Privacy Impact Assessment
for the Federal Flight Deck Officer Program

January 10, 2008

Contact Point

Jeffrey Davenjay
Special Agent in Charge, Flight Programs Division, OLE/FAMS
Transportation Security Administration
Jeffrey.Davenjay@dhs.gov

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 Federal Flight Deck Officer (FFDO) program was established by the Arming Pilots Against Terrorism Act (APATA) as Title XIV of the Homeland Security Act (Pub. L. 107-296, Nov. 25, 2003, 116 Stat. 2300), codified at 49 U.S.C. 44921. Under this program, TSA deputizes qualified volunteer pilots and flight crewmembers of passenger and cargo aircraft as law enforcement officers to defend the flight deck of aircraft against acts of criminal violence or air piracy. Participants in the program, known as Federal Flight Deck Officers (FFDOs), are trained and authorized to transport and carry a firearm and to use force, including deadly force. Through this program, TSA collects data on pilots to assess the qualification and suitability of prospective and current FFDOs through an online application, and to administer the program.

Introduction

The FFDO program is a voluntary program for which pilots are not compensated. The goal of the program is to train and arm flight crewmembers to defend the flight deck of commercial aircraft from takeover. The identity of an FFDO is strictly controlled to reduce endangerment to the individual or the air transport system. Thus, privacy is a key ingredient to the success of the program.

TSA collects information in order to evaluate an applicant's cognitive, psychological, medical, and physical skills before an applicant may enroll in training. FFDO applicants first complete an online application, and after receipt, TSA initiates the security threat assessment process, which includes a check of criminal history records and government watch lists, and a credit history check. TSA previously conducts immigration status checks on all Airman Certificate applicants and holders, which includes pilots and aircrews, per the TSA Airman Certificate Vetting Privacy Impact Assessment (PIA) posted publicly on October 22, 2007. TSA then schedules qualified applicants for a psychological evaluation, which consists of a computer-based assessment followed by an interview with a TSA-contracted psychologist. The psychologist provides a written recommendation to TSA. Qualified applicants are notified to schedule a training class date; their pertinent personal information, including name, date of birth, and contact information, is used to schedule FFDO initial and requalification training. TSA collects additional applicant health information via a questionnaire to inquire about previous or current injuries, medications, and to assess their overall ability to commence physical training. Information about an FFDO may also be used in forming a response to certain aviation security incidents.

FFDOs communicate with TSA FFDO program management primarily through an online website, otherwise known as the "dashboard." FFDOs provide incident reports concerning operations in the field, ask questions concerning clarification of operating procedures, provide updates to their personal contact information, arrange mission scheduling, and conduct myriad other communications with the TSA FFDO program through this system. In turn, FFDO program management sends messages to individual or specifically tailored groups of FFDOs through this system.

Initial program and continuation training is scheduled for FFDOs through a contractor-operated FFDO Program System. FFDOs communicate with TSA contractors via phone or email for all aspects of initial and continuation training.

Because this program entails a collection of information in identifiable form about a group of individuals, the E-Government Act of 2002 requires that TSA conduct a PIA.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

Through the dashboard, TSA collects the following information from pilots applying to become an FFDO: FAA Airman Certificate Number, name, date of birth, place of birth, Social Security number, citizenship status, home address, telephone number, eye color, hair color, airline employee number, email address, type of Airman's Certificate held, class of Airman's Medical Certificate held, employment history, military and law enforcement experience, specific health information, contact information for personal references, flight schedule, and passport number. Providing the Social Security number is voluntary, but failure to do so may delay or prevent completion of the security threat assessment. The online process requires an FFDO applicant to provide his or her Airman Certificate Number and last name to confirm identity. Once eligibility is confirmed, the crewmember will be directed to a secure web site to complete a questionnaire as the initial step in the selection process. In addition to the information listed above, the dashboard maintains FFDO flight scheduling information, psychological examination results, and health information. TSA will collect information for a psychological examination through a computer-based assessment and an interview with a TSA-contracted psychologist. Prior to training, TSA collects additional applicant health information via a questionnaire to determine suitability for training. TSA also conducts a credit history check on candidates.

Once applicants are determined eligible to participate in training, the contractor-operated FFDO Program System maintains the following information about FFDO applicants: FAA Airman Certificate Number, name, date of birth, place of birth, Social Security number, citizenship status, home address, telephone number, eye color, hair color, airline employee number, email address, type of Airman's Certificate held, class of Airman's Medical Certificate held, employment history, military and law enforcement experience, specific health information, contact information for personal references, flight schedule, passport number, and weapons qualification records. Once deputized, TSA collects the applicant's signature and photograph to issue an FFDO credential to the individual.

