Privacy Impact Assessment
for the

Security Threat Assessment for Airport Badge and Credential Holders

June 2, 2008

Contact Point
Douglas Hofsass
Acting General Manager, Commercial Airports
Transportation Sector Network Management
Transportation Security Administration
Douglas.Hofsass@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

Abstract

The Transportation Security Administration (TSA) is updating the Privacy Impact Assessment for the Security Threat Assessment (STA) for Airport Badge and Credential Holders to reflect an expansion of the covered population to include certain holders of airport approved badges, and to reflect the use of US-VISIT's Automated Biometrics Identification System (IDENT) database as part of the STA process, including enrollment of fingerprints in that database for recurring checks. This Privacy Impact Assessment (PIA) is an updated and amended version of the PIA originally published by TSA on June 15, 2004, and subsequently amended on August 19, 2005 and on December 20, 2006. The requirements addressed in the previous PIAs are still in effect, including the requirement to conduct name-based STAs on all individuals seeking or holding airport identification badges or credentials and the requirement to conduct fingerprint-based criminal history record checks (CHRCs) along with name-based checks on individuals seeking access to the Security Identification Display Area (SIDA) or Sterile Area of an airport.

Overview

TSA has the statutory responsibility for requiring by regulation "employment investigation[s], including a criminal history record check and a review of available law enforcement data bases and records of other governmental and international agencies" for individuals who have "unescorted access" to the secure areas of airports and aircraft. 49 USC §44936. In addition, TSA has statutory responsibility to assess threats to transportation. 49 USC §114. In order to facilitate the required "review of available law enforcement data bases and records of other governmental and international agencies," TSA requires name-based STAs for all individuals seeking or holding airport identification badges or credentials, regardless of the level of access to airport facilities, in order to identify potential or actual threats to transportation or national security. The name-based STA involves recurring checks against Federal terrorist, immigration, and law enforcement databases.

TSA implemented the criminal history record check requirement in regulations codified at 49 CFR parts 1542, 1544, and Security Directives requiring fingerprint-based CHRCs. In addition to undergoing the name-based STA, individuals seeking credentials authorizing unescorted access to sterile areas, secured areas, and Security Identification Display Areas (SIDA) must undergo a fingerprint-based CHRC. These individuals must submit their fingerprints to the sponsoring airport or aircraft operator who then sends the information to their service provider to aggregate the fingerprint data and convert any paper fingerprint cards into an electronic format. The service provider then sends the fingerprint information via secure email to TSA. TSA forwards the fingerprint information to the Federal Bureau of Investigation (FBI) to conduct a fingerprint-based CHRC. The results of the CHRC are returned through TSA to the airport for adjudication of the CHRC by the airport or aircraft operator.

With this update to the PIA, TSA will also now transmit these already collected fingerprints to US-VISIT for enrollment into IDENT for recurring checks against immigration, terrorism, and law enforcement databases held in IDENT. IDENT is a DHS-wide system for the storage and processing of biometric and biographic information for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.

Additionally, TSA is expanding the requirement for name-based STAs to include individuals who

hold or are applying for any identification credential or badge issued by an entity approved by the airport to issue identification credentials or badges, except entities holding TSA-approved or accepted security programs under 49 CFR parts 1544 or 1546. It does NOT include direct employees of a Federal, State, or local government, including law enforcement officers, who, as a condition of employment, have been subjected to an employment investigation that includes a fingerprint-based Criminal History Records Check (CHRC). For example, an airport may approve the employee badge of a tenant company on the airport such as a catering company or a fueler. Fingerprint-based checks will also be conducted for those individuals whose airport approved badge involves access to the sterile area, secure area, or SIDA.

Because this update entails the collection of personally identifiable information (PII) from a new population and adds IDENT database checks as part of the STA process, the E-Government Act of 2002 requires that TSA conduct a PIA.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

TSA collects the following information from individuals to conduct STAs: full name (last, first, middle as appearing on government-issued ID), alias(es), gender, date of birth, place of birth, Social Security Number (SSN), home address, phone number, submitting entity (i.e., employer or prospective employer), fingerprints, citizenship, and, if applicable, passport number and country of issuance, alien registration number, and non-immigrant visa number. In addition, individuals who must submit fingerprints will also provide race, height, weight, eye color, and hair color. TSA will also collect the results of STA.

1.2 What are the sources of the information in the system?

TSA collects the information provided by individuals to their airports. In addition, the system may also include information originating from the terrorism, immigration, or law enforcement databases queried as part of the STA, such as US-VISIT for IDENT checks.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is collected to conduct STAs on individuals to ensure they do not pose, and are not suspected of posing, a threat to transportation or national security.

