Privacy Impact Assessment (Amended)
for the

Security Threat Assessment for SIDA and Sterile Area Workers

August 19, 2005

Contact Point
Lisa Dean
Privacy Officer
Transportation Security Administration
(571) 227-3947

Reviewing Official
Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security
Arlington, VA 22202
(571) 227-3813

I. Introduction

This Privacy Impact Assessment (PIA) is an updated and amended version of the PIA originally published by TSA on June 15, 2004. TSA has revised the security threat assessment required for individuals who have "unescorted access" to the secure areas of airports and aircraft to include an immigration status check for these individuals. Immigration status information will be part of TSA security threat assessments to identify individuals who may be subject to coercion related to their immigration status or may otherwise pose a threat to transportation security. This change is necessary in order to improve the efficacy of security threat assessments for this program and should not negatively impact the privacy of individuals in the program.

The Transportation Security Administration 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.

TSA implemented the criminal history record check in regulations codified at 49 CFR parts 1542, 1544, and Security Directives by requiring a fingerprint-based criminal history records check (CHRC) for individuals with unescorted access authority to Security Identification Display Areas (SIDA), workers who perform duties in airport sterile areas, [and individuals who are applying for these positions (referred to collectively as SIDA and Sterile Area Workers throughout this document)]. In order to facilitate the required "review of available law enforcement data bases and records of other governmental and international agencies," TSA also conducts a name-based security threat assessment under the authority vested in the Under Secretary of Transportation for Security found at 49 U.S.C. § 114(f).

The TSA Office of Transportation Vetting and Credentialing (OTVC) is the office within TSA that is responsible for conducting name-based and fingerprint based checks on SIDA and Sterile Area Workers. Additionally, the OTVC implements policies associated with airport secure areas and provides support to the airport and airline security officers who adjudicate the results of the criminal history checks. Consequently, the OTVC shares information on a regular basis with the American Association of Airport Executives (AAAE), airport and airline industry personnel, the Federal Bureau of Investigation (FBI), U.S. Immigration and Customs Enforcement (ICE), other Department of Homeland Security components, and other federal, state, and local law enforcement entities in carrying out these responsibilities.

This PIA is conducted pursuant to the E-Government Act of 2002, P.L. 107-347, and the accompanying guidelines issued by the Office of Management and Budget (OMB) on September 26, 2003, and is based on the current design of the program and the Privacy Act System of Records Notice, Transportation Security Threat Assessment System (DHS/TSA 002), that was published in the Federal Register on September 24, 2004, and amended on December 10, 2004. This PIA provides further detail about the collection of personally identifiable information for the purpose of conducting the security threat assessments described above.

II. System Overview

1. What information will be collected and used for this security threat assessment?

The following information is collected for SIDA and Sterile Area Worker security threat assessments: full name, aliases, date of birth, citizenship information, including immigration status (if applicable), gender, race, height, weight, eye color, hair color, fingerprints, place of birth, social security number (voluntary but recommended), address, employer's name, and employer's address.

2. Why is the information being collected and who is affected by the collection of this data?

The information is being collected in order to carry out TSA's statutory mandate to perform security threat assessments on transportation workers. All SIDA and Sterile Area Workers holders will be affected by this program.

3. What information technology system(s) will be used for this program and how will they be integrated?

Fingerprint-based check

Currently, each SIDA and Sterile Area Worker must complete a fingerprint application and submit fingerprints. The sponsoring airport or aircraft operator employer collects and maintains this information in either paper or electronic form. Once the information is collected, the employer sends it to the AAAE, an association that completes quality control procedures on the information and facilitates the transfer of it between TSA and airline and airport employers. This is a service AAAE provides airports, air carriers, and AAAE members. Using AAAE provides one point of contact instead of multiple contacts, and facilitates formatting all data received into one workable format for TSA.

AAAE converts paper fingerprint submissions into an electronic format if the employer does not have the capacity to do so. This diminishes the number of unreadable prints and facilitates a better turn-around time. AAAE sends this information to TSA via secured email. TSA then transmits the information, including the fingerprints, to the FBI for a criminal history records check. The FBI returns the results to TSA's secure Fingerprint Results Distribution (FPRD) website, where the air carrier and airport employer security representatives can access the information and adjudicate the results.

Name-based Check

The information being transmitted to the AAAE by the employers will be used by TSA to conduct the security threat assessment, which includes an immigration status check. AAAE will forward a portion of the information being collected for the fingerprint-based checks via secured email to TSA. The information forwarded is as follows: name, aliases, social security number, address information, place of birth, date of birth, gender, citizenship, immigration status (if applicable), employer's name, and employer's address.

