threat can seek redress through TSA. TSA's redress process allows for an additional review of the completeness and accuracy of the information.

Section 3.0
Retention

3.1 What is the retention period for the data in the system?

TSA will retain the data it receives in accordance with a record schedule which was submitted for approval by the National Archives and Records Administration (NARA). TSA is seeking approval to retain records of individuals granted access for one year after the access privilege is no longer valid. TSA expects to retain records on individuals who are initially identified as potential matches to a government watch list but are ultimately cleared and granted the access privilege for seven years after the threat assessment is completed or one year after the access privilege is no longer valid, whichever is longer. TSA determined that seven years is an appropriate proposed retention period for these records due to the six year statute of limitations prescribed in 28 U.S.C. § 2401, which applies to civil litigation commenced against the United States. The seven year retention period ensures that all relevant documents will be available in the event of civil litigation concerning the threat assessment process. TSA is also seeking to retain records for individuals who are denied access based on the threat assessment for 99 years after completion of the threat assessment or seven years after TSA learns that an individual is deceased, whichever is shorter.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

No. TSA has submitted the retention schedule to NARA and is awaiting approval.

3.3 Privacy Impact Analysis

Information collected through this program will be maintained in accordance with schedules to be approved by NARA in furtherance of TSA's mission to ensure the security of the Nation's transportation system. The retention period is designed to permit records to be retained while the individual is acting under a grant of access based on a TSA threat assessment.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

The information TSA receives may be shared with DHS components that have a need to know the information in order to carry out their official duties, including but not limited to law enforcement and intelligence operations. It is expected that information will typically be shared with TSA employees or contractors in the following TSA offices: the Office of Chief Counsel, the Office of Transportation Threat Assessment and Credentialing, the SSI Office, the Office of Personnel Security, and the Office of Intelligence or Office of Security Operations in the event of a positive match. Information might also be shared with the TSA Office of Civil Rights and Civil Liberties, TSA Privacy Office, TSA Ombudsman, and TSA Legislative Affairs to respond to complaints from individuals. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a. While it is not expected that information will be routinely shared outside of TSA, TSA may need to share information within DHS as outlined in section 4.2.

4.2 For each organization, what information is shared and for what purpose?

TSA will share the information with the Office of Transportation Threat Assessment and Credentialing and the Office of Personnel Security in order to conduct the threat assessments. The information will be shared with the Office of Chief Counsel, Office of Transportation Threat Assessment and Credentialing, and the SSI Office to make determinations about whether the individual may be granted access to the SSI, and with the SSI Office in order to share SSI with approved individuals. Individuals' identifying information and positive results of comparisons to Federal terrorism and law enforcement databases will be shared with TSA's Office of Intelligence and Office of Security Operations. In order to respond to complaints from individuals, the information may also be shared with the Privacy Office, Ombudsman, Office of Civil Rights and Civil Liberties, and Legislative Affairs. The information may also be shared outside of TSA, within DHS, where there is a need to know the information for law enforcement, intelligence, or other official purposes. This information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. §552a.

4.3 How is the information transmitted or disclosed?

TSA will transmit this data within DHS electronically, via password-protected CDs, facsimile, in person, or telephonically to those who need the information to perform their official

duties. The method of transmission may vary according to specific circumstances and the urgency of the need for the information.

4.4 Privacy Impact Analysis

Information is shared within DHS with those individuals who have a need for the information to perform their official duties in accordance with the Privacy Act. Only TSA employees and contractors with proper access privileges are allowed access to this information to conduct threat assessments. Employees authorized to access the data receive appropriate privacy and security training and have necessary background investigations and security clearances for access to sensitive or classified information. Privacy protections include strict access controls, including security credentials, passwords, real-time auditing that tracks access to electronic information, and mandated training for all employees and contractors.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

TSA will share the information collected with the FBI, which will conduct the CHRC and return the results to TSA. The information collected will also be shared with the Terrorist Screening Center and other agencies in connection with the resolution of possible name matches and any operational response. TSA will also share the information with the Department of Justice attorney(s) handling the civil proceeding for which the SSI material has been requested and any related proceedings. Additionally, TSA will request that these individuals consent in writing to the disclosure of this information to the court overseeing the civil proceeding and other judicial bodies associated with the appeals process. Further, TSA may share the information it receives with Federal, State, local, or tribal law enforcement or intelligence agencies in accordance with the routine uses identified in the applicable Privacy Act system of records notice (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS). This SORN was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731- 67735.