1.4 How is the information collected?

The Airport Security Coordinator (ASC) as required by Title 49, Code of Federal Regulations (CFR) part 1542 submits the individual's information to TSA through a secure web-based application operated by a service provider used by the aviation industry. (ASCs at smaller airports may also submit hard-copy fingerprints to TSA via the enrollment aggregator.)

1.5 How will the information be checked for accuracy?

Information collected from individuals is presumed to be accurate. In addition, individuals have an opportunity to correct inaccurate information as part of the redress process. Further, the service provider to the aviation industry that aggregates the information ensures that biometric and biographic information is correctly matched. TSA also expects to verify the accuracy of SSN with the Social Security Administration.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

49 U.S.C. §114(f); 49 U.S.C. §44936; 31 U.S.C. §7701. TSA has issued regulations implementing this authority with reference to airports at 49 CFR part 1542.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

TSA collects data elements designed to assist in completing the STA. Based on its experience conducting STAs, TSA collects information used to match individuals against various databases containing different elements while reducing the number of false positives and false negatives. TSA also collects contact information so that TSA can communicate with the individual in the event there are any issues requiring redress. This updated PIA expanded the population covered, but collects the same types of data as previously collected. Privacy risks include the potential for loss or unauthorized access to information, which is mitigated by imposing administrative and technical limits on access to the information.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

TSA uses biographic information collected from individuals described in Section 1.1 above to conduct name-based STAs of persons seeking airport badges or credentials to identify potential or actual threats to transportation or national security. The STA involves recurring checks against Federal terrorist, immigration, and law enforcement databases. In addition, individuals seeking credentials authorizing unescorted access to sterile areas, secured areas, and Security Identification Display Areas (SIDA) must submit their fingerprints to the sponsoring airport or aircraft operator who, in turn, sends this information to their service provider to aggregate the fingerprint data and convert any paper fingerprint cards into an electronic format. The service provider then sends the information via secure email to TSA. TSA sends the fingerprint information to the Federal Bureau of investigation (FBI) to conduct a fingerprint-based CHRC. Adjudication of the CHRC is conducted by the airport. TSA will also transmit these already collected fingerprints to US VISIT to perform checks against immigration, terrorism and law enforcement databases held in IDENT. Additionally, TSA requires STAs for certain individuals with airport approved badges.

Fingerprint-based checks will be conducted for those individuals whose airport approved badge involves access to the sterile area, secure area, or SIDA.

TSA will also share information with the Social Security Administration in order to confirm the validity of SSN provided by the individual. Individuals will be asked to expressly authorize the Social Security Administration to confirm the validity of the SSN.

When necessary, TSA will forward the name of any individual who poses or is suspected of posing a threat to transportation or national security to the appropriate intelligence, immigration, and/or law enforcement agency or agencies. In these cases, the agency analyzes the information, determines whether the individual poses or is suspected of posing a threat to transportation or national security and notifies TSA of the determination so TSA can facilitate an appropriate operational response or notification to the airport or aircraft operator. Additionally, the immigration, law enforcement, or intelligence agency may take appropriate action concerning the individual, depending on the information.

2.2 What types of tools are used to analyze data and what type of data may be produced?

TSA matches individual information against terrorism, law enforcement, and immigration databases. The data produced is an STA result or CHRC result.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Commercial data is not used by this system, but it is anticipated that TSA may in the future require airports to conduct identity verification efforts that will include the use of commercial data. This PIA will be updated if commercial database checks are required. Publicly available information such as court records may be used on occasion to resolve individual status when criminal or immigration case disposition information is otherwise unavailable.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

User access is limited to individuals with a need to know the information for purposes of the program or to conduct the STA.

Section 3.0 Retention

3.1 What information is retained?

TSA retains the biographic and biometric information, as well as the STA result.

3.2 How long is information retained?

TSA will retain the information in accordance with the National Archives and Records Administration (NARA) records schedule approved March 8, 2007, Transportation Threat Assessment and Credentialing. The approved NARA schedule contains the following dispositions:

- TSA will delete/destroy information contained in the Subject Database System one year after an individual's credential or access privilege granted based upon the STA is no longer valid. In addition, for those individuals who may originally have appeared to be a match to a government watch list, but are subsequently cleared as not posing a threat to transportation or national security, retained information will be deleted/destroyed seven years after completion of the STA, or one year after any credential or access privilege granted based on the STA is no longer valid, whichever is longer.
- Information contained in the Subject Database System on individuals that are actual matches to a government watch list or otherwise pose a threat to transportation or national security, will be deleted/destroyed ninety-nine years after completion of the STA, or seven years after TSA learns that the individual is deceased, whichever is shorter.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, it was approved on March 8, 2007.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

