Privacy Impact Assessment
for the

e-Law Enforcement Officer Logbook Program

August 31, 2009

<u>Contact Point</u>
Ted Bradford
Office of Law Enforcement
Federal Air Marshal Service
Liaison Division
Edward.Bradford@dhs.gov

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

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Transportation Security Administration (TSA) is developing the ***e***-Logbook program as an electronic means of logging and confirming the identity of Law Enforcement Officers with a need to Fly Armed (hereinafter LEOFA). LEOFAs must satisfy the requirements set forth in 49 CFR § 1544.219, carriage of accessible weapons, prior to being admitted into an airport's sterile area or on-board a commercial aircraft. The purpose of this Privacy Impact Assessment (PIA) is to document in detail how the program collects, uses, and maintains data.

Overview

TSA is implementing the ***e***-Logbook program in order to comply with 49 U.S.C. § 44903 (as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53). 49 U.S.C. § 44903 requires TSA to establish a system to verify the identity of law enforcement officers (LEOs) with a need to fly armed in the performance of their official duties. Because this program entails a new electronic method for collecting personally identifiable information by TSA in an identifiable form, the E-Government Act of 2002 and the Homeland Security Act of 2002 require that the TSA conduct a PIA.

The ***e***-Logbook improves upon the old, paper-based LEOFA logbook in four ways. First, the ***e***-Logbook program permits TSA to improve its ability to confirm the identity and authority of the LEOFA. Second, electronically collecting flight information[1] (if applicable) from LEOFAs ensures that in the event of a security incident, TSA maintains the ability to access information on LEOFAs who may be able to respond to the incident, and to alert other responders that a LEOFA may be present. Third, collecting a LEOFA's information electronically and in real-time provides greater assurance of the accuracy of the information because LEOFAs update their contact and flight information for every flight for which they have a need to fly armed. Finally, the ***e***-Logbook electronically reflects when a LEO's issuing agency revokes or suspends his or her privileges, which ensures that LEOs who are not authorized to fly armed are not allowed to carry weapons into the sterile areas of airports.

The ***e***-Logbook entry and verification procedures vary depending on whether the LEOFA is a non-federal, state or local law enforcement officer, or a federal law enforcement officer.

Non-Federal LEOFA. Unless otherwise authorized by TSA, when a non-federal LEO has a need to fly armed, the LEO's issuing agency is responsible for submitting a National Telecommunication System (Nlets)[2] message to TSA for each day of travel. The Nlets message will include the LEO's name, agency name, phone number and address, badge or credential number, flight information (if applicable), LEO's current phone number, the name of the person being escorted (if applicable), and whether the LEO

[1] In certain instances, LEOs may have a need to enter the sterile area of an airport without an assignment to fly armed. These individuals may be involved in investigations or assigned to address criminal activity within the sterile area or awaiting an arriving flight.

[2] Nlets is a system that links together every state, local, and federal law enforcement, justice and public safety agency for the purpose of exchanging critical information.

has completed the requisite training. Effective July 15, 2009, the issuing agency for all non-federal LEOs, except security details for State and territorial governors, must submit an Nlets message to TSA. This LEOFA subset will follow federal LEOFA procedures. When TSA receives the Nlets message, TSA then provides a response message containing a unique alphanumeric identifier for the non-federal LEOFA to enter into the ***e***-Logbook for verification purposes at the airport. On the day of the non-federal LEOFA's travel, the non-federal LEOFA displays his or her ID to the Transportation Security Officer (TSO), Lead Transportation Security Officer (LTSO), or designated airport police officer, and enters the Nlets alphanumeric identifier into the ***e***-Logbook dedicated computer. Once the Nlets identifier is entered, the ***e***-Logbook screen auto-populates with the non-federal LEOFA's name, agency, badge or credential number, LEO's current phone number and flight information (if applicable), the name of the person being escorted (if applicable), and training information. Non-federal LEOs are required to have a new Nlets identifier for each day of travel. TSA will ask the non-federal LEO if the information provided is accurate to facilitate verification and/or update the information prior to final submittal to TSA for critical incident situational awareness. Additionally, the ***e***-Logbook electronically reflects when a LEO's issuing agency revokes or suspends his or her privileges. The TSO, LTSO, or designated airport police officer reviews the LEOFAs' badges and or credentials visually and verifies the information against the data contained on the ***e***-Logbook.

