Privacy Impact Assessment
for the

Maryland-Three (MD-3) Airports

February 20, 2009

Contact Point
Erik Jensen
Assistant General Manager, General Aviation
Transportation Sector Network Management
Transportation Security Administration

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

John Kropf
Acting Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Transportation Security Administration (TSA) conducts name-based Security Threat Assessments (STA) and fingerprint-based Criminal History Records Checks (CHRCs) on pilots who operate aircraft and apply for privileges to fly to or from the three General Aviation airports in the Washington, D.C. restricted flight zones (Potomac Airfield, Washington Executive/Hyde Field, and College Park Airport), otherwise known as the Maryland Three (MD-3) program, and for the Airport Security Coordinator (ASC)[1] at a MD-3 airport. For the STA process, TSA compares the biographical information of these pilots and ASCs, hereafter referred to as individuals, against Federal terrorist, immigration, and law enforcement databases. For the CHRC, TSA forwards the fingerprints to the Federal Bureau of Investigation (FBI), which conducts fingerprint-based CHRCs on individuals.

Overview

TSA conducts name-based STA's and fingerprint-based CHRC's on individuals who apply for privileges to fly to or from the three General Aviation airports in the Washington, D.C. restricted flight zones as part of the MD-3 program, and for the ASC at a MD-3 airport in accordance with 49 C.F.R. 1562.3.

The STAs include name-based checks against the consolidated terrorist watch list known as the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC)[2], and other relevant Federal immigration or law enforcement databases. In addition to undergoing the name-based STA, individuals must undergo a fingerprint-based CHRC conducted by the FBI. Fingerprints may also be shared within the DHS using DHS's US-VISIT IDENT[3] system in order to perform enhanced immigration checks. The purpose of these checks is to ensure that the individuals do not pose or are not suspected of posing a threat to transportation or national security.

Each of the MD-3 airports will direct individuals to the Reagan Washington National Airport's (DCA) badging office. Once at the airport badging office, the individual will provide the DCA ASC with his or her fingerprints[4] as well as biographic information. The DCA ASC sends this information over a password protected dial-up connection to a private sector service provider who collects and forwards the biographic and biometric information to TSA. TSA uses the biographic information to conduct the STA and forwards the biometric information to the FBI to conduct the CHRC. TSA adjudicates the results of the CHRC to determine if the individual has been convicted of any disqualifying criminal offenses.

---

[1] The Airport Security Coordinator is the official responsible for ensuring that the airport's security are implemented and followed.

[2] The TSC is an entity established by the Attorney General in coordination with the Secretary of State, the Secretary of Homeland Security, the Director of the Central Intelligence Agency, the Secretary of the Treasury, and the Secretary of Defense. The Attorney General, acting through the Director of the FBI, established the TSC in support of Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, which required the Attorney General to establish an organization to consolidate the Federal Government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. The TSC maintains the Federal Government's consolidated and integrated terrorist watch list, known as the TSDB.

[3] For additional information, see US-VISIT PIA and SORN at www.dhs.gov/privacy

[4] Paper fingerprint cards may be used if the individual's fingerprints are too light to be read by an electronic device.

In conducting STAs and CHRCs on these individuals, TSA communicates with private-sector enrollment providers[5], airport and airline industry personnel, the Federal Bureau of Investigation (FBI) and other Federal, state, and local law enforcement agencies. Because these programs entail a collection of personally identifiable information (PII), the E-Government Act of 2002 requires that TSA conduct a Privacy Impact Assessment (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 in order to conduct STAs and CHRCs: full name (last, first, middle as appearing on a government-issued ID), alias(es), date of birth, Social Security Number (SSN) (voluntary but failure to provide may delay or prevent completion of the STA), home address, phone number, submitting entity (i.e., employer, pilot), fingerprints, and, if applicable, pilot's airmen certificate or student pilot certificate, and pilot's current medical certificate.

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

TSA collects the information from the individuals through private sector service providers, and also collects the results of the STA and CHRC from agencies queried as part of the STA and CHRC.

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

TSA collects the information in order to conduct STAs and CHRCs on individuals and ensure that they do not pose or are not suspected of posing a threat to transportation or national security.

1.4 How is the information collected?

Each of the MD-3 airports will direct individuals to the Reagan Washington National Airport's (DCA) badging office. Once at the airport badging office, the individual will provide the DCA ASC with his or her fingerprints[6] as well as biographic information. The DCA ASC sends this information over a password protected dial-up connection to a private sector service provider who collects and forwards the biographic and biometric information to TSA. TSA uses the biographic information to conduct the STA and forwards the biometric information to the FBI to conduct the CHRC. TSA adjudicates the results of the CHRC to determine if the individual has been convicted of any disqualifying criminal offenses.