1.2 From whom is information collected?

TSA will collect the information directly from applicants who may be pilots, navigators, or flight engineers on passenger or cargo aircraft. TSA also collects certain information from federal investigative sources as a result of the checks performed against terrorist threat and criminal history databases. If the individual has a criminal record, a copy of that record will be collected. Otherwise, the result of the check will be collected. Additional suitability information may be obtained from employers upon their notification that the individual has applied for the FFDO Program.

1.3 Why is the information being collected?

Through the dashboard, TSA is collecting FFDO applicant Personally Identifiable Information (PII) in order to conduct a security threat assessment that includes a check of criminal history records and government watch lists to determine suitability of an applicant for the FFDO program and to conduct a credit history check. If the applicant is found suitable, TSA retains the information and uses it to contact

the applicant and manage his/her participation in the program. The applicant then undergoes a psychological examination, consisting of a computer-based assessment followed by an interview with a psychologist, to determine the applicant's suitability. The computer-based assessment occurs at contracted sites throughout the country. Applicants then meet with one of numerous psychologists contracted by TSA to conduct personal interviews using TSA-approved questions. Prior to training, TSA collects applicant health information via a questionnaire to determine suitability for training. When FFDO applicants are determined suitable for training, certain information collected through the dashboard is maintained in the contractor-operated FFDO Program System in order to schedule FFDO initial and continuation training. The information is also collected to create and issue the FFDO credential once an FFDO is deputized.

1.4 How is the information collected?

FFDO applicants submit information electronically, via a secure web site. FFDO applicants submit health information in person prior to participating in training for the program.

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

To further supplement the security measures being implemented by TSA, Congress and the President enacted APATA as Title XIV of the Homeland Security Act (Pub. L. 107-296, Nov. 25, 2003, 116 Stat. 2300), codified at 49 U.S.C. 44921. APATA requires TSA to establish a program to screen, select, train, deputize, equip, and supervise qualified volunteer pilots of passenger aircraft. APATA directed the Under Secretary of Transportation for Security to develop a "process for selection of pilots to participate in the program based on their fitness to participate in the program, including whether an additional background check should be required by section 44936(a)(1)" of Title 49 of the United States Code.[1] With the enactment of the Vision 100-Century of Aviation Reauthorization Act (Pub. L. 108-176, Dec. 12, 2003, 117 Stat. 2490, 2561), the program was expanded to include pilots of cargo aircraft, as well as flight engineers and navigators on both passenger and cargo aircraft. As a result, the Under Secretary established the information that must be collected in order to conduct a security threat assessment, credit history check, and psychological evaluation of pilots volunteering for the program, as well as to administer the program.

[1] Under Section 403(2) of the Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2315 (2002) (HSA), all functions of TSA, including those of the Secretary of Transportation and the Under Secretary of Transportation of Security related to TSA, transferred to the Secretary of Homeland Security. Pursuant to DHS Delegation Number 7060.2, the Secretary delegated to the Assistant Secretary (then referred to as the Administrator of TSA), subject to the Secretary's guidance and control, the authority vested in the Secretary with respect to TSA, including that in Section 403(2) of the HSA.

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.

TSA collects data to evaluate the suitability of pilots and flight crewmembers whom TSA trains, arms and deputizes as FFDOs to defend the flight decks of commercial aircraft against acts of criminal violence or air piracy. Privacy risks are mitigated by closely safeguarding the identity of each FFDO; the identity of each applicant, current, and former FFDO is treated as Sensitive Security Information under 49 CFR Part 1520. Privacy risks are also mitigated by limiting the amount of information collected at each stage of the process; for example, health information is collected from only those applicants who successfully complete the initial application and psychological examination processes.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

TSA uses the information to conduct security threat assessments and credit history checks, to assess the qualifications and suitability of prospective and current FFDOs, administer the program, issue credentials for applicants accepted into the program, and for security purposes. TSA uses the information to contact and manage participants in the program, as well as contact personal references provided by FFDO applicants.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (sometimes referred to as data mining)?

No.

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

The volunteers for the program will provide the information directly to TSA. The information will be checked for accuracy in the course of the suitability and security threat assessments.

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 voluntarily submit the information directly to TSA. TSA does not compensate FFDOs for participation, so there is no monetary

incentive to falsify information. The risk that inaccurate information will be submitted by individuals or terrorist elements seeking to infiltrate the program is minimized because potential applicants must provide a valid FAA Airman Certificate Number to access the FFDO online application system. Also, further checks such as employment history, criminal history, and credit history, along with personal reference and current employer interviews, are conducted to prevent hostile elements from entering the program. Individuals are interviewed several times during the application process and given the chance to correct inaccuracies/identified discrepancies. Finally, applicants to and participants in the program are thoroughly and repeatedly briefed on the possible ramifications of submitting false information to a federal agency.

