Privacy Impact Assessment
for the

Alien Flight Student Program (AFSP)

DHS/TSA/PIA-026

July 28, 2014

Contact Point
Steven Parsons
Aviation Program Management
Transportation Security Administration
Steven.Parsons@tsa.dhs.gov

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) conducts Security Threat Assessments (STA) on individuals who are not U.S. citizens or nationals and other individuals designated by TSA seeking flight instruction or recurrent training from Federal Aviation Administration (FAA)-certified flight training providers (hereinafter referred to as "covered persons" for purposes of this PIA). TSA previously conducted a Privacy Impact Assessment (PIA) and PIA Updates for the Alien Flight Student Program (AFSP), most recently on December 4, 2009. TSA is conducting this PIA because, since that time, several updates to AFSP have been made, including: 1) TSA performs recurrent vetting of covered individuals; 2) The Defense Attaché collects biographic information and creates a record in AFSP about foreign military pilots endorsed by the Department of Defense (DoD) for flight training in the United States; and 3) TSA has submitted an updated National Archives and Records Administration (NARA) schedule to change records retention to 80 years in order to permit TSA to comply with a requirement that it re-use fingerprints for recurrent flight training during the life of the covered individual.

For purposes of this PIA only, and because all covered individuals must submit the same information to TSA, this PIA does not separately analyze each of the four categories of flight training listed on the AFSP website: https://www.flightschoolcandidates.gov. The information collected has not changed.

This PIA should be read as a stand-alone document. Upon publication of this PIA, the previous PIA and PIA Updates for AFSP will be retired.

Overview

The mission of AFSP is to ensure that aliens and other individuals designated by TSA seeking training at flight schools regulated by the FAA do not pose a threat to aviation or national security. The Vision 100 – Century of Aviation Reauthorization Act prohibits flight schools regulated by the FAA from providing flight training to covered individuals unless the Secretary of Homeland Security first determines that they do not pose a threat to aviation or national security.[1] Vision 100 transferred responsibility for conducting STAs from the Department of Justice to the Department of Homeland Security (DHS). TSA issued an Interim Final Rule (IFR) in 2004, which established the current requirements for covered individuals seeking flight training in the United States or from an FAA-certified flight training provider.[2] TSA implemented the AFSP in order to conduct the STAs authorized by the Aviation and Transportation Security Act (ATSA)[3] and Vision 100. STAs include checks against law enforcement, immigration, and intelligence databases, as well as a fingerprint-based criminal history records check (CHRC).[4] TSA will also enroll fingerprints with the Office of Biometric Identity

[1] Section 612 of the Vision 100 – Century of Aviation Reauthorization Act, Public Law 108-176, December 12, 2003.
[2] Transportation Security Regulations, 49 CFR Part 1552.
[3] See 49 U.S.C. § 114(f).
[4] TSA conducts CHRCs pursuant to 49 CFR Part 1542.209.

Management's (OBIM) Automated Biometric Identification System (IDENT) biometric database for purposes of conducting recurrent fingerprint-based immigration and law enforcement checks.[5]

A covered individual seeking flight training creates an AFSP account[6] and submits his or her background information and required documentation (see Section 2.0). No STA is performed until the covered individual submits an actual training request. Once the covered individual submits a training request (i.e., initial flight training or recurrent training), the AFSP performs a STA to determine whether he or she poses a threat to aviation or national security. The STA consists of recurring checks against intelligence, law enforcement, and immigration databases. If the training request is approved, TSA notifies the individual and the flight training provider via the email address he/she provided, and the covered individual may begin training within 180 days of the approval. If the covered individual is unable to begin training within 180 days, a new training request must be submitted. If the training request is canceled or denied, both the covered individual and flight training provider are notified by email that training is not authorized. The covered individual will have an opportunity to correct or clarify information in the application before he/she submits the application, or appeal the decision after a final determination is made.