[5] Private sector enrollment providers are the mechanisms through which airports and airlines submit data to TSA for STA and CHRC.
[6] Paper fingerprint cards may be used if the individual's fingerprints are too light to be read by an electronic device.

1.5 How will the information be checked for accuracy?

Information will be collected directly from individuals and is presumed to be accurate. As discussed in Section 7.0 of this PIA, individuals who believe they are wrongly identified as posing a threat to transportation or national security will have an opportunity for redress.

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

49 U.S.C. §114(f) authorizes TSA to assess threats to transportation and conduct security threat assessments for transportation security personnel. TSA has issued the following regulation governing the MD-3 program: 49 CFR Part 1562. In addition, Federal Aviation Administration (FAA) regulation 14 CFR Part 93 details the enhanced security procedures required for aircraft operators utilizing the MD-3 airports.

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 and the CHRC. Based on its experience conducting STAs, TSA collects information necessary to match individuals against various databases containing different elements while attempting to reduce 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. Privacy risk includes 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 the information to conduct STAs and CHRCs on individuals who are subject to TSA requirements for the MD-3 program. The STAs include name-based checks against the TSDB and other relevant Federal immigration and law enforcement databases on a recurring basis so long as the individual has privileges granted under a covered program, and for a year after TSA is notified that the individual's privileges are no longer valid. TSA expects to enroll individuals within the DHS IDENT database for recurring checks against immigration, law enforcement, and terrorism databases.

The purpose of the STA and the CHRC is to ensure that these individuals do not pose or are not suspected of posing a threat to transportation or national security. 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 and/or law enforcement agency or agencies, as described in Section 4 and Section 5 of this PIA. In these cases, the law enforcement and/or intelligence agency analyzes the information, and determines whether the individual poses or is suspected of posing a threat to transportation or national security. The law enforcement and/or intelligence agency will notify TSA of the

determination so TSA can facilitate an appropriate operational response. Additionally, the 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?

The STA and CHRC processes use name-matching and fingerprint-matching tools. The data produced is the matching result.

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

This system does not use commercial data. 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. The risk of collecting inaccurate information is minimized because individuals directly provide their information and are therefore likely to provide accurate information. The impact of inaccurate information is also minimized because individuals who feel they have been wrongly identified as a security threat can pursue redress through TSA allowing for additional review of the completeness and accuracy of the information (See Section 7.0 of this PIA).

Section 3.0 Retention

3.1 What information is retained?

TSA retains the biographic and fingerprint information noted in Section 1.1, as well as the results of the STA and CHRC checks.

3.2 How long is information retained?

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

TSA will delete/destroy the individual's information one year after TSA is notified that an individual's privilege granted based upon the STA/CHRC is no longer valid. In addition, information 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, will be deleted/destroyed seven years after completion of the STA/CHRC, or one year after any privilege granted based on the STA/CHRC is no longer valid, whichever is longer.

Information 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/CHRC, 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. TSA will maintain these records according to the schedule as reference materials for current and future checks involving the individual. Data retained for any length of time is subject to data security risks that are mitigated as described elsewhere in this PIA. There are no particular risks associated with the records retention schedule for this program.

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, employees, and contractors 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 with the Office of Transportation Threat Assessment and Credentialing (TTAC), Office of Intelligence (OI) in the event of a match or possible match, Office of Chief Counsel (OCC) for enforcement action or other investigation, Office of Security Operations (OSO) for operational response, and the Office of Transportation Security Network Management (TSNM) 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 expects to share fingerprints and associated biographic information with IDENT. Further information about IDENT can be found in the IDENT PIA and System of Records Notice (SORN) published by US-VISIT and publicly available on the DHS website (www.dhs.gov/privacy).

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.

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 private sector service providers who collect and forward individual information to TSA. Employers and individuals assigned to airport security offices may also have access to the information if the data is filtered through their operations. The information will be shared with the Terrorist Screening Center (TSC) to resolve potential watch list matches. TSA also may share the information it receives with Federal, State or local law enforcement or intelligence agencies or other organizations, in accordance with the routine uses identified in the applicable Privacy Act 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.

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.

The private sector service providers have a Memorandum Of Understanding (MOU) with TSA with respect to the sharing of this information. 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 a secure 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. By limiting the sharing of this information to those who have an official need to know the information, TSA is mitigating any attendant privacy risks.

Section 6.0 Notice

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

A TSA Privacy Act Statement (see Appendix A) is provided to individuals at the time they submit their information to the appropriate entity as described in Section 1.4. 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 individuals have the opportunity and/or right to decline to provide information?

Yes, the collection of information is voluntary. 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 requested information may result in TSA being unable to determine whether an individual poses a threat to transportation or national security, which will result in a denial of privileges for the applicable program for which the individual applied.

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

No.