Section 3.0 Retention

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

TSA intends to retain FFDO application records for a minimum of six years. Final disposition will be determined by applicants' date of deputization as an FFDO. TSA expects to maintain records of applicants who are not accepted into the program for six years. TSA expects to maintain records of deputized FFDOs until six years after they leave the program. TSA expects to maintain records of FFDOS who have been removed from the program due to misconduct, including those who appeal the action, for forty years, which is consistent with the average career lifetime of a pilot. The applicable record retention schedule covering the FFDO program records will be submitted to NARA for approval. Until approval, TSA will not destroy any records.

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

The applicable record retention schedule covering the FFDO program records will be submitted to NARA for approval. TSA anticipates approval of this retention schedule.

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

TSA expects to maintain information collected through this program in accordance with NARA-approved record retention schedules in furtherance of TSA's mission to ensure the security of the Nation's transportation system. TSA expects to retain FFDO applicant records for not less than six years to provide accountability of those individuals who may reapply to the FFDO program. The six year retention is sufficient to cover those individuals. TSA expects to retain records of FFDOs who have been removed from the program due to misconduct, including those who appeal the action, for forty years, which is consistent with the average career lifetime of a pilot.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

Portions of the data collected are routinely shared with the TSA Office of Human Capital (OHC), Office of Transportation Threat Assessment and Credentialing (TTAC), Office of Personnel Security, and the Transportation Security Freedom Center. Each organization has access to items of information necessary to conduct its mission. The information also is shared with several TSA contractors as part of the assessment, evaluation, and training process in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

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

The OHC, TTAC, and the Office of Personnel Security have access to information necessary to determine suitability of an applicant for the FFDO Program, including employment history, credit history, and other biographical data necessary to conduct a security threat assessment. The Freedom Center has access to FFDO flight schedules and personal data including Social Security number, date of birth, FAA Airman Certificate Number, airline employee number, airline domicile, e-mail address, telephone number, hair/eye color, and airline Chief Pilot contact information for aviation operations purposes. Access to this information is necessary to contact and manage the FFDO mission.

FFDO contact and identifying information is shared with TSA contractors for purposes of scheduling initial and continuation FFDO training, developing and administering the FFDO secure website, conducting appropriate security threat assessments of all FFDO candidates, conducting psychological examinations of FFDO applicants.

4.3 How is the information transmitted or disclosed?

TSA will transmit this data within DHS to those employees and contractors who need the information to perform their official duties in person, 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, such as SSI markings.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified 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?

TSA may share information with the Terrorist Screening Center (TSC) 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 other Federal agencies, 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, including the Federal Aviation Administration (FAA), 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, DHS/TSA 013, Federal Flight Deck Officer Record System (FFDORS), and the Office of Personnel Management's General Personnel Records (OPM/GOVT-1). The T-STAS SORN was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731-67735. The FFDORS SORN was last published in the Federal Register on August 18, 2003, and can be found at 68 FR 49509- 49511. OPM/GOVT-1 was last published in the Federal Register on April 27, 2000, and can be found at 65 FR 24732.

In addition, TSA will also share the information with individual air carriers who are employers of either deputized FFDOs or FFDO candidates. Much of the individual's information is already in the possession of air carriers as their employer.

5.2 What information is shared and for what purpose?

Biographical and information identified during the security threat assessment is shared with external organizations based on need to know and is evaluated on a case by case basis. TSA also notifies an FFDO's employer (i.e., an air carrier) upon deputation into the FFDO Program of a pilot in their employ.

5.3 How is the information transmitted or disclosed?

Depending on the recipient and the urgency of the request or disclosure, the information may be disclosed in person, telephonically, electronically via a secure data network, via facsimile, or via password protected CD.

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. There is an MOU between TSA and the Terrorist Screening Center (TSC) in connection with security threat assessments. The Privacy Act System of Records Notices described above reflects the scope of the information that will be shared.

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, the Federal Information Security Management Act (FISMA) and their applicable SORNs. Further, information concerning the identity of current or past FFDOs and FFDO applicants is SSI and must be properly handled and safeguarded in accordance the requirements of with 49 C.F.R. part 1520.

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

No specific training is required by TSA. Federal agency employees typically are required to undergo Privacy Act Training by their employing agencies. Further, all records containing SSI have an SSI disclosure warning as required by 49 C.F.R. §1520.13.