Foreign military pilots who are endorsed by DoD for flight training in the United States are not required to seek approval to train through AFSP.[7] The DoD endorsee does not undergo the standard STA process and approval to train within AFSP is not required. The DoD takes responsibility for those candidates whom the Defense Attaché endorses. However, biographic information for DoD endorsees is entered into the AFSP system by the endorsing Defense Attaché to create an electronic tracking record of candidates and their associated training event(s).

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The ATSA grants TSA authority to, among other things, assess threats to transportation, serve as the primary liaison for transportation security to the intelligence and law enforcement communities, and carry out such other duties relating to transportation security as the TSA Administrator considers appropriate.

Vision 100 - Century of Aviation Reauthorization Act transferred threat assessment responsibilities to TSA. TSA promulgated an IFR to implement the threat assessment program and security awareness training requirements on September 20, 2004.[8]

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

[5] See the Privacy Impact Assessment for Automated Biometric Identification System (IDENT), DHS/NPPD/PIA-002 at http://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system-ident.
[6] https://www.flightschoolcandidates.gov.
[7] 49 CFR Part 1552, Subpart A.
[8] See 69 Fed. Reg. 56324.

The DHS/TSA-002 Transportation Security Threat Assessment System (T-STAS) SORN[9], applies to the information collected for AFSP.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes, the Authority To Operate was granted on February 28, 2013.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

AFSP currently operates within the schedule for the Office of Transportation Threat Assessment and Credentialing (TTAC), N1-560-06-6, approved by NARA on March 8, 2007. An updated retention schedule has been submitted to NARA seeking to retain AFSP records for 80 years after they are entered in the system in order to comply with a requirement to re-use fingerprints for recurrent training that may occur over the lifetime of a covered individual.[10]

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Flight Training for Aliens and Other Designated Individuals; Security Awareness Training for Flight School Employees, OMB Control Number 1652-0021.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

TSA will collect and retain biographic and biometric data for covered individuals seeking flight instruction or recurrent training from FAA-certified flight training providers.

TSA requires the following personally identifiable information (PII):

- full name (aliases and any other names previously used);
- date of birth;
- gender;
- country of birth;
- nationality;
- height;

[9] See 75 FR 28046, May 19, 2010.
[10] 49 CFR Part 1552.

- weight;
- biometric information;
- photograph;
- eye and hair color;
- country of citizenship;
- type of citizenship (current, dual, or historical);
- whether citizenship is acquired through birth or naturalization;
- dates of citizenship;
- passport information including the issue date and expiration date, status, and city of issuance;
- current address plus last five addresses with dates of residence, phone number(s), email address; and
- visa information.

Covered individuals who are unable to obtain a current and valid passport from their country of nationality because they are refugees, asylees, or holders of a temporary protected status must submit one or more of the following documents in lieu of a passport: a refugee travel document, a permanent or conditional resident card, and/or document issued by the United States Citizenship and Immigration Services (USCIS) indicating their status as lawfully present in the U.S. and the expiration of such status.

In addition, TSA may request airman certificate information, as applicable, to include a candidate's current airman certificate, issuing country, certificate number, and type rating data, since the information may be relevant to the type of training being requested. Individuals may also choose to provide employment information, including occupation and employer's name and email address, since the employment is relevant to certain training, and certain training may be initiated by the employer.

TSA also collects training event-related information for each application as follows: type of training requested, dates and location of requested training, and a history of currently scheduled and/or previously completed training, including types, dates, and locations. Flight training providers upload a photograph of the covered individual to AFSP.

TSA conducts a name-based security threat assessment by running the biographic data through law enforcement, immigration, terrorist-related, and intelligence data sources. The FBI processes digital fingerprint files. The results of the name-based and biometric checks are returned to and stored in the AFSP system within that candidate's training application. The review, adjudication, and approval processes are executed within the AFSP system. STA results received from other government systems are returned to, analyzed, and stored in the AFSP system within the training application.[11]

[11] These include, but are not limited to: U.S. Immigration and Customs Enforcement's (ICE) Student Exchange Visitor Information Systems (SEVIS) and U.S. Customs and Border Protection's (CBP) TECS. Additional

TSA continuously vets all covered individuals against the Government watchlist. Additionally, for each new training request, their fingerprints are re-submitted to the FBI for a new CHRC.[12] Fingerprints will also be enrolled with the DHS National Protection & Programs Directorate/OBIM IDENT system[13] for recurrent immigration and law enforcement checks when this capability becomes available to TSA.

