Privacy Impact Assessment
for the

Airmen Certificate Vetting Program

October 22, 2007

Contact Point
Chang Ellison
Director, Airmen Certificate Vetting
Transportation Security Administration
Chang.Ellison@dhs.gov

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

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

Abstract

The Department of Homeland Security (DHS) Transportation Security Administration (TSA) is implementing a process to conduct security threat assessments on all Federal Aviation Administration (FAA) Airmen Certificate applicants and holders to ensure that the individual does not pose or is not suspected of posing a threat to transportation or national security. As described below, FAA Airmen Certificate holders include pilots, air crews, and others required to hold a certificate pursuant to FAA regulations. Because this program entails a new collection of information by TSA about members of the public in an identifiable form, the E-Government Act of 2002 and the Homeland Security Act of 2002 require that the TSA issue a Privacy Impact Assessment (PIA). The data collected and maintained for this program and the details and uses of this information are outlined in this PIA.

Introduction

Under the Aviation Transportation Security Act (ATSA), 49 U.S.C. § 114 TSA is responsible for assessing information in order to identify individuals who pose a threat to transportation security and to coordinate countermeasures with other Federal agencies, including the Federal Aviation Administration (FAA). 49 USC §114(f)(1)-(2). Pursuant to 49 U.S.C. § 114(f)(13), Congress specifically required TSA to work with the FAA to take actions that may effect aviation safety or air carrier operations. In addition, 49 U.S.C. § 44903(j)(2)(D)(i) requires TSA, in coordination with the FAA, to ensure that individuals are screened against all appropriate records in the consolidated and integrated Federal terrorist watch list.

As part of this effort, the FAA has screened individuals on the FAA Airmen Registry[1] against the Federal "No Fly" and "Selectee" watch lists, and notified TSA when it discovers that selected applicants or holders of Airmen Certificates appear on those watch lists. Through a Memorandum of Agreement (MOA) between TSA and FAA, TSA will conduct security threat assessments on individuals who are on FAA's Airmen Registry. Under this process, TSA will obtain biographic information on all Airmen Certificate holders and applicants from FAA. The information is used to conduct a security threat assessment by comparing the biographic information against terrorist-related, immigration, and criminal databases that TSA maintains or uses in order to determine whether the individual poses or is suspected of posing a risk to transportation or national security.

[1] FAA's Airmen Registry includes biographical information pertaining to, among others, both active and inactive Airmen Certificate applicants and holders who are subject to the regulations set forth in 14 C.F.R. Parts 61, 63, and 65. These regulations cover the following groups:

- Pilots, flight instructors and ground instructors
- Flight crewmembers other than pilots: flight engineers and flight navigators
- Airmen other than flight crewmembers: air-traffic control-tower operators, aircraft dispatchers, mechanics, repairmen, flight attendants, and parachute riggers.

The FAA will continue to manage the Airmen Registry, and will make information concerning the Airmen Certificate holders and applicants available to TSA to conduct security threat assessments. If TSA determines that an Airmen Certificate holder or applicant poses or is suspected of posing a threat to transportation or national security, TSA will send the individual an Initial Determination of Threat Assessment (IDTA). The IDTA will advise the individual of their opportunity to respond to the adverse determination in accordance with the requirements set forth in 49 U.S.C. § 46111 as described more fully in Section 7.2 below.

An individual poses a security threat when the individual is suspected of posing, or is known to pose —

(1) A threat to transportation or national security;

(2) A threat of air piracy or terrorism;

(3) A threat to airline or passenger security; or

(4) A threat to civil aviation security.

Based on the results of the security threat assessment and any response to an adverse determination, TSA may recommend that the FAA immediately suspend the Airmen Certificate and, ultimately, revoke the Airmen Certificate, or deny the Airmen Certificate application. Airmen Certificates do not expire and all Airmen Certificate holders will be perpetually vetted to ensure that the individual does not pose or is not suspected of posing a threat to transportation or national security.

