Privacy Impact Assessment
for the

Large Aircraft Security Program

October 2, 2008

Contact Point

Michal Morgan
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

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

Abstract

The Transportation Security Administration (TSA) proposes to amend current aviation transportation security regulations to expand the scope of current general aviation requirements and add new requirements for large aircraft operators and airports that service these aircraft. The proposed regulation would establish a security program called the Large Aircraft Security Program (LASP) for the large aircraft operators, and will require security threat assessments (STAs) for various categories of individuals. This Privacy Impact Assessment (PIA) is being conducted in conjunction with a Notice of Proposed Rule Making (NPRM). This PIA will be updated to reflect any changes made prior to publication of the Final Rule. No information will be collected by TSA prior to publication of the Final Rule.[1]

Introduction

To date, the government's focus with regard to aviation security generally has been on air carriers and commercial operators which offer transportation for compensation or hire. These carriers or commercial operators are required to submit to TSA security threat assessments (STA) and security programs prior to operating their aircraft. With a few exceptions, TSA does not currently require security threat assessments or security programs for general aviation aircraft operators, that is, individuals who are not offering transportation for compensation or hire.

Proposed Rule

TSA is proposing that most operations being conducted in aircraft with a maximum certificated takeoff weight (MTOW) above 12,500 pounds ("large aircraft"), including corporate and private aircraft, be required to adopt a large aircraft security program.[2] The large aircraft security program would require large aircraft operators to contract with TSA-approved auditors to conduct audits of the operators' compliance with their security programs and TSA regulations. Large aircraft operators would also be required to contract with TSA-approved watch list service providers to conduct watch list matching of their passengers against the No-Fly and Selectee Lists (collectively "watch list"). Passenger data would not be sent to TSA (except in the event of a possible match) under the NPRM, though it is expected that this population will eventually be covered by TSA's Secure Flight program. Auditors, relevant personnel employed by watch list service providers, and the flight crew members[3] of these large aircraft would be required to undergo a STA including a fingerprint-based criminal history records check (CHRC) and checks against law enforcement, terrorism, and immigration databases. Aircraft operators will undergo an STA and/or checks to confirm whether the operators are legitimate business entities and whether their owners are individuals who appear to pose a risk to aviation security. Additionally, operators of aircraft over 45,500 kilograms (kg) or with a 61 or more passenger seating configuration operated for compensation or hire will be

[1] The U.S Customs and Border Protection is issuing a Notice of Proposed Rule making that would require the advanced electronic transmission of information by private aircraft arriving from, departing, continuing within or overflying the United States.

[2] Exceptions will apply for operators under the full program, the full all-cargo program, a limited program, and certain government operations

[3] Flight crew member means a pilot, flight engineer, or navigator assigned to duty in an aircraft during flight time. See 49 C.F.R § 1540.5.

required to screen all passengers and their accessible property. Personnel performing these screening functions will also have to undergo an STA.

Section 1.0 Characterization of the Information

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

Passenger information: Under the NPRM, aircraft operators would be required to submit passenger full name to an approved Watch List Service Provider for watch list matching purposes. Passenger information will not be provided to TSA unless there is a possible match to the watch list. Aircraft operators would request, but not require, submission of passenger gender, date of birth, and TSA Redress Number (if applicable) to assist in eliminating misidentification.

Although TSA would not require large aircraft operators to request passport information from passengers, the proposed rule would require large aircraft operators to transmit certain information from an individual's passport (full name, passport number, country of issuance, expiration date, gender, and date of birth), if it is available and was provided to the aircraft operator. Aircraft operators will transmit the full name and other available passenger information after verifying the information with a government issued identification card[4]. Passengers who frequently fly with the aircraft operator may request to be placed on a Master Passenger List that will be continuously vetted by the Watch List Service Provider.

*Aircraft Operators***:** Aircraft operators required to have a security program under the LASP must submit the following information for purposes of administering the program and communicating with responsible personnel, and conducting a STA and/or checks confirming whether the operators are legitimate business entities and whether their owners are individuals who appear to pose a risk to aviation security:

1. Business name to include "doing business as" business names, state of incorporation if applicable and tax identification number;

2. Address of primary place of business or headquarters;

3. Name and address of each proprietor, general partner, officer, director, and owner;

4. FAA operating certificate number of the applicant, if applicable;

5. For contact purposes, the name, title, business address, business telephone number(s) and business electronic mail address of the Aircraft Operator Security Coordinator (AOSC) and any alternates.