TSA will retain these records in accordance with the records retention schedule approved by NARA. The retention schedule was developed to provide flexibility to accommodate continued facility access by the individual. TSA will delete the individual's information one year after it is notified by the airport that the individual's access is no longer valid. Individuals originally identified as a possible match but subsequently cleared will have their information retained for seven years in order to provide the maximum opportunity for redress or review.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information will be shared within DHS with those officials and employees who have a need for the information in the performance of their duties. In the ordinary course, it is expected that information will be shared within TSA with the Office of Transportation Threat Assessment and Credentialing (TTAC),

Office of Intelligence in the event of a match or possible match, Office of Chief Counsel for enforcement action or other investigation, Office of Security Operations for operational response, and the Office of Transportation Security Network Management for program management. Information may 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 or inquiries. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a. It is also expected that information will be shared with U.S. Immigration & Customs Enforcement (ICE) and U.S. Citizenship & Immigration Service (USCIS) for immigration issues.

TSA will also share fingerprints and associated biographic information with DHS's Automated Biometric Identification System (IDENT) as part of the STA. Further information about IDENT can be found in the IDENT PIA published by US-VISIT and publicly available on the DHS website.

4.2 How is the information transmitted or disclosed?

Depending on the urgency, information may be transmitted electronically, in person, in paper format, via facsimile, or by telephone. In most cases, the data will be shared within DHS on the encrypted DHS information technology (IT) network.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Information is shared internally with those DHS employees and officials, including contractors, who have a need for the information in the performance of their duties. Privacy risks that personal information may be disclosed to unauthorized individuals is minimized using a set of layered privacy safeguards that include physical, technical, and administrative controls to protect personal information in the automated system, appropriate to its level of sensitivity. Privacy risks associated with sharing information with IDENT is mitigated by sharing in accordance with the Privacy Act and DHS/TSA 002 SORN, (Transportation Security Threat Assessment System) and by the system user limitations within the IDENT system identified in the IDENT PIA.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The information will be shared with airports and their service providers who aggregate individual information to provide to TSA. The information will be shared with the FBI for criminal history records checks and with the Terrorist Screening Center to resolve potential watch list matches. TSA also may share the information it receives with Federal, State or local law enforcement, immigration, or intelligence agencies or other organizations, in accordance with the routine uses identified in the applicable Privacy Act systems of records notice (SORN), DHS/TSA 002, Transportation Security Threat Assessment System

(TSTAS). This SORN was last published in the *Federal Register* on November 8, 2005, and can be found at 70 FR 67731-67735.

TSA will also share information with the Social Security Administration in order to confirm the validity of SSN provided by the individual. Individuals will be asked to expressly authorize the Social Security Administration to confirm the validity of the SSN.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes, sharing of information outside the Department is compatible with the original collection. Sharing will be to identify individuals who may pose a risk to transportation or national security, or for purposes of issuing credentials or other benefit. All sharing of information outside of DHS is covered by the above referenced SORN.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Depending on the recipient and the urgency of the request or disclosure, the information may be transmitted or disclosed telephonically, electronically via a secure data network, via facsimile or via password-protected electronic mail.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

TSA will share this information under the applicable provisions of the SORN and the Privacy Act. TSA mitigates attendant privacy risk by limiting the sharing of this information to those who have an official need to know the information.

Section 6.0 Notice

6.1 Was notice provided to the applicant prior to collection of information?

A Privacy Act Statement is provided to individuals at the time they submit their information to the appropriate entity. The publication of this PIA and the applicable SORN, DHS/TSA 002, Transportation

Security Threat Assessment System, also serves to provide public notice of the collection, use and maintenance of this information.

6.2 Do applicants have the opportunity and/or right to decline to provide information?

The individual is notified that they have an opportunity and/or right to decline to provide the identifying information requested. However, failure to provide the required information will result in TSA declining to process the application or being unable to determine whether the individual poses a threat to transportation or national security, which will result in a denial of access privileges or access credentials for which the individual applied.

6.3 Do applicants have the right to consent to particular uses of the information? If so, how does the applicant exercise the right?

No.

6.4 Privacy Impact Analysis: Describe how notice is provided to applicants, and how the risks associated with applicants being unaware of the collection are mitigated.