Foreign military pilots who are endorsed by DoD for flight training in the United States are not required to seek approval to train through AFSP.[14] They do not undergo the standard STA process and approval to train is not required. Biographic information for DoD endorsees is entered into the AFSP system by the endorsing Defense Attaché to create an electronic record for a training event.

2.2 What are the sources of the information and how is the information collected for the project?

Covered individual information is submitted through forms on the TSA AFSP website, https://www.flightschoolcandidates.gov. The collection requires the participation of the individual. The AFSP website provides information about the locations that will collect fingerprints.

Information used by AFSP during the STA (for example, watch lists or criminal history records) may be supplied by law enforcement, immigration, and intelligence agencies.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes, commercial or publicly available information may be used as part of the authentication process to determine the validity of some information or to assist in resolving potential disqualifying factors. For example, if a disqualifying crime is identified with the CHRC but does not show the disposition of charges, publicly available information may provide the disposition.

2.4 Discuss how accuracy of the data is ensured.

TSA relies on the accuracy of the information provided by covered individuals and by the federal agencies whose databases are checked for the STA. Covered individuals are required to enter, review, and assert that the data entered in the system is true and accurate to the best of their knowledge.

The AFSP customer relations team reviews the application and validates it against documents uploaded by the covered individual during the application process. Other information, e.g., physical address or details about the aircraft type, may be authenticated using commercial data sources.

---

information about DHS systems can be found at the DHS website at www.dhs.gov. Please refer to www.fbi.gov for information on the Terrorist Screening Database.

[12] TSA conducts CHRCs pursuant to 49 CFR Part 1542.209.

[13] See the Privacy Impact Assessment for Automated Biometric Identification system (IDENT), DHS/NPPD/PIA-002 at http://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system-ident.

[14] 49 CFR Part 1552, Subpart A.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that a covered individual may be incorrectly denied flight school training eligibility or incorrectly identified as a match to the Government watchlist.

Mitigation: TSA mitigates this risk by requiring covered individuals to submit information that should be sufficient to distinguish them from individuals on the watchlist. TSA further mitigates the risk by requiring covered individuals to certify the accuracy of the information submitted to TSA. The covered individual may appeal a denial decision directly to TSA or the U.S. Court of Appeals.[15] Information regarding the appeal process is available on the AFSP website.

Privacy Risk: There is a risk that AFSP maintains incorrect information.

Mitigation: This risk is reduced by collecting information directly from the covered individual and by emphasizing the importance of accurate data collection within the system. Covered individuals have the opportunity to correct inaccurate information during data collection and again after the application has been processed. If initially deemed ineligible, they will have an opportunity to correct inaccurate information, including resolving any issues with their criminal or immigration records.

Privacy Risk: There is a risk that the information obtained from other federal agencies or commercial sources is inaccurate.

Mitigation: The covered individual may appeal a denial decision either directly to TSA or through the U.S. Court of Appeals. Information regarding appeals is available on the AFSP website and is included in the cancellation or denial notice sent to the covered individual.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

AFSP uses PII to determine whether a covered individual poses a threat to aviation or national security such that he or she may not be eligible for flight training or recurrent training. TSA uses PII to conduct STAs, which consist of recurring checks against intelligence, law enforcement, and immigration databases.

TSA also uses PII to communicate with the covered individual about his or her application and to clarify information, such as employment status or passport information, when applicable.

TSA uses fingerprints for a CHRC conducted by the FBI. The FBI will also check fingerprints against its unsolved crimes database, but the result will not be returned to TSA since it is not actionable by TSA without more formal action beyond the possible identification of a covered individual possibly

[15] Appeals of final agency orders are covered by the U.S. Court of Appeals as required by law. See 49 U.S.C. § 46110 (a).

associated with an unsolved crime. Fingerprints will also be enrolled with the OBIM/IDENT biometric database[16] for recurrent immigration and law enforcement checks.