Flight Crew, Auditors[5]*, Watch List Service Provider Covered Personnel*[6]*, and Screeners*[7]**:** These individuals must submit the information below for purposes of conducting a security threat assessment:

---

[4] For passengers on the Master Passenger List, this comparison will only be required when the passenger is initially placed on the list.

[5] Auditors must also provide an e-mail address and contact telephone number, as well as a copy of their accreditation or certification from a TSA approved organization.

[6] Employees, officer, principal, or program manager of the watch list service provider who collects, handles, or uses passenger information or watch list matching results or who conducts watch list matching.

(1) Legal name, including first, middle, and last: any applicable suffix, and any other named used previously;

(2) Current mailing address and residential address if it differs from the mailing address; and the previous residential address;

(3) Date of birth;

(4) Social security number; (Voluntary but failure to provide it may delay or prevent completion of the threat assessment);

(5) Gender;

(6) Height, weight, hair and eye color;

(7) City, state, and country of birth;

(8) Immigration status and date of naturalization if the individual is a naturalized citizen of the United States;

(9) Alien registration number, if applicable;

(10) The name, telephone number, and address of the individual's current employer(s). If the individual's current employer is the U.S. military service, include branch of service;

(11) Fingerprints in a manner prescribed by TSA;

(12) Passport number, city of issuance, date of issuance, and date of expiration (Voluntary but may assist the adjudication process);

(13) Department of State Consular Report of Birth Abroad (Voluntary but may assist the adjudication process);

(14) If the individual is not a national or citizen of the United States, the alien registration and/or the number assigned to the applicant on the U.S. Customs and Border Protection Arrival-Departure Record, Form I–94 (Voluntary but may assist the adjudication process);

(15) Whether the applicant has previously completed a TSA threat assessment, and if so, the date and program for which it was completed (Voluntary but may assist the adjudication process);

(16) Federal security clearance, if applicable, and the date the clearance was granted and the name of the agency that processed the clearance (Voluntary but may assist the adjudication process).

---

[7] Screeners are individuals who inspect individuals and property for weapons, explosives, and incendiaries. See 49 C.F.R. § 1540.5. For this program, they are employees and contractors for aircraft over 45,500 kilograms and with 61 or more passenger seating configuration operated for compensation or hire.

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

Except for passenger information, TSA proposes to collect the information listed in paragraph 1.1 above from the aircraft operators, flight crew members, auditors, covered personnel of watch list service providers, and screeners through an enrollment provider under contract to TSA. For passenger information, the aircraft operators will collect the information directly from the passengers.

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

Passengers.

The information is collected from the passengers in order to compare their names against the most current watch list. TSA has determined an individual's full name, gender, and date of birth are critically important for effective watch list matching. A redress number and passport information, if available, will reduce the chance of a false positive.

Aircraft Operators.

The information is collected from the aircraft operators in order to obtain addresses for where to send correspondence, to ensure that the operators are authorized to fly, to administer the program, and to provide a point of contact (the AOSC) if there is a need to immediately contact the operator. These individuals may undergo a STA. The business entity may undergo checks into the validity of the aircraft operator.

Flight crew member, auditors, watch list service provider covered personnel, and screeners.

Biographic information is collected from flight crew member, auditors, covered personnel of watch list service providers, and screeners to conduct security threat assessments on these individuals. TSA will compare the individuals' information against terrorist-related, law enforcement, and immigration databases that TSA uses in order to ensure that the individual does not pose or is not suspected of posing a threat to transportation or national security. Email address and telephone numbers for auditors are collected to facilitate administrative communication. Fingerprints are collected from the flight crew members, auditors, covered personnel of watch list service providers, and screeners to conduct a fingerprint-based criminal history records check.