TSA will run this information through terrorist-related and immigration databases it maintains or uses. Any application that meets the minimum criteria established by TSA as a possible match with

information contained in these databases will undergo further analysis. After TSA reviews the records of potential matches and any records regarding immigration status checks, the name of any SIDA and Sterile Area Worker that poses or is suspected of posing a security threat will be forwarded to appropriate intelligence and/or law enforcement agency(ies) for further analysis. The law enforcement or intelligence agency will analyze the information, determine whether the individual's identity can be verified and whether he or she continues to pose a threat or is suspected of posing a threat.

If the individual is found to continue to pose or is suspected of posing a security threat, the law enforcement or intelligence agency will notify TSA of the determination so TSA can inform the airport or air carrier employer that the worker's access should be rescinded. The law enforcement or intelligence agency may take further action concerning the individual. Individuals will be given an opportunity to correct any incorrect underlying identification or court records. TSA will continue this procedure to ensure that any resulting information suggesting a connection between a SIDA and Sterile Area Worker and terrorist activities or illegal immigration status is as narrowly drawn as possible. TSA plans to continue conducting these security threat assessments and immigration status checks indefinitely.

4. What notice or opportunities for consent are provided to individuals regarding what information is collected, and how that information is shared?

SIDA and Sterile Area Workers are provided with a Privacy Act notice describing the authority to collect the data, the purpose for collecting the data, and the routine uses for the collection of biographic and biometric (fingerprint) data. TSA's System of Records Notice entitled Transportation Security Threat Assessment System (DHS/TSA 002), which was published in the Federal Register, and is discussed below, also provides public notice of the collection, use, and disclosure of this information.

5. Does this program create a new system of records under the Privacy Act?

No. This program is covered under a Privacy Act system of records that was established in 2004 called the Transportation Security Threat Assessment System (DHS/TSA 002). The purpose of this system of records is to facilitate the performance of background investigations of transportation workers to ensure transportation security. The System of Records Notice was published in the Federal Register on September 24, 2004, and amended on December 10, 2004. It can be found at 69 Fed. Reg. 57348, 57349 and at 69 Fed. Reg. 71837.

6. What is the intended use of the information collected?

The information collected will be used for performing security threat assessments for SIDA and Sterile Area Workers, which includes fingerprint-based checks of criminal databases and name-based checks against terrorist-related databases and immigration databases TSA maintains or uses.

7. With whom will the collected information be shared?

The information will be shared with the appropriate Department of Homeland Security (DHS) personnel and contractors who, by law or contract are subject to the Privacy Act and who are involved in the security threat assessment process, including conducting immigration status checks. TSA may also share

information within DHS law enforcement components who need the information as part of law enforcement activities. For example, information may be shared with ICE for review of immigration status. If persons pose or are suspected of posing a security threat, then TSA will notify the appropriate law enforcement and/or intelligence agency. The collection, maintenance, and disclosure of information will be conducted in compliance with the Privacy Act and the published System of Records Notice.

8. How will the information be secured against unauthorized use? (What technological mechanism will be used to ensure security against hackers or malicious intent?)

TSA will secure personal information against unauthorized use through the use of a layered security approach involving procedural and information security safeguards. Specific privacy safeguards can be categorized by the following means, which are described in greater detail elsewhere in this document:

- Technical limitations on, and tracking of, data access and use;
- Use of secure telecommunications techniques; and
- Limitation of physical access to system databases and workstations.

This approach protects the information in accordance with the following requirements:

The Privacy Act of 1974, as amended, (5 USC 552a) which requires Federal agencies to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of information protected by the Act.

Federal Information Security Management Act of 2002, (Public Law 107-347), which establishes minimum acceptable security practices for Federal computer systems.

9. Will the information be retained and if so, for what period of time?

TSA is in the process of developing a records retention schedule that would permit it to destroy these records after a determined period of time. Until NARA approves this records schedule, however, TSA does not have legal authority to dispose of these records. TSA has requested a short retention period for these records from NARA. TSA intends to retain the information related to the criminal history records check for up to sixty days. Once TSA receives authority to dispose of these records, TSA will purge results from individuals who no longer possess a credential. TSA will update the other records periodically consistent with regulations that will require SIDA and Sterile Area Workers to submit to periodic security threat assessments including the criminal history records check. The criminal history records check results (rap sheet information) are maintained by TSA on the Fingerprint Results Distribution website. TSA will need to keep this information because it formed the basis for the final adjudication decision. The individual record may be used to determine if the granting of the credential was made correctly. These records may also be used for auditing airports/airlines.