Federal LEOFA. A federal LEO who has a need to fly armed displays his or her credentials and one other form of identification, such as a driver's license or passport, to the TSOs, LTSOs, or designated airport police officers. Upon identity verification, the federal LEO manually enters into the ***e***-Logbook dedicated computer his or her name, agency name and address, badge or credential number, LEO's current phone number, flight information (if applicable), name of the person being escorted (if applicable) and whether he or she has completed the requisite training. On subsequent airport visits, after the federal LEO's identity has been verified, he or she enters his or her agency name and credential number into the ***e***-Logbook dedicated computer. TSA uses this information to associate the individual with the data contained in the database and auto-populate the static fields. The federal LEOFA will be required to update information that may change, such as current cell phone number, flight information (if applicable), and when applicable, the name of the person being escorted. The federal LEOFA is not required to have a new identifier of travel. The federal regulation that governs carriage of accessible weapons does not require federal law enforcement officers to provide a letter of authority. Therefore, Nlets messages are not required for federal law enforcement officers. The federal LEO will be asked if the information provided is accurate to facilitate verification and/or update the information prior to final submittal to TSA. Additionally, the ***e***-Logbook electronically reflects when a LEO's issuing agency revokes or suspends his or her privileges. In the future, TSA plans to develop a non-static agency-specific 8-digit code that federal LEOFA must possess in order to access the sterile area of an airport with a weapon. This code provides TSA with a method to verify a LEOFA authority to fly armed. To coordinate these efforts within the federal law enforcement community, TSA will collect a variety of agency-specific and a limited amount of point-of-contact information (name, phone number, and e-mail address) from agency program managers to facilitate code management.

TSA attaches the data obtained during the ***e***-Logbook process to specific flight records in the event of a security incident that might require retrieval of the information. If retrieved in response to a security incident, TSA will only share this information with those individuals who have a need to know the information in performance of their official duties.

TSA's Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) manages the ***e***-Logbook and LEOFA program on behalf of TSA by providing training support and materials to LEOFA and serving as the agency liaison with federal, state, and local law enforcement organizations to ensure adherence to TSA established procedures.

In the future, certain Federal LEOFAs will be issued credentials allowing for biometric confirmation of their identity.[3] Either TSA or the employing agency will issue credentials to the LEOFA's. The credential will contain a photograph of the individual and an internal application (applet) with encrypted data. No other identifying information will reside on the credential. As of the date of this PIA, no particular procedures or biometric identifier(s) have been determined. Once biometric procedures and verifiers are developed, TSA will update this PIA to reflect these changes.

Section 1.0 Characterization of the Information

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

TSA will collect the following information[4] from LEOs desiring to fly armed:

- Date/time of ***e***-Logbook entry;
- LEO's full name;
- Agency name, phone number, and address;
- Type of agency (federal, state, local, or Federal Flight Deck Officer (FFDO)[5]);
- LEO's badge and/or credential number;
- Current cell-phone number;
- Flight information (if applicable);
- Name of person being escorted (if applicable);
- Nlets identifier; and

[3] In accordance with 49 U.S.C. § 44903, TSA is working to establish the use of biometric identification cards to identify federal LEOFAs. This technology is not yet operational, but is expected to become operational in the future.

[4] Once TSA has implemented biometric verifying technologies, TSA will collect the LEO's unique fingerprint template as a biometric identifier.

[5] FFDOs are considered Federal law enforcement officers only for the limited purposes of carrying firearms and using force, including lethal force, to defend the flight deck of an aircraft from air piracy or criminal violence. FFDOs must undergo specific training are issued credentials and badges to appropriately identify themselves to law enforcement and security personnel, as required in the furtherance of their mission.