Individuals are provided with notice that enables them to exercise informed consent prior to disclosing any information to TSA, and have the right to refuse to provide information. Collection of the requested information is overt and apparent to the individual. Fingerprints and biographic information shared with IDENT will be enrolled in the IDENT system and may be shared within DHS with those employees who have a need for the information in the course of performing their duties, and outside of DHS in accordance with the Privacy Act and TSA system of records DHS/TSA 002. The privacy risk associated with sharing information with IDENT without notice to those individuals who have already provided information is mitigated because sharing internal to DHS for immigration purposes has previously been disclosed to individuals.

Section 7.0 Access, Redress and Correction

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

Individuals may request releasable 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
Freedom of Information Act Office, TSA-20
11th Floor, East Tower
601 South 12th Street

Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by or by email at FOIA.TSA@dhs.gov. 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/research/foia/index.shtm).

In addition, individuals may request access to and amendment of their records through the redress process as explained in paragraph 7.2 below.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If an individual is disqualified because of the criminal history records check, the individual must notify the airport in writing of his or her intent to correct any information believed to be inaccurate within 30 days of being advised of disqualifying information. The applicant is responsible for correcting information by contacting the law enforcement jurisdiction responsible for the information and must apply for redress from the airport.

If the applicant believes he or she has been wrongly identified as a security threat relative to the STA, TSA provides a redress process and information on how to obtain releasable materials. There may be information or materials that are classified or otherwise protected by law or regulation that TSA will not disclose. All requests for releasable materials and challenges to the STA, must be submitted to TSA's Office of Transportation Threat Assessment and Credentialing at the below address.

Transportation Security Administration
TSA AV WORKER
TSA-19
601 S. 12th Street
Arlington, VA 22202

If TSA is unable to confirm the validity of the SSN, the individual must work through the Social Security Administration to resolve any issue.

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

TSA may send adverse notification directly to the individual in writing, by letter, electronic mail message, or facsimile. At the time of an adverse notification to an individual, TSA includes the appropriate procedures for redress and correction of information.

7.4 If no formal redress is provided, what alternatives are available to the applicant?

A redress process is provided for individuals who believe that they have been wrongfully denied the airport area access privileges and/or credentials for which they applied.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to applicants and how those risks are mitigated.

Individuals may request access to or correction of their personal information pursuant to the redress process described in 7.2 and pursuant to the Freedom of Information Act and Privacy Act of 1974. Privacy risks associated with redress include the collection of additional information on the individual. Risks are mitigated by handling the information in the same way other data associated with the STA process are handled.

Section 8.0 Technical Access and Security

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

TSA information systems are protected by systems of passwords, restricted access and other measures to mitigate the risk of unauthorized access to sensitive information.

8.2 Will Department contractors have access to the system?

Yes. Contractors hired by TSA to perform IT maintenance and security monitoring tasks have access to the systems to perform their official duties. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA IT Security Officers. Additionally, TSA may use contract adjudicators to review STA information. All contractors performing this work are subject to requirements for suitability and a background investigation as required by TSA Management Directive 1400.3, TSA Information Security Policy.

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

All government and contractor personnel are required to complete on-line TSA Privacy Training, which includes a discussion of Fair Information Practices (FIPs) and instructions on handling personally identifiable information in accordance with FIPs and TSA Privacy Policies. Compliance with this requirement is audited monthly by the TSA Privacy Officer. In addition, security training is provided which helps to raise the level of awareness for protecting personal information being processed. All IT security training is reported as required in the Federal Information Security Management Act of 2002,

Pub.L.107-347 (FISMA). Individuals accessing the system must have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on TSA security policies and procedures.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. Information in TSA's IT 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. The TSA systems associated with this PIA are operating on the authority of the Designated Accrediting Authority (DAA). Certification and Accreditation for the Crew Vetting Platform was received on September 1, 2005, and for the Screening Gateway on December 2, 2005.

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

TSA system logs are reviewed to ensure no unauthorized access has taken place. All IT systems are audited annually for IT security policy compliance and technical vulnerability by the TSA IT Security Office. TSA ensures the confidentiality, integrity and availability of the data through a defense in depth strategy. Use of firewalls, intrusion detection systems, virtual private networks, encryption, access controls, identity management and other technologies ensures that this program complies with all DHS Security requirements.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

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 and biometrics. 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.

Section 9.0 Technology

9.1 What type of project is the program or system?

This program is a database matching program that seeks to determine whether individual individuals are identified in law enforcement, immigration, or intelligence databases as posing or potentially posing a threat to transportation or national security.

9.2 What stage of development is the system in and what project development lifecycle was used?

The programs assessed are operational. This PIA reflects the expansion of certain STA requirements to a larger population, and the enrollment of fingerprints within IDENT.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security