TSA will maintain the data for the name-based portion of the security threat assessments. TSA also intends to retain these records for a sufficient period of time to permit affected individuals an opportunity to pursue redress or appeal measures, as well as for program auditing purposes.

10. How will the SIDA and Sterile Area Workers be able to seek redress?

In the case of criminal history records checks adjudicated by employers, if an individual applying for a credential disputes the results of a CHRC (i.e., that the disposition of a charge (s) is incorrect), the applicant can provide court documentation to his or her employer's security office. If the applicant can show that the disposition (or charge) does not fall under the disqualifying offense category; he or she will be granted a credential. If the applicant can show that corrected disposition or charge no longer falls under the disqualifying offense category; he or she will be granted a credential. NOTE: The employer's security office will need to contact TSA (the CHRC requestor) to verify with the Federal Bureau of Investigation that the court record has been changed in favor of the applicant.

Individuals who believe that they have been wrongly identified as a security threat will be given the opportunity to contact TSA to address their concerns. Redress based on the name-based portion of the security threat assessment will be handled on a case-by-case basis due to the classified and/or security sensitive information that may be involved. TSA will provide information on which the determination was based to the applicant to the extent permitted by law. There may be items that are classified or sensitive security information that cannot be released. Individuals who believe that their immigration status check determination is inaccurate should contact ICE to address their concerns.

11. What is the step-by-step process of how the systems will work once the data has been input and what is the process for generating a response?

The process for completing the security threat assessment is described below.

For the fingerprint-based criminal history records check, AAAE consolidates information from the airlines and airports and provides it to TSA, which forwards the information to the FBI. The FBI runs the information in its Criminal Justice Information System (CJIS). Results from the run (rap sheet information) are provided back to TSA, and TSA posts the results on a secure, password protected website. Airport and airline personnel security officers review and adjudicate the results based on a list of disqualifying criminal offenses and decide to either grant or deny access to the SIDA and Sterile Area Worker.

For the name-based portion of the security threat assessment, AAAE consolidates information from the airlines and airports and provides it to TSA. TSA runs the information provided through terrorist-related and immigration databases it maintains or uses. TSA will analyze the record of any individual that appears to be a possible match.

After TSA reviews the records of potential matches and any records regarding immigration status, the name of any individual that poses or is suspected of posing a security threat will be forwarded to appropriate law enforcement and/or intelligence agency for further analysis. The law enforcement or intelligence agency will analyze the information, determine whether the individual's identity can be verified and whether he or she continues to pose a threat or is suspected of posing a threat. If so, the law enforcement or intelligence agency will notify TSA of the determination so TSA can inform the airport or airline that the worker's access should be rescinded. The law enforcement or intelligence agency will take appropriate action concerning the individual, depending on what information connects the individual to terrorist activity or immigration violation. Individuals will be given the opportunity to correct any

incorrect underlying identification or court records. TSA will continue this procedure to ensure that any resulting information suggesting a connection between a SIDA and Sterile Area Worker and terrorist activities or illegal immigration status is as narrowly drawn as possible.

12. What technical safeguards are in place to secure the data?

DHS employs the following technical safeguards to secure data:

- Use of advanced encryption technology to prevent internal and external tampering of TSA data and transmissions.
- Secure data transmission, including the use of password-protected e-mail for sending files among the participants listed above, to prevent unauthorized internal and external access.
- Password protection for files containing personal or security threat assessment data to prevent unauthorized internal and external access.
- Network firewalls to prevent intrusion into DHS network and TSA databases.
- User identification and password authentication to prevent access to security threat assessment systems by unauthorized users.
- Security auditing tools to identify the source of failed TSA system access attempts by unauthorized users and the improper use of data by authorized operators.

13. Will the staff working with the data have appropriate training and security clearances to handle the sensitivity of the information?

All TSA and contractor staff receives TSA-mandated privacy training on the use and disclosure of personal data. Additionally, training will be conducted that relates to the handling of personal data specifically related to the SIDA and Sterile Area Workers security threat assessment. Staff assigned to handle classified threat assessment information will be required to obtain appropriate security clearances.

Additionally, all staff must hold appropriate credentials for physical access to the sites housing the security threat assessment databases and management applications. Physical access safeguards include the use of armed or unarmed security guards at sites; hard-bolting or fastening of databases, servers, and workstations; and credential readers for internal and external site access. The DHS contractors also hold appropriate facility security clearances.

III. For questions or comments, please contact:

Lisa S. Dean, Privacy Officer, Transportation Security Administration, 571-227-3947

Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, 571-227-3813