- Certification that the individual has completed LEOFA training as required by 49 CFR § 1544.219: Carriage of accessible weapons.

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

TSA will collect the full name, credential number, one other form of identification, such as a driver's license or passport, flight information (if applicable), and current cell phone number directly from all federal LEOFAs at the time the LEO seeks to enter an airport's sterile area. For non-federal LEOFA, TSA will receive the LEO's Nlets message with the above information prior to arrival at the airport.

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

The ***e***-Logbook ensures that TSA can better identify and verify LEOs with a need to fly armed. TSA also collects information from LEOFAs in order to ensure that in the event of a security incident, TSA is able to access accurate real-time information regarding the number and location of LEOFAs worldwide. Knowing which flights carry armed LEOs will assist TSA leadership in advising national command authorities on whether there are armed law enforcement officers aboard a particular commercial flight on which hostile activities may be suspected. Collecting this information electronically and in real-time provides a greater assurance of the accuracy of the information. Also, the ***e***-Logbook enables TSA to know when an issuing or sponsoring agency has revoked or suspended LEOFA privileges.[6]

1.4 How is the information collected?

Non Federal: For all non-federal LEOs, the issuing agency is responsible for submitting an Nlets message to TSA containing the LEOFA's name, flight information (if applicable), current cell phone number, and whether the individual has completed the requisite training. A new Nlets identifier is required for each day of travel.

Federal: All federal LEOs flying armed will provide TSOs, LTSOs, or designated airport police officers their travel information and supporting documentation for manual data entry into the ***e***-Logbook. This information will populate a database maintained by TSA and will include information such as the LEOFAs name, his/her agency's name and address, badge or credential number, contact and flight information, and whether the individual has completed LEOFA training as required by 49 CFR § 1544.219. On subsequent airport visits, federal LEOFAs will enter the designated LEO lane and proceed to enter their agency's name and credential number into the ***e***-Logbook dedicated computer. This information will be used to match the data contained in the database and auto-populate the static fields. The LEOFA will be required to update information that may change, such as the cell phone number in his or her possession, flight information (if applicable), and the name of the person being escorted (if applicable). The LEOFA will have an opportunity to verify the information prior to final submittal.

[6] Once the biometric identification procedures are operational, if a federal LEOFAs privileges are revoked, the issuing agency will physically collect revoked or suspended biometric access credentials, eliminating the possibility of unauthorized individuals gaining access to the sterile area.

In instances when a federal or non-federal LEO's privileges have been revoked or suspended, the LEO's issuing agency will notify TSA by using a 24-hour phone line to call the TSA and place the LEO into a "denial of access" database. In the event that the denied LEO attempted to enter the sterile area with a weapon, the ***e***-Logbook will reflect that the LEO's access is denied.

1.5 How will the information be checked for accuracy?

The information will be checked for accuracy by the LEO when he or she enters the information into the dedicated computer. In addition, the information will be checked by a TSO, LTSO, or designated airport police officer, who will ensure that the information entered corresponds with information on the required documents, by coordinating with the LEO's agency. Biometric verifiers will further enhance accuracy as they are introduced into the LEOFA identity verification system.

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

Under 49 USC § 44903, as amended by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, P.L. 110-53, DHS, through TSA, is required to establish a national registered armed law enforcement program, using biometric technology, for law enforcement officers needing to fly armed when traveling by commercial aircraft.

The regulatory requirements for a LEO to fly armed are set forth in 49 CFR § 1544.219: Carriage of accessible weapons.

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

The privacy risks associated with this collection are the possibility of mishandling the LEOFA's information or loss of control of the device, which, in some instances could jeopardize the LEOFA's anonymity. These privacy risks are mitigated by collecting information directly from the LEOFA and limiting the information collected to those data elements that are required to identify the LEOFA and validate that he or she has an operational need to fly armed. Additionally, each display screen will have privacy filters that prevent nearby travelers from viewing entered data. Similarly, no storage capability exists on the *e*-Logbook used at the airport to collect and/or verify a LEO's authorization to fly armed. After the LEOFA enters the information into the database, there is no capability for subsequent users to access previously submitted data.