1.4 How is the information collected?

Passenger information will be collected by aircraft operators orally or by electronic means. Information about individuals who are a possible match to a watchlist will be sent to TSA verbally or electronically. Information for other individuals will be collected by an enrollment provider who will transmit the information to TSA electronically**.**

1.5 How will the information be checked for accuracy?

Information will be confirmed by the aircraft operators and enrollment providers. To further ensure that correct and accurate information is provided, flight crew members, auditors, covered personnel

of watch list service providers, and screeners will be required to sign a statement under penalty of perjury that the information is true, complete and correct.

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

49 U.S.C. § 114(f).

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

The information collected will be used to conduct watch list screening or security threat assessments on flight crew members, passengers, auditors, covered personnel of watch list service providers, and screeners. Aircraft operators may undergo a STA and/or checks to confirm the validity of the business. TSA will seek comments on methods of conducting such checks on aircraft operators. The data elements collected increase the ability to promptly adjudicate any potential watch list match without having to contact the individual and reduce the number of individuals who will provide more extensive identifying information under the processes set forth in 7.2 for redress. Watch List Service Providers and enrollment providers will be required to implement data security measures prior to being approved by TSA.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

TSA will use information gathered from individuals for the following purposes:

1. To allow the watch list service providers to check passengers against the watch list;

2 To conduct security threat assessments on flight crew members, auditors, covered personnel for watch list service providers, and screeners;

3. To assist in the management of records and security threat assessments associated with the LASP;

4. To ensure that the aircraft operator meets the required security qualifications;

5. To refer to the appropriate intelligence and law enforcement entities the identity of flight crew members, passengers, auditors, covered personnel of watch list service providers, and screeners who pose or are suspected of posing a threat to transportation or national security.

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

None.

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

Per the NPRM, TSA will consider comments on methods for checking the validity of the aircraft operator. Such checks may involve a check against Dun & Bradstreet or similar commercial database. Commercial or publicly available data will not be used for the individuals covered by the LASP.

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.

This PIA and the TSA Office of Privacy Policy & Compliance are controls to ensure that information is handled in accordance with the uses described herein. In addition, the Privacy Act and applicable System of Records Notice are also such controls. TSA enforces the restrictions on the use of the information as part of the standards for participation in the program. Furthermore, the results of the watch list matching would be Sensitive Security Information (SSI). Therefore, the handling of SSI is be subject to 49 CFR part 1520, which provides in Section1520.17 grounds for civil penalties for unauthorized disclosure. The NPRM would also prohibit any unauthorized uses of the watchlist matching results.

Section 3.0 Retention

3.1 How long is the information retained?

TSA will retain security threat assessment data in accordance with the records retention schedule previously approved for the Transportation Threat Assessment and Credentialing program. Under this record retention schedule, TSA will retain records for one (1) year after an individual's access privilege under the STA is no longer valid. In addition, for those individuals who may originally have appeared to be a match to a watch list, but are subsequently cleared, TSA will retain the records for at least seven years or one year after which access privilege under the STA is no longer valid. For individuals who are an actual match to a watch list or otherwise determined to pose a threat to transportation or national security, TSA will retain the records for ninety-nine (99) years or seven (7) years after TSA learns the individual is deceased.

TSA is developing a records schedule to cover AOSC contact information, which will be submitted to National Archives and Records Administration (NARA) for review and approval. TSA expects the schedule to allow for the deletion of contact information when it becomes outdated and is no longer accurate. Until a schedule is approved by NARA, TSA will securely maintain all stakeholder POC information. The updated PIA and Final Rule will detail the retention schedule for OOSC contact information.

TSA will propose that auditor reports be retained for at least three years from the date of the last audit inspection. A record retention schedule will be prepared and will be submitted to the National Archives and Records Administration (NARA) for approval as described in Section 3.2. Until the schedule is approved by NARA, TSA will not destroy any audit records.

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

Yes. A schedule for audit inspection reports will be developed as described above and submitted to NARA when finalized.

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

Information collected through this program will be maintained in accordance with NARA-approved record retention schedules in furtherance of TSA's mission to ensure the security of the Nation's transportation system. Audit records will be retained for at least three (3) years to allow for adequate time between the biennial audit inspections. 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 organizations is the information shared, what information is shared, and for what purpose?