Finally, AFSP data will be enrolled in the DHS Common Entity Index (CEI)[17] and Cerberus systems[18] for DHS mission purposes.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

TSA shares information within DHS in order to conduct STAs. This sharing includes U.S. Citizenship and Immigration Services (USCIS) for immigration checks, and with the OBIM IDENT system for recurrent immigration and law enforcement checks.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized access to or unauthorized use of the information maintained in AFSP.

Mitigation: This risk is reduced by controlled access to AFSP, which is limited to TSA users associated with the AFSP program, the covered individual submitting his or her information, and flight training providers to provide information regarding training events. TSA AFSP system users receive privacy training and the AFSP managers were involved in the drafting of this PIA. Covered individuals are only permitted to enter and modify data they submit. The flight training providers are only allowed to enter and modify specific data surrounding a training event for which the provider has been selected to offer to the candidate. The AFSP customer relations team, adjudication analysts, and technical support team each have access to all system information and are permitted to make certain amendments or changes to system information.

Privacy Risk: There is a risk that covered individuals will not know that their information may be shared with other federal agencies.

Mitigation: This risk is reduced by issuing this PIA, which describes the ways in which information may be shared. Information is also provided at the AFSP website.

---

[16] For more information about IDENT, see the DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA at http://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd.
[17] DHS/ALL/PIA-046-2 Common Entity Index Prototype. September 26, 2013.
[18] DHS/ALL PIA-046-3 Cerberus Pilot. November 22, 2013.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

TSA's AFSP website, used by the covered individual to establish his or her account, provides a written privacy policy, including a Privacy Act statement as required by the Privacy Act of 1974.[19] The Privacy Act statement explains why TSA collects personal information, the authority for the collection, and how it will be used. Additionally, TSA provides notice through the publication of this PIA and the DHS/TSA-002 T-STAS SORN.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals who decide not to provide the required information may choose not to apply or suspend their application.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that a candidate may not know how his or her information is used.

Mitigation: This risk is reduced by information provided by TSA at the time of application through the Privacy Act statement on TSA's AFSP website, as well as this PIA and the DHS/TSA-002 T-STAS SORN. Covered individuals cannot create an account without going to the website.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

AFSP operates within the NARA-approved schedule TTAC, N1-560-06-6 (March 8, 2007). An updated retention schedule has been submitted to NARA seeking to retain AFSP records for 80 years after they are entered in the system in order to permit the re-use of fingerprints and other biographical information for additional training events that may occur over the lifetime of a candidate.

TSA has a legal requirement to conduct STAs on covered individuals associated with AFSP. In accordance with the law,[20] promulgated through the IFR, an individual who has submitted his or her information to TSA is not required to re-submit biometric information with future applications for training. AFSP is seeking to revise its retention schedule to retain records for 80 years after data is entered into the system in order to accommodate this requirement.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information is retained for longer than necessary.

[19] 5 U.S.C. § 552a(e)(3).
[20] 49 CFR Part 1552.

Mitigation: TSA currently retains these records in accordance with the records retention schedule approved by NARA, March 8, 2007. The retention schedule was developed to retain information for a short period except when the individual was a match to a watchlist. An updated AFSP retention schedule has been submitted to NARA to permit covered individuals to apply for recurrent training without resubmitting fingerprints.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

TSA shares biographic and biometric information with the FBI in order to conduct a background check. Further, TSA may share biographic and biometric information with external users of the DHS CEI and Cerberus Systems.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

DHS/TSA-002 T-STAS SORN, Routine Use I. permits disclosure "to the appropriate Federal, State, local, tribal, territorial, foreign, or international agency regarding candidates who pose, or are suspected of posing, a risk to transportation or national security." This is compatible with the collection of information for purposes of conducting STAs since the Terrorist Screening Center (TSC) is the agency that maintains the Terrorist Screening Database (TSDB) and may coordinate an operational response if appropriate.

Routine Use K. allows TSA to share biographic and biometric information with the FBI to conduct a background check. This is compatible with the original collection because the FBI is the leading authorized government entity to determine whether a candidate has committed crimes.