These risks also are mitigated by strict access requirements and by using a secure TSA network for data entry and transfer of information only to individuals who have a need to know the information in the performance of their official duties.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

Information entered into the ***e***-Logbook will be used to verify a LEO's identity and need to fly armed and to authorize LEOFA access to the sterile area. The information will be electronically forwarded to TSA for critical incident situational awareness. Information gathered through the ***e***-Logbook may also be provided to the TSA Federal Security Director (FSD) to facilitate airport and/or local law enforcement incident response options.

This system will also provide an opportunity for issuing or sponsoring agencies to provide notification that it has revoked or suspended LEOFA privileges. This process is discussed in Section 1.4 above.

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

The system does not use any tools to analyze the data, and TSA will not generate any regularly recurring reports from the data. The system, however, will be used to help identify and prevent LEOs from flying armed when not authorized and will be used to help TSA identify trends in LEO flying patterns.

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

The system does not use commercial or publicly available data.

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.

The privacy risks associated with these uses of information involve insecure data transmission and inappropriate access. To mitigate the data security risk, the information entered into the ***e***-Logbook will be electronically forwarded to TSA via a secure encrypted network. To mitigate the opportunity for inappropriate access, upon receipt of this information, TSA will share it only with those individuals who have a need to know the information in performance of their official duties. In addition, audits of the system are conducted periodically to ensure proper use of the system.

Section 3.0 Retention

3.1 What information is retained?

The following information will be retained: Date/time; LEO's full name; agency name and address; type of agency (e.g., Federal, state, local, tribal, territorial, or air carrier FFDOs); LEO's badge and/or credential number; current cellular telephone number; name of person being escorted (if applicable); Nlets identifier, flight information (if applicable); and whether the individual has completed LEOFA training.

3.2 How long is information retained?

TSA proposes to retain the information for a maximum of 20 years to provide Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) adequate information required to analyze trends in LEOFA over a substantial timeframe. This information will allow TSA to determine appropriate resource levels and flight assignments.

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

No. The TSA Records Management Officer is currently reviewing the retention schedule, and will in turn submit the schedule request to NARA for approval. All records will be retained until the schedule is approved.

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

The privacy risk associated with the length of time that *e*-Logbook data is retained is that the information may become vulnerable to unauthorized use or disclosure. To mitigate this risk, TSA will only retain minimal contact information, flight information related to a specific flight, and PII associated with credentials that present minimal risks to the individual should they become available to someone without a need to know the information. In addition, strict internal controls and auditing requirements are in place to guard against unauthorized use or disclosure. The risks are further mitigated by not storing or maintaining the information on technology devices used at the airport and by using a secure TSA network for electronic data transmission.

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?

The information may be shared with DHS employees and contractors who have a need for the information in the performance of their duties. It is expected that information typically will be shared with TSA employees or contractors in the following TSA offices: Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS), Office of Chief Counsel, Office of Transportation Threat Assessment and Credentialing (TTAC), Office of Security Operations, Transportation Sector Network Management Office (TSNM), Office of Inspection, Office of Intelligence and all those agency components whose legitimate law enforcement or governmental terrorism-related missions require access to the information. While this information is not routinely shared outside of TSA, TSA may need to share information within

DHS, specifically with U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE).

In order to respond to complaints from individuals, the information may also be shared with the following TSA offices: Office of Privacy Policy and Compliance, the Ombudsman, or the Office of Civil Rights and Civil Liberties. To respond to congressional inquiries, the information may be shared with the Office of Chief Counsel and the Office of Legislative Affairs. Where access to sensitive information, such as personal information, is determined to be necessary, access will be based on a need to know. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

4.2 How is the information transmitted or disclosed?

TSA will transmit ***e***-Logbook information within DHS via a secure or encrypted data network, in person, in paper format, on a password-protected CD, or via a secure facsimile or telephone only to those who have a need for the information in the performance of their official duties. The method of transmission may vary according to specific circumstances and the urgency of the need of the information in accordance with OMB guidance regarding the transmission and storage of personal information.