5.2 What information is shared and for what purpose?

The information and fingerprints collected will be shared with the FBI in order to conduct the CHRC and send those results back to TSA. It is anticipated that results of the threat assessment, including the results of the CHRC, will be shared with the Department of Justice attorney(s) handling the civil proceeding in which the individual has requested access to SSI, and any related proceedings. TSA will also request that individuals consent in writing to permit TSA to disclose the results of the threat assessment, including the results of the CHRC, to the court overseeing the civil proceeding for which access to SSI has been requested and other

judicial bodies associated with the appeals process. It is expected that individually identifying data and the threat assessment status of individuals identified as security threats will also be shared in accordance with the SORN described in Section 5.1, as needed, with Federal, State, local, or tribal law enforcement or intelligence agencies to communicate security threat assessment results and to facilitate an operational response.

5.3 How is the information transmitted or disclosed?

Depending on the recipient and the urgency of the request or disclosure, the information may be disclosed in person, telephonically, electronically, by mail, facsimile, or a password-protected CD. The method of transmission may vary according to specific circumstances, and will be in conformance with OMB guidance for handling of personal information. The information may also be marked with specific handling requirements and restrictions to further limit distribution.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Yes. Sharing of information between TSA and the TSC is subject to an MOU. The MOU reflects the scope of the information shared and imposes restrictions on use of the information. TSA also has an agreement in place with the FBI to conduct a CHRC. The Privacy Act SORN described above also reflects the scope of the information that may be shared outside of TSA.

5.5 How is the shared information secured by the recipient?

Federal agencies are subject to the safeguarding requirements of the Privacy Act and the Federal Information Security Management Act (FISMA), Title III of the E-Government Act, Pub.L. 107-347.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

No specific training is required, however Federal agencies are subject to the Privacy Act and Federal employees and contractors typically receive Privacy Act training.

5.7 Privacy Impact Analysis

TSA will share this information under the applicable provisions of the SORN and the Privacy Act. By limiting the sharing of this information to individuals who have an official need to

know and by ensuring that recipients properly handle this data, TSA is mitigating any attendant privacy risks.

Section 6.0
Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Yes. TSA will provide a Privacy Act Statement to individuals seeking access to SSI for use in Federal civil court proceedings so that individuals may exercise informed consent before providing personal information for the CHRC and threat assessment. TSA will also present these individuals with a consent form to authorize TSA to disclose the results to additional parties, such as the court overseeing the civil proceeding. If the individual declines to provide the requested information, TSA may not be able to complete a threat assessment, without which the individual may not be granted access to the SSI. In addition, notice is provided through publication of this PIA and of the SORN for DHS/TSA 002, Transportation Security Threat Assessment System. This SORN was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731-67735. In the event that an individual is determined to be a security threat and the individual believes that the results of the screening are inaccurate, he or she will be informed by TSA on how to pursue redress from TSA.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. Individuals may decline to provide information. If the individual declines to provide the information, TSA may not be able to complete a threat assessment, without which the individual may not be granted access to the SSI. If additional information is needed during the redress process, that collection will also be voluntary.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No. However, all uses of such information by TSA will be consistent with the Privacy Act and the DHS/TSA 002, Transportation Security Threat Assessment System SORN identified in paragraph 5.1 above.