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 of the SORNs 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. The information shared with the FAA and applicant's employer is largely comprised of data the FAA and the applicant's employer already possess, which mitigates privacy risks surrounding that information sharing. Further, all SSI information must be handled and safeguarded in accordance with the requirements of 49 C.F.R. part 1520.

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 Notice. If notice was not provided, why not?

Individuals who apply for the FFDO program receive a Privacy Act Statement upon logging in to the FFDO applicant site. The Privacy Act Statement is at Appendix A of this PIA.

The publication of this PIA and of the SORNs for DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS), DHS/TSA 013, Federal Flight Deck Officer Record System (FFDORS), and the Office of Personnel Management's General Personnel Records (OPM/GOVT-1) also serve to provide public notice of the collection, use and maintenance of this information. These SORNs were last published respectively in the Federal Register on November 8, 2005, August 18, 2003, and April 27, 2000, and can be found at 70 FR 67731-67735, 68 FR 49509- 49511 and 65 FR 24732-24736.

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

Yes. Individuals volunteer for the program and may withdraw from the program at any time and at any step in the application process. Disclosure of personal information is voluntary. However, failure to provide the requested information may result in TSA's inability to complete the security threat assessment and/or psychological evaluation, which are prerequisites for participation in this program.

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

FFDO applicants are provided with meaningful notice that enables them to exercise informed consent prior to disclosing any information to TSA.

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 gain access to and correct the personal information provided during the application process by logging on to the FFDO secure web site. They do so using their name and user designated password. Individuals can also 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?

Individuals may correct erroneous information by logging on to the FFDO secure website and changing the information. If a candidate or deputized FFDO discovers erroneous or outdated information that they cannot change themselves (such as employer information), they may contact FFDO program management and advise that the information is incorrect. FFDO program management then verifies and corrects the information in the system. In the case of a change of employer, program management verifies employment with the air carrier and makes the appropriate changes.

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

Contact information is posted on the web site for candidates and deputized FFDOs, along with the procedure to follow for correcting erroneous information. Candidates and FFDOs are also periodically advised to review personal data for accuracy.

7.4 If no redress is provided, are alternatives available?

FFDOs whose deputation has been suspended or revoked may appeal the action. TSA sends written notification of suspension or revocation action. Within 15 days after receiving this written notice from TSA, the FFDO may make a written request for all releasable materials upon which the initial action was based. The FFDO then has 30 days from date of receipt of any releasable materials to file a written appeal. Not later than 30 calendar days, or such longer period as TSA determines for good cause, after TSA receives the appeal, TSA will serve a final determination.

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 incorporated processes for allowing individuals to access and correct their own records. Individuals are capable of changing erroneous information on their own in most cases. In those cases where they may not correct the information, they may contact the FFDO program management via telephone, e-mail, or the FFDO 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

8.1 Which user group(s) will have access to the system?

The FFDO Program uses two distinct Information Technology systems that provide access to authorized user groups. These systems consist of the FFDO Dashboard and the contractor-operated FFDO Program System.

The FFDO dashboard system user group includes:

The Aviation Operations Watch Officers in the Transportation Security Freedom Center, FFDO Program Management, Office of Chief Counsel, TTAC, OHC, the Office of Personnel Security, TSA contractors, and management of the air carriers that employ the FFDO. Also, the FFDO program's information technology (IT) system administrators may access this system in order to perform their duties in support of this system.

The contractor-operated FFDO Program System user group includes:

The Aviation Operations Watch Officers in the Freedom Center, FFDO Program Management, Office of Chief Counsel, TSA contractors and FFDO program IT system administrators.

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. TSA contractors supporting the FFDO program have access to the dashboard system and the contractor-operated FFDO system in order to perform their assigned roles in the operations and maintenance of these systems.

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

Yes. Role-based access controls are used for controlling access to the dashboard and the contractor-operated FFDO system using the policy of Least Privilege, which states that the system will enforce the most restrictive set of rights/privileges or access needed by users based on their roles.

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

Limited access to the dashboard and the contractor-operated FFDO system is provided for respective users. Access level is determined by FFDO Program Management, specifically the Special Agent in Charge (SAC) of Flight Programs Division, Federal Air Marshal Service (FAMS). The systems are 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 DHS-mandatory privacy training on the use and disclosure of personal data. They also 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.