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.

The privacy risk associated with sharing this information is the opportunity for improper dissemination of PII to individuals who do not have authority to receive or access it. To mitigate this risk, TSA will share this information only with DHS employees and contractors who have a need to know the information to perform their official duties in accordance with the Privacy Act. Employees authorized to access the data receive appropriate privacy and security training and have necessary background investigations and security clearances for access to sensitive or classified information. Privacy protections include strict access controls, including security credentials, passwords, real-time auditing that tracks access to electronic information, and mandated training for all employees and contractors.

Section 5.0 External Sharing and Disclosure

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

TSA may share the information discussed in Section 1.1 with the relevant Chief of Police or airport law enforcement operations center, and other Federal, state, local, or tribal law enforcement or intelligence agencies. Information is shared in accordance with the Privacy Act and the routine uses identified in the Transportation Security Enforcement Record System (TSERS) System of Records Notice (SORN) DHS/TSA-001 (December 10, 2004, 69 FR 71828-71830).

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. The information is shared in accordance with Privacy Act system of records notice (SORN) DHS/TSA 001, Transportation Security Enforcement Record System (TSERS). DHS/TSA 001 was last published in the Federal Register on December 10, 2004, and can be found at 69 FR 71828-71830.

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 disclosed via a secure data network, password-protected CD, paper files, facsimile, or telephone.

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

The privacy risk associated with sharing this information with external stakeholders is the opportunity for dissemination to individuals who do not have a need to know the information in the performance of official duties. TSA will limit sharing of this information under the applicable provisions of the SORN and the Privacy Act. By limiting the amount of information collected, and the sharing of this information with those who have a need to know, TSA is mitigating attendant privacy risks. These risks are further mitigated by allowing the local FSDs to use discretion, based on their experience, to carefully determine which external stakeholders have a need to know and should receive the information.

Section 6.0 Notice

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

Individual LEOs seeking to fly armed receive a Privacy Act statement upon logging into the ***e***-Logbook. See Appendix A of this PIA.

The publication of this PIA and of the SORN for DHS/TSA 001, Transportation Security Enforcement Records System (TSERS), also serve to provide the public notice of this collection, use and maintenance of this information.

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

Yes. Disclosure of PII is voluntary. However, pursuant to statute and TSA regulations, LEOFAs will not be able to enter the sterile area with a weapon unless they have submitted the information. Individuals escorted by LEOFAs do not have the opportunity or right to decline to provide their information.

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. All uses of the information obtained by TSA will be consistent with the Privacy Act and the applicable SORN.

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.

LEOs who seek to fly armed are aware that they must provide PII in order to verify identity and to receive authorization to carry weapons into the sterile areas of airports. TSA provides notice to LEOs who seek to fly armed via a Privacy Act Statement displayed on the *e*-Logbook screen. Notice is also provided to the LEOFA via this PIA and the SORN listed in Section 5.2 above.

Section 7.0 Access, Redress and Correction

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

Individuals may gain access to and correct the personal information provided during the ***e-***Logbook process 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

Freedom of Information Act/Privacy Act (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 include 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) for further instructions.

Individuals who are denied permission to fly armed by their agency must seek redress directly from the parent agency.

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

During the enrollment process, it is ultimately the responsibility of the individual LEO, whether a Federal or non-Federal LEO, and his/her agency to ensure the accuracy of the information provided.

All LEOs will also have the opportunity to correct inaccurate or erroneous information. The individual LEO will be asked if the information provided is accurate to facilitate verification and/or update of the information prior to final submission to TSA for critical incident situational awareness. In those instances where errors are detected, the LEO has an opportunity to correct the submitted information.