Section 1.0 Information collected and maintained

1.1 What information is to be collected?

The FAA currently collects Personally Identifiable Information (PII) directly from FAA Airmen Certificate applicants and holders. The FAA will provide TSA with the following information: full name, date of birth, place of birth, country of citizenship, gender, height, weight, hair color, eye color, current address, telephone number, and alien registration number, if applicable.

In addition, the FAA will also provide TSA status information of an airman. This information, which would typically be maintained as a historical record of certification, includes, but is not limited to: unique Airmen identification number, certificate type, and certificate class(es). FAA will also provide TSA with any Social Security numbers (SSNs) that applicants submit to the FAA.[2]

1.2 From whom is information collected?

The FAA collects information from Airmen Certificate holders and applicants, via the Airmen Certificate Branch, P.O. Box 25082, Oklahoma City, Oklahoma 73125

[2] It is voluntary for Airmen Certificate applicants to provide their personal information. SSN is specifically identified as a voluntary submission to the FAA..

1.3 Why is the information being collected?

TSA will use this information to perform a security threat assessment on Airmen Certificate holders or applicants to ensure they do not pose or are not suspected of posing a threat to transportation or national security.

The SSN is collected as an additional item to help identify persons who may have the same name or other particulars as individuals on the watch lists or other lists.

1.4 How is the information collected?

The FAA collects PII from Airmen Certificate applicants on paper application forms submitted via mail or facsimile. The FAA processes the applications and maintains this information. TSA will access the required PII electronically through a secure web portal in order to perform a security threat assessment.

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

Pursuant to 49 U.S.C. § 114, TSA has authority to, among other things, carry out the statutory provisions set forth in 49 U.S.C. Chapter 449, relating to civil aviation security, and related research and development activities. 49 U.S.C. § 114(d)(1). Among its security-related responsibilities, TSA has authority to "assess threats to transportation," and to "establish procedures for notifying the Administrator of the Federal Aviation Administration, appropriate State and local law enforcement officials, and airport or airline security officers of the identity of individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety." 49 U.S.C. §§ 114(f)(1)-(2). In accordance with the requirements set forth in 49 U.S.C. § 114(f)(13), TSA works with the FAA on actions that may affect aviation safety or air carrier operations. 49 U.S.C. § 44903(j)(2)(D)(i) specifically requires TSA, in coordination with the FAA, to ensure that individuals are screened against all appropriate records in the consolidated and integrated Federal terrorist watch lists before being certificated by the FAA.

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

The incorrect identification of an individual as a security threat (false positives) is one of the privacy risks associated with this collection. TSA seeks to reduce the potential for misidentification by requesting sufficient items of information in order to distinguish the individual from others that may have the same name. TSA limits the amount of personal information to determine a person's identity and conduct a security threat assessment to determine if the individual poses or is suspected of posing a threat to the transportation or national security while collecting sufficient information to reduce the risk of false positives with attendant burden on individuals.

Section 2.0 Uses of the system and the information

2.1 Describe all the uses of information.

TSA will use the information received from the FAA to conduct a security threat assessment on Airmen Certificate holders and applicants to determine whether the individual poses or is suspected of posing a threat to transportation or national security. The security threat assessment includes checking the individual's information against terrorist-related, criminal, and immigration databases that TSA maintains or uses in order to confirm that the Airmen Certificate holder or applicant does not pose or is not suspected of posing a security threat. All Airmen Certificate holders will be perpetually vetted to ensure that the individual does not pose or is not suspected of posing a threat to transportation or national security.

The SSN is collected as an additional item to help identify persons who may have the same name or other particulars as individuals on the watch lists or other lists.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The FAA will collect the biographic information directly from the Airmen Certificate applicant or Airmen Certificate holder, who must certify that the information provided is accurate. FAA will transmit that information to TSA to conduct a security threat assessment. It is presumed that the applicant is providing accurate information in order to receive the appropriate certificate.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The risk of collecting inaccurate information is minimized because applicants provide their information directly to the FAA and that information will be transmitted to TSA. The impact of collecting inaccurate information is also minimized because individuals who feel they have been wrongly identified as a security threat can seek redress through TSA allowing for an additional review of the completeness and accuracy of the information.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

TSA will retain the data it receives from FAA and information concerning the security threat assessment in accordance with record schedules approved by the National Archives and Records Administration (NARA). As airmen certificates have no expiration dates, an individual's valid certificate record, either active or non-active, will be retained unless TSA receives notification that the record is no longer valid.