6.3 Does the project place limitations on re-dissemination?

No, TSA does not place limitations on re-dissemination of information except to the extent match information is Sensitive Security Information (SSI).[21] Re-dissemination of SSI is limited by the SSI regulation.[22]

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Through the AFSP system, TSA maintains an accounting for all information sent to the FBI for background checks. For each training application with a completed STA, the transmission to and results from the FBI are captured within the AFSP system. For other disclosures outside of DHS, the AFSP

[21] 49 U.S.C. § 114(r), November 19, 2001.
[22] 49 CFR Part 1520, May 18, 2004.

system provides a transaction log of the export or file transfer of the requested data. System documentation includes disclosure details manually entered into the file, including date and nature of each disclosure, and name and address of the candidate or agency to which the disclosure is made.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be inappropriately shared.

Mitigation: TSA may share this information only in accordance with the Privacy Act. TSA employees receive privacy training to mitigate the risk of inappropriate sharing. Further, TSA has entered into an MOU with the FBI and TSC governing the conditions of sharing information related to STA programs.

Section 7.0 Redress

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

The online AFSP application process allows covered individuals to enter, edit, save, and submit their required data. They may access and edit their data prior to the STA being conducted. Candidates may request access to their data under the Privacy Act by contacting the TSA Headquarters Freedom of Information Act (FOIA) Office, at FOIA Officer, Transportation Security Administration, TSA-20, Arlington, VA 20598-6020 or by email at FOIA.TSA@dhs.gov. Please refer to the TSA FOIA web site (http://www.tsa.gov/research/foia/index) for more information. Access may be limited pursuant to exemptions asserted under 5 U.S.C. § 552a (k)(1) and (k)(2).

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The online AFSP application process allows covered individuals to enter, edit, save, and submit their own required data, and they may access and edit their data prior to application acceptance and the STA being conducted.

A covered individual may also seek correction through the procedures described in Section 7.1 above. Additionally, if they believe TSA's determination on a training request is incorrect, they may seek judicial review through the United States Court of Appeals.

7.3 How does the project notify individuals about the procedures for correcting their information?

TSA provides procedures for correcting information, and this PIA further provides notice on how to correct information held by TSA. If the application is cancelled (e.g., due to immigration-related concerns), TSA will notify the covered individual using the email address he or she has provided. The email provides instructions regarding redress and a telephone number to call in case there are questions. In addition, the TSA website provides information on how to submit a Privacy Act request.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that covered individuals will not have an opportunity to correct, access, or amend their records maintained by TSA.

Mitigation: Covered individuals have an opportunity to check their data when it is submitted to TSA. In addition, they may seek access to TSA records by submitting a request under the Privacy Act, though some aspects of their record may be exempt from access.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

TSA uses encrypted sessions between the end user's browser and the web for data integrity and privacy. Once user data has been obtained at the web server, it will be transferred to a TSA database server over an encrypted network. Only TSA system administrators, security administrators, IT specialists, vetting operators, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Role-based access controls are employed to limit the access of information by different users and administrators based on the need to know the information for the performance of their official duties. TSA also employs processes to enforce separation of duties, to prevent unauthorized disclosure, or to prevent 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. Finally, AFSP's program management was involved in the conduct and approval of this PIA.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project?

TSA users receive annual DHS privacy training on appropriate protection of PII, including handling and sharing.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to AFSP is approved specifically for, and limited only to, users who have an official need for the information in the performance of their duties. As discussed above, covered individuals have access to their application data, and flight training providers have access to flight training event data. The AFSP customer relations team, adjudication analysts, and technical support team each have access to all system information and are permitted to make appropriate amendments or changes to system information.

All access to, and activity within, the system are tracked by auditable logs.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

New information sharing, uses, or access are controlled in accordance with Sections 8.2 and 8.3 above, and are reviewed by the program manager, appropriate program leadership, component Privacy Officer, and counsel and sent to DHS for formal review as needed.

Responsible Officials

Steve Parsons
Transportation Security Administration
Aviation Program Management
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security