In the ordinary course, information will be retained and used within the Transportation Threat Assessment and Credentialing (TTAC) office, and within the Office of Transportation Sector Network Management (TSNM). TSA will also ordinarily share information with DHS components, including components contacted in connection with conducting immigration checks. TSA may also share information about individuals posing or suspected of posing a threat to transportation or national security within DHS for intelligence, counterintelligence, law enforcement, or other official purposes related to transportation security in accordance with the provisions of the Privacy Act, 5 U.S.C. §552a. TSA will share information about individuals with those DHS employees who need the information in the performance of their duties. For example, if an individual writes his/her Congressperson, information may be shared with the Office of Legislative Affairs or Office of Chief Counsel.

4.2 How is the information transmitted or disclosed?

TSA will only transmit this data within DHS and to TSA contractors who need the information to perform their official duties via a secure data network, facsimile, password protected CD, or telephonically. The method of transmission may vary according to specific circumstances. The information may also be marked with specific handling requirements and restrictions to further limit distribution.

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 may be shared with DHS employees and contractors who have a need for the information in the performance of their duties in accordance with the Privacy Act. 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, what information is shared, and for what purpose?

The watch list service providers will share the results of the watch list matching of each passenger with the aircraft operator that submitted that passenger's information. This information will be used by the aircraft operator to determine whether a passenger may be permitted to board the aircraft

TSA will inform flight crew members, auditors, screeners, and watch list service provider covered personnel of the results of his or her security threat assessment. If an individual receives a "Final Determination of Security Threat Assessment," TSA will inform the individual directly and provide the individual with the basis for that Final Determination. For an employee of the watch list service provider, TSA will notify the individual and the watch list service provider of the results of the security threat assessment but TSA would not inform the watch list service provider of the basis of a "Final Determination of Security Threat Assessment." Similarly, for a flight crew member or a screener, TSA will notify the individual and the aircraft operator of the results of the security threat assessment but TSA would not inform the aircraft operator of the basis of the Final Determination of Security Threat Assessment.

TSA may share passengers', flight crew members', auditors', screeners' or watch list service provider (including subcontractors) covered personnel's biographic and biometric information and security threat assessment information with the Terrorist Screening Center (TSC) and the agency that nominated the individual for placement on a watch list in order to resolve any potential or suspected matches to a terrorist watch list. TSA may also share information about individuals posing or suspected of posing a threat to transportation or national security outside of DHS, including with TSC or the nominating agency, for intelligence, counterintelligence, Department of Transportation, law enforcement or other official purposes related to transportation security in accordance with the provisions of the Privacy Act. In addition, TSA may share the information it receives with Federal, state, or local law enforcement or intelligence agencies or with the airport operator or other organizations in accordance with the routine uses identified in the applicable Privacy Act system of records notices (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS). DHS/TSA 002 was last published in the Federal Register on November 8, 2005 and can be found at 70 FR 67,731-67,735 and 70 FR 67,735-67,736

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?

TSA may share the information outside DHS in accordance with several routine uses identified in the applicable Privacy Act system of records notices (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS). DHS/TSA 002 was last published in the Federal Register on November 8, 2005 and can be found at 70 FR 67,731-67,735 and 70 FR 67,735-67,736. In addition, there is an MOU between TSA and the TSC in connection with security assessments.

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

Depending on the specific situation and need, TSA may transmit this data via secure data network, facsimile, in paper format, telephonically, via password protected CD or in person. The method of transmission and security safeguards may vary according to specific circumstances. Transmission of individual information between the watch list service providers and TSA is transmitted electronically and encrypted in transit.

Biographic information collected by a large aircraft operator will be sent to the watch list service provider electronically, telephonically or by facsimile. TSA will require that all watch list service providers access the TSA web board on a daily basis to obtain the most current watch list. Watch list service providers and enrollment providers must comply with the Privacy Act of 1974, 5 U.S.C. §552a, and the Federal Information Security Management Act (FISMA), (P.L. 107-347) to ensure the privacy and security of the data collected that may be submitted to TSA. The watch list matching results would be SSI and must be safeguarded and handled in accordance with the requirements of 49 C.F.R. part 1520. The NPRM would also prohibit any unauthorized uses of the watch list matching results.