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

TSA employees and contractors are assigned roles for accessing the systems based on their function. TSA ensures personnel accessing the systems have security training commensurate with their duties and responsibilities. All personnel are trained through TSA's Security and Awareness Training Program when they join the organization and periodically thereafter. The status of personnel who have completed the training is reported to TSA on a monthly basis. The Facility Security Officer ensures compliance with policy and manages the activation or deactivation of accounts and privileges as required or when expired.

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

The dashboard system is continuously monitored to audit compliance with policy. Weekly logs are reviewed to ensure no unauthorized access has taken place. All IT systems, both TSA and contractor-operated, are under required continuous monitoring by the Information System Security Officer (ISSO) for compliance and to ensure confidentiality, integrity and availability of the data. .

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

The FFDO dashboard system and the contractor-operated FFDO system incorporate user privileges, roles, and permissions which restrict access to only those personnel working within the FFDO program personnel and contractors working specifically on the credentialing 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. The systems also enforce data integrity rules to safeguard against corruption of data.

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

All government and contractor personnel are required to complete the on-line TSA Privacy Training. Compliance with this requirement is audited monthly by the TSA Privacy Officer. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting personal information being processed. All IT security training is reported as required in the Federal Information Security Management Act of 2002, Pub.L.107-347 (FISMA).

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

Yes. Information in the dashboard and FFDO program systems is safeguarded in accordance with the FISMA, which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. Certification and Accreditation was completed and the Authority to Operate was granted on August 15, 2006.

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

Data in the dashboard system and the contractor-operated FFDO 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/or biometrics. The systems are housed in controlled computer centers 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 Was the system built from the ground up or purchased and installed?

The FFDO dashboard system was built from commercial off the shelf (COTS) and government off the shelf (GOTS) products. The system is continually updated, and security patches applied to ensure the protection of the system.

The contractor-operated FFDO system was built from the ground up in support of the FFDO program. The system is continually monitored and updated with vented security patches to ensure the protection of the system and data.

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 Federal Information Processing Standards (FIPS) methodology. FIPS methodology categorizes a system as High, Medium, or Low, depending on how important the function is to the agency. The system completed a FIPS-199, Standards for Security Categorization of Federal Information and Information Systems analysis on July 13, 2006, in order to categorize the system. All security controls are applied in accordance with the results from the FIPS-199 analysis.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, TSA has limited its data collection to specific elements necessary to determine suitability of an applicant for the FFDO program. 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 and who have a need to know will have permission to use and view this information. TSA will not transmit or otherwise share this information with entities outside of DHS that are not described in the routine uses in the applicable SORNs, OPM GOVT-1, DHS/TSA 002, (T-STAS), and DHS/TSA 013, (FFDORS), or with other agencies as may be required pursuant to the Privacy Act.

Additionally, both systems include a real time audit function to track access to electronic information, and any infractions of information security rules will be addressed appropriately. Strict incident response plans are followed. 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: What design choices were made to enhance privacy?

The deployment of a defense in depth architecture addresses the physical server security, network security, data integrity, and application security and privacy limit access to personal information, thereby mitigating possible privacy risks associated with this program.

Conclusion

The Federal Flight Deck Officer Program was created to provide an added layer of security to commercial aircraft. TSA assesses the suitability of volunteers for the program while guarding the privacy of these individuals. The program continues to seek means to improve communications with FFDOs and therefore provide secure means to communicate personal data. TSA has built physical and network security into the system, and continually strives to maintain data integrity. Because disclosure of a FFDOs identity poses a security risk to the individual and to the air transport system, protection of a FFDOs identity and privacy is part of the essence of the program.

Responsible Officials

Jeff Davenjay
Special Agent in Charge, Flight Programs Division
Office of Law Enforcement/Federal Air Marshal Service
Transportation Security Administration

Approval Signature Page

_____

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Privacy Act Statement

Authority: 49 U.S.C. 114 and 49 U.S.C. 44921 authorize collection of this information.

Purpose: TSA will use this information to assess your qualification and suitability to participate in the Federal Flight Deck Officer (FFDO) program, including conduction a security threat assessment and credit history check. TSA will also use this information to administer the FFDO Program.

Routine Uses: TSA may share this information with U.S. Department of Transportation (DOT) and the Federal Aviation Administration (FAA) 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, or for other routine uses identified in TSA system of records, DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS). DHS/TSA 013, Federal Flight Deck Officer Record System (FFDORS), and the Office of Personnel Management's General Personnel Records (OPM/GOVT-1).

Disclosure: Furnishing this information, including your Social Security number (SSN), is voluntary. Your SSN will be used to verify your identity and may be used as your identification number in this process. However, failure to furnish the requested information may delay or prevent the completion of your security threat assessment and the psychological evaluation, which may result in your inability to enter the FFDO Program.