TSA will destroy records one year after an individual's access 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 the individual's certificate 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 years, or seven years after TSA learns that the individual is deceased, whichever is shorter.

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

Yes.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Information collected through this program will be maintained in accordance with the NARA-approved record retention schedules in furtherance of TSA's mission to ensure the security of the Nation's transportation system. These retention periods will permit review of records for individuals who may have been cleared as a match to a watch list after more extensive review. Further, TSA will retain records on individuals identified as an actual match or otherwise determined to pose or to be suspected of posing a threat to transportation or national security in order to detect attempts to reapply for an Airmen Certificate.

Section 4.0 Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

TSA will share the information collected on Airmen Certificate holders and applicants as well as security threat assessment information with DHS employees and contractors who have a need for the information in the performance of their duties.

It is expected that information will typically be shared with TSA employees or contractors in the following TSA offices: the Office of Chief Counsel, the Office of Transportation Threat Assessment and Credentialing, and the Office of Transportation Security Redress.

In the event of a possible match to a watch list, information will be shared with the Office of Intelligence, the Office of Security Operations, and the Office of Transportation Security Network Management-International.

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 from individuals. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

While it is not expected that information will be routinely shared outside of TSA, TSA may need to share information within DHS as outlined in section 4.2, specifically with U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement.

4.2 For each organization, what information is shared and for what purpose?

TSA will routinely share this information within the Office of Transportation Threat Assessment and Credentialing in order to conduct the threat assessments. Information will also be shared with the Office of Chief Counsel in support of the IDTA process discussed in Section 7.2 below. Individuals' identifying information and positive or suspected matches to terrorist-related, immigration or criminal databases will ordinarily be shared with TSA's Office of Intelligence and Office of Security Operations. In order to respond to complaints from individuals, the information may also be shared with the Privacy Office, Ombudsman, Office of Civil Rights and Civil Liberties, and Legislative Affairs. The information may also be shared outside of TSA, within DHS (CBP/ICE), where there is a need to know the information for law enforcement, intelligence, or other official purposes. This information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. §552a.

4.3 How is the information transmitted or disclosed?

Depending on the identity of the recipient and the urgency of the request for information, TSA may transmit the personally identifying information in person, in paper format, via facsimile, electronically via password-protected attachments to electronic mail, or telephonically.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Information is shared within DHS and other governmental agencies that have a need for the information in the performance of their official duties in accordance with the Privacy Act. Privacy protections shall include strict access controls, including passwords and mandated training for all TSA employees and contractors.

Section 5.0 External sharing and disclosure

5.1 With which external organizations is the information shared?

TSA will share the information, such as results of security threat assessments, with the FAA. TSA may also share biographic information about individuals posing or suspected of posing a security threat with the Terrorist Screening Center (TSC). TSA may share additional information with other Federal, state, tribal, territorial, or local law enforcement or intelligence agencies in accordance with the official, routine uses identified in the applicable Privacy Act system of records notice (SORN), DHA/TSA 002, Transportation Security Threat Assessment System (T-STAS). This SORN was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731-67735.

5.2 What information is shared and for what purpose?

If an individual is identified as posing or suspected of posing a security threat, TSA may share that individual's information (see section 1.1) and any other information (immigration violations, crimes, wants/warrants) uncovered during the database checks conducted with the TSC as part of the security threat assessment process. Further, individual information uncovered during the security threat assessment process will be shared, as needed, with Federal, state, or local enforcement or intelligence agencies to communicate the threat assessment results and to facilitate an operational response. Security threat assessment information will be shared with the FAA in order to suspend or revoke current Airmen Certificates or deny Airmen Certificate applications for individuals who pose or are suspected of posing a threat to transportation or national security.