Any Federal agency receiving this information is required to handle it in accordance with the Privacy Act, the Federal Information Security Management Act (FISMA) and their applicable SORNs.

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

TSA will share this information under the applicable provisions of the SORN and the Privacy Act. Privacy risks are mitigated by the protections offered by the Privacy Act and TSA policies on disclosure of personally identifying information. . Furthermore, the results of the watch list matching would be SSI. Therefore, the handling of this information would be subject to 49 CFR Part 1520 which provides in 1520.17 grounds for civil penalties for unauthorized disclosure. The NPRM would also prohibit any unauthorized uses of the watchlist matching results. Such penalties provide mitigation of the risks of misuse by managed watchlist providers and carriers.

Section 6.0 Notice

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

Consistent with 5 U.S.C. 552a(e)(3), TSA will provide a Privacy Act Statement to flight crew members, watch list service providers covered personnel, auditors, and screeners regarding the information collected. (See Appendix A for statement.) The Privacy Act Statement will describe the authority for the collection of the information, the purpose for the collection of information, whether provision of the information is voluntary, and any consequences of failing to provide the requested information.

Through the notice of proposed rulemaking, TSA is seeking comments on, and will evaluate, methods for providing a Privacy Act Statement to individual passengers. For example, a Privacy Act Statement can be provided to those passengers seeking to be placed on the Master Passenger List, and there may be ways to for aircraft operators to provide a Privacy Act statement to other passengers. The LASP population, however, is unique in that many passengers are fractional owners of covered aircraft, family members or close associates of aircraft operators or have reservations placed on their behalf such that individual notice is exceedingly difficult or impractical.

In addition, this collection is covered by the Privacy Act system of records notices (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS). DHS/TSA 002 was last published in the Federal Register on November 8, 2005 and can be found at 70 FR 67,731-67,735 and 70 FR 67,735-67,736.

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

Yes. Flight crew members, watch list service providers covered personnel, auditors, and screeners may decline to provide the information. However, without a Final Determination of no threat, the individual will not be allowed to be employed as a flight crew member, watch list service provider covered personnel, or applicable screener, and an auditor will not be authorized to perform the required TSA audits.

A passenger may decline to provide the requested information. However, individuals will be denied boarding if they decline to provide their full name. Passengers who do not provide date of birth and/or gender may be denied boarding if the watch list service provider or TSA is unable to distinguish the individual from a person on the No Fly List based on the information provided.

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.

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.

Flight crew members, watch list service providers covered personnel, auditors, and screeners are provided with notice through the application process prior to disclosing any information to TSA. During development of the Final Rule, TSA will evaluate the desirability and feasibility of providing a Privacy Act statement to individual passengers.

Section 7.0 Access, Redress and Correction

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

Individuals can seek access to their records by submitting a request under the Privacy Act to:

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 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). 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?

Passengers who have been denied boarding because their name was a match with a name on the Watch List may request redress through the Department of Homeland Security (DHS) Traveler Redress Inquiry Program (TRIP) by logging onto the DHS TRIP website www.dhs.gov/trip and following the online instructions. Additionally, the passengers may resubmit the Traveler Inquiry Form with updated information.

Flight crew members, auditors, watch list service provider covered personnel, and applicable screeners (hereinafter applicants) who believe that they have been wrongly identified as posing a security threat and believe they meet the standards for the security threat assessment have the opportunity to appeal an Initial Determination of Threat Assessment. This appeal must be submitted within 60 days after the date of service of the Initial Determination of Threat Assessment or 60 days from TSA's response to the applicant's request for materials pertaining to the determination.