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

TSA is collecting information provided by the individual to accurately conduct the STA and CHRC. Individuals are provided with notice that enables them to exercise informed consent prior to disclosing any information to TSA, and an individual always has the right to refuse to provide information.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals 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 20598-6020

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 amend 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?

In the event that any information is erroneous and/or an individual would like to appeal the adjudication decision, TSA provides a redress process.

For correction of criminal history records, the individual must notify the ASC at the appropriate MD-3 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 individual may request a copy of his or her criminal record from TTAC by submitting a written request to the address listed below. The individual is responsible for correcting information by contacting the law enforcement jurisdiction responsible for the information. The individual must submit all applicable information to TTAC within 45 days of the date when he or she notified their employer or ASC of their intent to correct the record. TSA will accept a copy of the revised FBI record or certified true copy of the information from the appropriate court or law enforcement agency. All documentation should be mailed to:

Transportation Security Administration
Office of Transportation Threat Assessment and Credentialing
Attention: Aviation Programs (TSA-19)
601 12th Street South
Arlington, VA 20598-6019

When individuals are disqualified as a result of the CHRC or immigration check, TSA provides written instructions as to how the individual may appeal the determination. If the individual can show that the disposition (or charge) does not fit within the disqualifying offense criteria set forth in the regulation, he or she will be approved. In addition, if the individual obtains a corrected criminal history record, and can show that corrected disposition or charge no longer falls under the disqualifying offense category, he or she will be approved.

If the individual believes he or she has been wrongly identified as a security threat based upon the STA, he or she will be given the opportunity to contact TTAC (at the address above) to address their concerns. Redress based on the STA 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 individual to the extent permitted by law. There may be items that are classified or sensitive security information that TSA cannot release. For the name-based STA, TSA will be the final adjudicator.

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

TSA sends all adverse notifications directly to the individuals in writing, by either letter or facsimile. At the time of an adverse notification to an individual, TSA includes the appropriate procedures (see 7.2 above) for redress and correction of information.

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

A redress process is provided for individuals who believe that they have been wrongfully denied the ability to avail themselves of the MD-3 program privileges.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals 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 and CHRC processes 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?

Access to the systems is only provided to users with a need to know. Those requiring access must meet security requirements and obtain approval from the system administrator before gaining access to the system. 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. TSA also employs processes to enforce separation of duties to prevent unauthorized disclosure or 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.

8.2 Will Department contractors have access to the system?

Yes. Contractors who are hired to perform many of the IT maintenance and security monitoring tasks have access to the systems in order 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, the TSA may use contract adjudicators to review criminal history and STA information. 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 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 DHS privacy training, which includes a discussion of Fair Information Practices (FIPs) and instructions on handling PII in accordance with FIPs and DHS 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 Program (CVP[7]) as received on March 1, 2007.

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

TSA system logs are audited annually to ensure no unauthorized access has taken place. All IT systems are audited for IT security policy compliance and technical vulnerability by the TSA IT Security Office. Through a defense in-depth strategy, TSA will ensure the confidentiality, integrity and availability of the data. 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 a DHS access badge. 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?

The programs assessed in this PIA are operational programs.

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

The programs assessed in this PIA underwent a regulatory rule-making process including notice to the public and evaluation of comments. The IT programs utilized in this PIA were developed using the System Development Life Cycle and are currently in the Operations and Maintenance phase.

[7] The CVP platform is the "system" that processes STAs for crew members. It also supports STAs for Airport Badge and Credential Holders (see PIA dated June 2, 2008.)

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

No.

Responsible Officials

Erik Jensen, Assistant General Manager, General Aviation

Transportation Sector Network Management

Transportation Security Administration

Approval Signature

Original signed copy on file with the DHS Privacy Office

John Kropf
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A – Privacy Act Notice

Privacy Act Notice

Authority: The authority for collecting this information is 49 U.S.C. 114, "Transportation Security Administration," and 49 U.S.C. 44936, "Employment Investigations and Restrictions."

Purpose: The information is needed to verify your identity and to retrieve your criminal history record to evaluate your suitability for access to airport sterile areas and security identification display areas (SIDAs), and aircraft. Your Social Security Number (SSN) will be used as your identification number in this process and to verify your identity. Furnishing this information, including your SSN, is voluntary, however, failure to provide it will prevent the completion of your criminal history records check, without which you may not be granted aircraft, sterile area or SIDA access.

Routine Uses: Routine uses of this information may include disclosure to the U.S. Office of Personnel this information may include disclosure to the U.S. Office of Personnel Management for processing and data verification, to the FBI to retrieve your criminal history record, to TSA contractors or other agents who assist in the maintenance and operation of the fingerprint system, to airport operators or aircraft operators to evaluate suitability for aircraft, sterile area or SIDA access, to appropriate governmental agencies for law enforcement or security purposes, or in the interests of national security, and to foreign and international governmental authorities in accordance with law and international agreement.