5.3 How is the information transmitted or disclosed?

Depending on the identity of the recipient and the urgency of the request for information, TSA may transmit the personally identifying information in person, in paper format, via facsimile, electronically via password-protected attachments to electronic mail, or telephonically.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Yes. TSA currently has an MOU in place with the TSC, which establishes procedures and requirements under which TSC will provide TSA access to terrorist identities and identifiers contained in the Terrorist Screening Database. The TSA also has an MOA with the FAA which will address the exchange of Airmen Certificate holder and applicant information as well the action required if an individual poses or is suspected of posing a threat to transportation or national security based on the results of the security threat assessment. Information may be shared in accordance with the applicable SORN, DHS/TSA 002 Transportation Security Threat Assessments, or in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

5.5 How is the shared information secured by the recipient?

Any Federal agency receiving this information is required to handle it in accordance with the Privacy Act, their applicable SORNs. In addition, Federal agencies and their contractors are subject to information security requirements of the Federal Information Security Management Act (FISMA), Title III of the E-Government Act, Pub. L. 107-347.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

TSA does not mandate any specific training, however, any Federal agencies receiving this information are required by other authorities to provide Privacy Act training to their employees and contractors.

5.7 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 and routine uses under the applicable SORN. By limiting sharing of this information to those who have an official need to know it, TSA is mitigating any attendant privacy risks. Because FAA databases already exist and FAA performs the STA function, privacy risks attendant with sharing with the FAA are not appreciably greater than existing risks.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register. If notice was not provided, why not?

FAA provides a Privacy Act statement as required by section(e)(3) of the Privacy Act (see appendix A) on the application. 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. In the event an individual is determined to be a security threat and the individual believes that the results of the screening are inaccurate, he or she will be informed by TSA on how to pursue redress from TSA. The FAA SORN (April 11, 2007, 65 FR 19527) provides notice to individuals regarding the collection of information.

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

Yes, both as part of the application process and during any redress.

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. However, if TSA determines the individual poses or is suspected of posing a security threat, all uses of such information by TSA will be consistent with the Privacy Act and the DHS/TSA 002, Transportation Security Threat Assessment System SORN identified in paragraph 5.1 above.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The information sent to TSA by FAA will be used to conduct a security threat assessment to determine whether the Airmen Certificate holder or applicant poses or is suspected of posing a threat to transportation or national security. Individuals in this population must already send the same information to the FAA and receive an FAA Privacy Act statement.

Section 7.0 Individual Access, Redress and Correction

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

Individuals may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration
Freedom of Information Act Office, TSA-20
11th Floor, East Tower
601 South 12th Street
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by facsimile at 571-227-1406 or by email at FOIA.TSA@dhs.gov. The FOIA/PA request must contain the following information: requester's full name, address, telephone number, and email address (optional). Please refer to the TSA FOIA web site (http://tsa.gov/research/foia/index). Individuals who have received an Initial Notification of Threat Assessment may also request access to all releasable materials in connection with their appeal as described below in section 7.2.

7.2 What are the procedures for correcting erroneous information?

If TSA determines that an Airmen Certificate holder or applicant poses or is suspected of posing a threat to transportation or national security, TSA will send the individual an IDTA.[3] The IDTA provides the

[3] Under 49 U.S.C. § 46111, an FAA issued certificate must be immediately suspended by the FAA upon notice

individual with the opportunity to respond to the determination in accordance with the requirements set forth in 49 U.S.C. § 46111 as described more fully below. Moreover, receipt of the IDTA provides individuals with the opportunity to respond on the basis that they have been misidentified or that the underlying information pertaining to them is erroneous, which effectively results in providing these individuals with an opportunity to seek redress.

TSA's procedures governing the appeal of an initial determination can take one of three paths depending on an individual's status as a U.S. citizen, lawful permanent resident alien or alien. Regardless of citizenship or immigration status, all Airmen Certificate holders who receive an IDTA are advised that they may challenge the IDTA, request the release of any document upon which the IDTA was made, and submit a written reply to the initial determination. Specific rights are based on citizenship or alien status.