An applicant may appeal an Initial Determination of Threat Assessment by: 1) serving TSA with a written answer to the Initial Determination of Threat Assessment that includes relevant agency or court

documents to verify the applicant's identity and correct errors in his or her records; or 2) requesting a copy of the documents on which TSA based the Initial Determination. However, no documents that are classified or otherwise protected by law can 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 Initial Determination of Threat Assessment, the materials upon which the decision was based, the applicant's appeal materials and any other relevant information or material available to TSA. An appeal of an Initial Determination of Threat Assessment based on a criminal offense, immigration status, mental capacity, or checks of appropriate terrorists watch lists and related data bases is reviewed and decided by the Assistant Secretary. Upon review of the appeal, the Assistant Secretary may overturn the initial determination and serve a Withdrawal of the Initial Determination on the applicant. Conversely, if the Assistant Secretary upholds an Initial Determination of Threat, TSA will issue a Final Determination of Threat Assessment to the applicant. For purposes of judicial review, the Final Determination constitutes a final TSA order.

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

This PIA provides individuals with information on how to correct their information. In addition, contact information is posted on the web site for candidates along with procedure to follow for correcting erroneous information.

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

Redress is provided.

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

TSA has incorporated processes for allowing individuals to access and correct their own records. In those cases where they may not correct the information, they may contact the LASP program management via telephone, e-mail, or the LASP web site and request correction of the data. In addition, individuals may request access to their application records in accordance with the Privacy Act and the DHS Privacy Act regulation.

Section 8.0 Technical Access and Security

This PIA is being conducted in connection with the NPRM. No data will be received by TSA until after a Final Rule has been published and the comment period closed. An amended PIA will be issued at that time. As such, all of the system answers below reflect the state of the system that TSA expects to implement.

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

Limited system access is provided for respective users. Access level is determined by LASP Program Management, specifically program manager, of either the TSA Office of Transportation Sector Network Management or the TSA Office of Security Operations. The system is secured against unauthorized use through the use of a layered, defense-in-depth security approach involving procedural and information security safeguards.

All TSA and DHS employees and assigned contractor staff receive appropriate significant security responsibility (SSR) training and have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on TSA security policies and procedures.

All government and contractor personnel are vetted and there are established procedures for approved access to the facility where IT systems are housed, issued picture badges with integrated proximity devices imbedded, and given specific access only to areas necessary to perform their job function.

8.2 Will Department contractors have access to the system?

Yes. Contractors have access in order to perform their assigned roles in the operations and maintenance of the LASP system.

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

All TSA and DHS employees and assigned contractor staff receive DHS-mandatory privacy training on the use and disclosure of personal data. Training status is monitored monthly by the Privacy Officer.

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

No. This PIA is being conducted in connection with the NPRM. No data will be received by TSA until after a Final Rule has been published and the comment period closed. An amended PIA will be issued at that time. This system will not become operational until after C&A has been completed.

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

The system is continuously monitored to audit compliance with policy. Weekly 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.

All logs (including file system audit) are reviewed on a regular basis and are being backed up daily as part of regular backup process.

Employees and authorized contractors are given the most restricted access necessary to perform their duties. Only authorized personnel have access to edit the data, while most employees have "read only" capability.

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 in the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, integrity, and availability (CIA) 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 identify unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts. All data collected is archived by secure electronic media.

Section 9.0 Technology

9.1 What type of project is the program or system?

This system will be an operational program following publication of a Final Rule.

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

No project development lifecycle was used.

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

The LASP program does not employ technology raising privacy concerns.

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A

Privacy Act Statement

Authority: The authority for collecting this information is 49 U.S.C. 114, "Transportation Security Administration" and 49 U.S.C. 44921 "Large Aircraft Security Program."

Purpose: This information is needed to verify and assess your qualification for participation in the LASP program, to include a security threat assessment with a criminal history records check. Furnishing this information, including your Social Security Number, is strictly voluntary; however, failure to furnish the requested information may delay or prevent the completion of your security threat assessment without which you may not participate in the LASP program.

Routine Uses: routine uses of this information include disclosures to the United States Department of Transportation and the Federal Aviation Administration when relevant or necessary to the issuance, maintenance, or renewal of a license, certificate, contract, grant, or other benefit; to your employing air carrier or airport to the extent relevant and necessary for the maintenance of a secured-area access credential; to the FBI to retrieve your criminal history record; to TSA contractors or other agents who assist in the maintenance and operation of this system; and appropriate governmental agencies for law enforcement, security or regulatory purposes, or in the interests of national security.