6.4 Privacy Impact Analysis

TSA has made the process for transmission of individual information to TSA transparent. TSA will provide a Privacy Act statement, which will explain the authority for the collection, the purpose of the collection, the voluntary nature of providing the information, and that failure to provide the information may not permit TSA to complete a threat assessment, without which the individual may not be granted access to the SSI. By providing this statement, individuals are given meaningful notice enabling them to exercise informed consent prior to disclosing any information to TSA.

Section 7.0
Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Individuals may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration, TSA-20, East Tower
FOIA Division
601 South 12th Street
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (URL: http://www.tsa.gov/public/contactus). The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (http://www.tsa.gov/public). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.

7.2 What are the procedures for correcting erroneous information?

If it is determined that covered individuals are not eligible to receive access to particular SSI based on the threat assessment, TSA will notify the individuals by mailing an Initial Determination of Threat Assessment (IDTA) containing the reason(s) for the issuance of the IDTA and directions as to how applicants may submit an appeal. The appeal must be submitted within thirty days after the date of service of the IDTA or thirty days from TSA's response to the individual's request for further information pertaining to the determination.

An individual may appeal an IDTA by: 1) serving TSA with a written answer that includes relevant agency or court documents to verify the individual's identity and correct errors in the individual's records; or 2) requesting a copy of the documents on which TSA based its Initial Determination. No documents that are classified or otherwise protected by law will be released. TSA will release as much information to the applicant as permitted by law to provide for a meaningful appeal. The appeal process consists of a review of the IDTA, the materials upon which the decision was based, the individual's appeal materials and any other relevant information or material available to TSA. When an Initial Determination is made that an individual poses a transportation security threat, and the individual appeals the decision, the Assistant Secretary or designee will review the case and make the Final Determination.

If the threat assessment does not reveal that providing the individual access to SSI would present a security threat, but TSA determines that granting the individual access to SSI otherwise presents a risk of harm to the nation because the requested SSI is too sensitive or not relevant to the litigation, TSA will issue a Final Determination that the individual may not be granted access to that SSI. TSA's Final Determination on the requester's access to SSI, whether it be based on the security threat assessment, other suitability information, or relevancy grounds, is reviewable by the judge presiding over the underlying litigation.

7.3 How are individuals notified of the procedures for correcting their information?

The Initial Determination of Threat Assessment letter sent to the individual will contain the procedures for submitting appeals.

7.4 If no redress is provided, are alternatives are available?

N/A. A redress process, as described in section 7.2 above, is provided for individuals who believe that they have been wrongfully identified as a threat.

7.5 Privacy Impact Analysis

In order to mitigate the risk that incorrect information may be associated with an individual, TSA has developed a robust redress process that provides notice to the individual of the determination and instructions on how to access and/or correct the information.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system?

The System Security Plan defines the environment within which a system will operate and the plan identifies user groups as system administrators, security administrators, system operators, and general users (intelligence analysts). These groups access the system in order to perform their duties in managing, upgrading, and utilizing the system resources.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes. Contractors who are hired to perform many of the IT maintenance and security monitoring tasks have access to the system in order to perform their official duties. Strict adherence to access control policies is enforced by the system in coordination with and through oversight. All contractors performing this work are subjected to requirements for suitability and a background investigation as required by TSA Management Directive 1400.3, TSA Information Security Policy.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Role-based access controls are used for controlling access to the system using the policy of Least Privilege, which states that the system will enforce the most restrictive set of rights/privileges or access needed by users based on their roles.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The system is secured against unauthorized access through the use of a layered, defense-in-depth security approach involving procedural and information security safeguards. The system security plan limits the system access for purposes of conducting these security threat assessments. All government and contract personnel who require access to perform their official duties have passed personnel, physical, and network verifications.