U.S. Citizens

As set forth in 49 U.S.C. § 46111, a U.S. citizen has the right to request an unclassified summary of any classified material upon which the IDTA was made.[4] A U.S. citizen also may request that an Administrative Law Judge (ALJ) conduct a paper review of the IDTA or hold an in-person hearing regarding the determination. A U.S. citizen may appeal an adverse ALJ decision to the Transportation Security Oversight Board (TSOB). The TSOB's decision may be reviewed by an appropriate court of appeals at the request of either party. *See* 49 U.S.C. § 46111(e).[5] If the U.S. citizen does not challenge the initial notification, or challenges the determination without seeking review by an ALJ or the TSOB, the Assistant Secretary for the TSA Administrator conducts a *de novo* review of the threat assessment. The Assistant Secretary's decision constitutes a final agency action and is subject to review by a court of appeals under 49 U.S.C. § 46110(a).

Lawful Permanent Resident Aliens

A Lawful Permanent Resident (LPR) alien may request that an ALJ conduct a paper review of the initial determination or an in-person hearing. An LPR may appeal the ALJ's adverse decision to the Assistant Secretary for the TSA, who will conduct a *de novo* review of the threat assessment and ALJ's determination. The Assistant Secretary's decision constitutes a final agency action and is subject to review by a court of appeals under 49 U.S.C. § 46110(a).

Aliens

Aliens may request a paper review of the initial determination by the TSA Deputy Assistant Secretary. The Deputy Assistant Secretary's decision constitutes a final agency action and is subject to review by a court of appeals under 49 U.S.C. § 46110(a).

---

from the Under Secretary for Border and Transportation Security that the holder of the certificate poses, or is suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger security. The authority for certificate actions under section 46111 has been delegated to the Administrator of the TSA. Therefore, if TSA determines that any Airmen's Certificate should be immediately suspended when the initial notification of threat assessment is issued, TSA will make a request to the FAA for immediate suspension.

[4] TSA does not disclose any classified information, or any other information or material that is otherwise protected from disclosure by law.

[5] As noted above, the authority for certificate actions under section 46111 has been delegated to the Administrator of the TSA.

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

Individuals will receive a written IDTA that contains the procedures to be followed for responding to the initial threat assessment determination. If TSA ultimately withdraws its IDTA, affected individuals may seek amendment of underlying records that were used in making the initial determination, which are maintained by other law enforcement and intelligence agencies to correct any incorrect information.

7.4 If no redress is provided, are alternatives are available?

A redress process is provided.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction, and redress rights are not provided please explain why not.

TSA has provided a redress process that allows the individual to access and correct their records as well as respond to IDTAs. In addition, individuals may request access to or correction of their personal information pursuant to the Privacy Act.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

In order to perform their duties in managing, upgrading, and using the system, system administrators, security administrators, IT specialists, vetting operators and analysts have access to 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 contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes. DHS will hire contractors to perform many of the IT maintenance and security monitoring tasks. These contractors will have access to the system in order to perform their official duties.

8.3 Does the system use "roles" to assign privileges to users of the system?

Role-based access controls are employed to limit the access to information by different users and administrators based on their need to know.

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

A documented procedure has been established to determine whether an individual has the need to access the system directly. Once that need is verified, the system administrator grants access to users utilizing role-based controls and the policy of least privilege.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The system administrators assign roles to TSA employees or contractors for accessing the system based on their function in accordance with an established documented procedure. TSA ensures personnel accessing the system have security training commensurate with their duties and responsibilities. The system is also audited daily to identify any unauthorized use or misuse of the system.

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

TSA systems for security threat assessments maintain an auditing function of individuals who access the system. The system is audited daily by system administrators and annually by the TSA IT Security Office. An audit trail is maintained on the system to track access to the system. 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. Compliance will also be ensured through adherence to all FISMA required documentation to include National Institute of Standards and Technology (NIST) risk management methodology. Creation and maintenance of all required security documentation will ensure there is an IT security risk management program in place. Security documentation includes, but are not limited to, System Security Plan (NIST publication 800-18), Risk Assessment (NIST publication 800-30), Federal Information Processing Standard (FIPS) number 199, Data Categorization, Self-Assessment (NIST publication 800-26) and other pertinent System Development Life Cycle (SDLC) artifacts. Through continuous monitoring this program office will ensure intrusion prevention and privacy protection is foremost.