Individuals seeking to correct inaccurate information may also write to the TSA FOIA office, using the contact information provided:

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) for further instructions.

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

This PIA serves as notification to individuals that they may seek correction of erroneous or inaccurate information. The TSO, LTSO, or designated airport police officer provides additional notification and an opportunity to update or correct their information by asking the LEO if the information is correct prior to final submittal to TSA.

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

Appropriate 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.

The privacy risk associated with redress is the collection of inaccurate information. This risk is mitigated by the individual's ability to correct his or her information via the same process by which the information submitted. In addition, individuals may correct their information at any time during which TSA possesses their information.

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?

The TSA Command Duty Officer (CDO) or the Assistant Command Duty Officer (ACDO) will have immediate access to LEOFA information. This information may then be disseminated to critical incident managers as the CDO/ACDO and the TSA Assistant Special Agent in Charge deem appropriate.

With regard to airport FSDs, should the CDO/ACDO determine that providing LEO flying armed data to airport specific FSDs is appropriate, this information would be sent by way of the TSA intranet, which requires user identification and password before access is granted.

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 system 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 security officers. All contractors are subjected to requirements for suitability and a background investigation.

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

All TSA employees and contractors are required to complete on-line TSA Privacy Training, which includes instructions on handling PII in accordance with the Privacy Act. Compliance with this requirement is audited monthly by the TSA Privacy Officer.

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

No. This PIA is being conducted in conjunction with the acquisition process and to assist the program with building privacy considerations into the overall development of the system. Certification and Accreditation will be completed before the system becomes operational. Additionally, these devices will be locked down according to DHS and TSA Security Requirements and will go through normal TSA

Certification and Accreditation (C&A) and auditing processes.

TSA's operational integration team will perform operational testing and evaluation of the device to determine its efficacy and will develop a formal evaluation of the technology and supporting processes.

A PIA update will be submitted upon completion of the Certification and Accreditation process.

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. All IT systems are audited annually for IT security policy compliance and technical vulnerability by the TSA IT Security Office.

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?

Identifiable privacy risks of the ***e***-Logbook Program include unauthorized access to data, accidental disclosure of PII, and improper modification of data. These risks have been mitigated by the implementation of strict access controls, including security credentials, passwords, real-time auditing that tracks access to electronic information, and mandated training for all employees and contractors. The program is designed to limit the use of PII only to approved uses by authorized parties and protect against inadvertent and unnecessary disclosure. Only individuals with proper authorization, credentials, training, and a need to know will be granted access to the system in performance of their duties as approved by the Information System Security Officer (ISSO). Access and audit log reviews, along with other security precautions are in place to further secure system and data access.

Section 9.0 Technology

9.1 What type of project is the program or system?

The ***e***-Logbook effort is considered by TSA to be an information technology program and is expected to go through several iterations over the next several months/years. The collection and use of information will remain consistent with this PIA, however, and the PIA will be updated as necessary.

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

Project development is currently in the program initiation phase and no lifecycle estimates have been established.

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

In the future, the ***e***-Logbook program will require a biometric identifier for federal LEOs as mandated by Congress. The biometric will be used for a one-to-one match. The use of biometric identifying technology and ID cards will greatly enhance identity verification. If TSA implements biometric operations, this PIA will be updated accordingly.

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Privacy Act Statement

Authority: 49 U.S.C. § 44903 and 49 CFR § 1544.219 authorize collection of this information.

Purpose: TSA will use this information to confirm the identity of law enforcement officers with a need to fly armed.

Routine Uses: TSA may share this information with the relevant Chief of Police or airport law enforcement operations center, and other Federal, state, local, or tribal law enforcement or intelligence agencies. The information is shared in accordance with the Privacy Act system of records notice (SORN) DHS/TSA 001, Transportation Security Enforcement Record System (TSERS).

Disclosure: Furnishing this information is voluntary. However, failure to furnish the requested information may preclude you from being given permission to fly armed.