All government and contractor personnel are vetted and approved access to the facility where the system is housed, issued picture badges with integrated proximity devices imbedded, and given specific access to areas necessary to perform their job function. A Rules of Behavior document provides overall guidance on how employees are to protect their physical and technical environment and the data accessed to perform their official duties. All new employees are required to read and sign a copy of the TSA Rules of Behavior prior to getting access to any TSA IT system.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

All system roles and rules must comply with TSA Management Directive 1400.3, TSA Information Security Policy. Access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role. All roles and rules are reviewed, audited, scanned, and evaluated on a continuous basis to ensure that the system provides a level of protection required by the system security plan.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

The system maintains a real-time auditing function on individuals who access the system. Weekly logs are reviewed to ensure no unauthorized access has taken place. All TSA IT systems are audited annually for IT security policy compliance and technical vulnerability by the TSA IT Security Office.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All government and contractor personnel are required to complete on-line TSA Privacy Training. Compliance with this requirement is audited monthly by the TSA Privacy Officer. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting personal information being processed. All IT security training is reported annually as required by FISMA.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Information in TSA's record systems is safeguarded in accordance with FISMA, which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. All systems are operating on the authority of the Designated Accrediting Authority (DAA). The Transportation Vetting Operations system completed FISMA Certification and Accreditation on September 1, 2005.

8.9 Privacy Impact Analysis

Data on the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical

access to the system is strictly controlled with the use of proximity badges. The system is housed in a controlled computer center within a secure facility. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts. The protection of data contemplated under this assessment will be governed by the applicable System Security Plan for this system.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The system is built from Commercial Off the Shelf (COTS) products and customized applications or Government Off the Shelf (GOTS) products. System components include COTS hardware and operating systems with GOTS applications.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Security and privacy requirements were analyzed based on Federal Information Processing Standards (FIPS) methodology. FIPS methodology categorizes a system as High, Medium, or Low, depending on how important the function is to the agency. The system completed a FIPS-199, Standards for Security Categorization of Federal Information and Information Systems analysis on October 5, 2005, in order to categorize the system. All security controls are applied in accordance with the results from the FIPS-100 analysis.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, TSA has limited its data collection to specific elements necessary for security vetting. TSA has developed an information technology infrastructure that will protect against inadvertent use of personally identifying information not required by the government. Access to data collected for this program will be strictly controlled; only TSA employees and contractors with proper access controls will have permission to use and view this information. Additionally, the record system will include a real time audit function to track access to electronic information, and any infractions of information security rules will be dealt with appropriately. All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses.

9.4 Privacy Impact Analysis

The system was developed using COTS and GOTS products with the appropriate information security controls. An in-depth FIPS methodology analysis was completed to ensure that privacy protections were built into the system. These conscious design choices will limit access to the personal information, thereby mitigating any possible privacy risks associated with this program.

Conclusion

TSA is performing these threat assessments to determine whether access to SSI may be granted to individuals for use in federal civil court proceedings. Privacy impacts associated with this collection have been minimized by limiting the information provided to TSA and employing appropriate technical and operational safeguards and requirements. If TSA makes any changes to this program or the data elements needed for conducting the relevant threat assessments on individuals, those changes will be reflected in an amended version of this PIA.

Responsible Official

Andrew Colsky
Sensitive Security Information Office
Transportation Security Administration
Arlington, VA 22202

Approval Signature

_____

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

APPENDIX 1

Privacy Act Notice

Authority: 49 U.S.C. §114 authorizes the collection of this information.

Purpose: TSA will use this information to conduct a security threat assessment on individuals who seek access to Sensitive Security Information (SSI) for use in civil proceedings in federal courts.

Routine Uses: The information will be used by and disclosed to DHS personnel and contractors or other agents who need the information to assist in activities related to transportation security. Additionally, DHS may share the information with law enforcement, intelligence, or other government agencies as necessary to identify and respond to potential or actual threats to transportation security, or pursuant to its published Privacy Act system of records notice, DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS). This SORN was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731- 67735.

Disclosure: Furnishing this information is voluntary. However, failure to furnish the requested information may delay or prevent the completion of your security threat assessment, without which you may not be granted access to the SSI. Providing your SSN is voluntary but failure to provide it may result in a delay in processing your threat assessment.