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

All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. Compliance with this training requirement is audited monthly by the TSA Privacy Officer, and failure to complete the training is reported to program management for remedial action. Additionally, all staff must hold appropriate credentials for physical access to the sites housing the security threat assessment databases and management applications. In addition, all government and contractor personnel must complete annual information technology security training as required by FISMA.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Information in TSA threat assessment and vetting systems is safeguarded in accordance with the FISMA requirements. The Certifications and Accreditations for the systems that will perform the vetting operation were last completed on September 1, 2005 and October 17, 2005.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

TSA has implemented security controls and technology features that fully incorporate protection of privacy. TSA has complied with FISMA, and mitigated privacy risks through the following methods:

- Access to the system is controlled through role-based user accounts.
- System access through user accounts is auditable.
- The system strictly controls the transmission and storage of data.
- All government and contract personnel are required to complete privacy training.
- The system is audited to ensure FISMA compliance.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The system is built from Commercial Off the Shelf (COTS) products, customized applications and Government Off the Shelf (GOTS) products. System components include COTS hardware and operating systems with GOTS applications.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Security and privacy requirements were analyzed based on NIST guidance and FIPS-199 methodology. FIPS-199 methodology categorizes a system as High, Medium, or Low, depending on the criticality to the agency. The systems that will perform the vetting completed a FIPS-199, Standards for Security Categorization of Federal Information and Information Systems analysis on August 3, 2005 and August 5, 2005.

9.3 What Design Choices Were Made to Enhance Security

In order to support privacy protections, TSA has limited its data collection to specific elements necessary for security threat assessments. TSA has developed an information technology infrastructure that will protect against inadvertent use of personally identifying information not required by the government. Access to data collected for this program will be strictly controlled; only TSA employees and contractors with proper access controls will have permission to use and view this information. Additionally, the system will include a real time audit function to track access to electronic information, and any infractions of information security rules will be dealt with appropriately. Strict incident response plans are in place. All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses.

9.4 Privacy Impact Analysis

These conscious design choices will limit access to the personal information, thereby mitigating possible privacy risks associated with this program.

Responsible Officials

Chang Ellison
Director, Airmen Certificate Vetting
Transportation Security Administration
Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A

FAA Privacy Act notice

Privacy Act

The information on the accompanying form is solicited under authority of Title 14 of the Code of Federal Regulations (14 CFR), Part 61. The purpose of this data is to be used to identify and evaluate your qualifications and eligibility for the issuance of an Airmen Certificate and/or rating. Submission of all requested data is mandatory, except for the Social Security Number (SSN) which is voluntary. Failure to provide all the required information would result in you not being issued a Certificate and/or rating. The information would become part of the Privacy Act system of records DOT/FAA 847, General Air Transportation Records on Individuals. The information collected on this form would be subject to the published routine uses of DOT/FAA 847. Those routine uses are: (a) To provide basic airmen certification and qualification information to the public upon request. (b) To disclose information to the national Transportation Safety Board (NTSB) in connection with its investigation responsibilities. (c) To provide information about airmen to Federal, state, and local law enforcement agencies when engaged in the investigation and apprehension of drug violators. (d) To provide information about enforcement actions arising out of violations of the Federal Aviation regulations to government agencies, the aviation industry, and the public upon request. (e) To disclose information to another Federal agency, or to a court or an administrative tribunal, when the Government or one of its agencies is a party to a judicial proceeding before the court or involved in administrative proceedings before the tribunal.

Submission of your Social Security Number is voluntary. Disclosure of your SSN will facilitate maintenance of your records which are maIDTAined in alphabetical order and cross-referenced with your SSN and Airmen Certificate number to provide prompt access. In the event of nondisclosure, a unique number will be assigned to your file.