Transportation
Security
Administration

Alien Flight Student Program
Privacy Impact Assessment

June 18, 2004

Contact Point:

Lisa S. Dean
Privacy Officer
Transportation Security Administration
571.227.3947

Reviewing Official:

Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security
202.772.9848

Rulemaking Overview

On November 19, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA). Under Section 113 of ATSA (49 U.S.C. 44939), certain aviation training providers were prohibited from providing flight training to aliens and other designated individuals (candidates) in the operation of aircraft with a maximum certificated takeoff weight (MTOW) of 12,500 pounds or more, unless the aviation training provider notified the Attorney General of the identity of the candidate and the Attorney General did not notify the aviation training provider within 45 days that the candidate presented a threat to aviation or national security. If the Attorney General determined that a candidate presented a threat to aviation or national security more than 45 days after receiving notification from the training provider, the Attorney General was required to notify the training provider, and the training provider was required to terminate the candidate's flight training immediately.

In accordance with Section 113 of ATSA, the Department of Justice (DOJ) issued a final rule on February 13, 2003, establishing the Flight Training Candidate Checks Program (FTCCP). The FTCCP used a web-based portal to collect information and a computer-based information and analytical tool to facilitate the risk assessment process for candidates seeking flight training from U.S. aviation training providers.

On December 12, 2003, Congress enacted Vision 100 – Century of Aviation Reauthorization Act, Pub. L. 108-176 (Vision 100). Section 612 of Vision 100 made several changes to 49 U.S.C. 44939, including: (1) transferring the threat assessment responsibilities from the Attorney General to the Secretary of Homeland Security; (2) clarifying that training providers include "a person operating as a flight instructor, pilot school, or aviation training center"; (3) specifying various categories of identifying information the Secretary can require training providers to submit for training candidates; (4) reducing the amount of time a provider must wait after submission of a candidate's identifying information before initiating training for the candidate, and thus the time the Secretary has to conduct a threat assessment, from 45 days to 30 days for most candidates; (5) requiring the Secretary to conduct a threat assessment for certain classes of candidates, such as pilots who are employed by a foreign air carrier that is certified under 14 CFR part 129 and that has a security program approved under 49 CFR part 1546, within 5 days; (6) expanding the population of candidates subject to the threat assessment requirements to include candidates who apply for training in the operation of an aircraft having an MTOW of 12,500 pounds or less; (7) authorizing the Secretary to assess a fee for the threat assessment; (8) specifying that the threat assessment requirements do not apply to foreign military pilots who are endorsed by the Department of Defense (DOD) for flight training in the U.S.; (9) clarifying that flight training does not include recurrent training, ground training or demonstration flights for marketing purposes; and (10) mandating that the Secretary require flight training providers to provide security training to certain flight school employees to increase their awareness of suspicious circumstances and activities of individuals enrolling in or attending flight schools.

Section 612 also required TSA to promulgate an Interim Final Rule (IFR) to implement the threat assessment program and security awareness training requirements. TSA published the IFR on September 20, 2004. *See* 69 Federal Register 56324. TSA has developed a threat assessment program (named the Alien Flight Student Program, or AFSP) and is implementing the required changes. Because the AFSP system contains personal information about individual candidates in the United States and abroad, TSA is sensitive to the important privacy interests at stake.

In an effort to make the AFSP as transparent as possible, as well as to address any privacy concerns that may arise as a result of changes to the program, TSA is conducting this Privacy Impact Assessment (PIA) in accordance with the guidance issued by the Office of Management and Budget (OMB) on September 26, 2003. This PIA will be modified as necessary to reflect future changes and updates to the program.

System Overview

- ### Why is personal data and information being collected?

TSA will collect personal information about certain flight-training candidates to conduct the security threat assessments required by ATSA and Section 612 of Vision 100. For pilots seeking recurrent training, AFSP will verify eligibility for recurrent training. This information will enable TSA to identify individuals who may pose a threat to aviation or national security, or who may be wanted for the commission of a crime in the United States or elsewhere, or are currently in violation of United States immigration laws or regulations.

- ### What personal information will be collected?

TSA will collect and retain personal biographical and biometric data about the flight-training candidates who are required to undergo a security threat assessment or verification of eligibility for recurrent training. The IFR defines four categories of candidates that are subject to this requirement and the actual data that TSA will collect varies by category. Appendix A identifies the specific data that will be collected for each category. For all categories of candidates, as defined by the IFR, either the candidate or the flight school must complete an online personal information form, located on a secure government website at https://www.flightschoolcandidates.gov, and submit the form electronically to TSA prior to the candidate's enrollment. The completed application will be transmitted electronically to TSA where a unique candidate identification number and record will be created.

- ### Who is affected by the collection of this data?

TSA will collect information about four (4) categories of flight-training candidates: Category 1 is for candidates who request training on aircraft with an MTOW of more than 12,500 pounds and are not eligible for expedited processing; Category 2 is for candidates who request training on aircraft with an MTOW of more than 12,500 pounds and are eligible for expedited processing; Category 3 is for candidates who request training on aircraft with an MTOW of 12,500 pounds or less; and Category 4 is for candidates who request recurrent training on aircraft for which they are current and qualified.[1] Those who apply and qualify for Category 4 status will not undergo a security threat assessment. If a candidate has applied for but does not meet the requirements for Category 4 status, TSA will notify the candidate and flight school and the candidate will have to re-apply under another category and undergo the required threat assessment.

- ### What information technology system will be used for this program and how will it be integrated?

For candidates whose security threat assessment includes the collection of fingerprints, the process will generally occur in two steps.[2] The first step is a collection of information for a name-based security threat assessment. All candidate applications will be submitted via a secured government Internet website at www.flightschoolcandidates.gov by the candidate. The application process includes an interactive application to walk the candidate through the process and, where appropriate, collect the candidate's applicant fee. Once the application is submitted, an electronic file is created linked to a unique identification number assigned to the candidate.

[1] TSA will not collect information about foreign military pilots who are endorsed by the DOD for flight training in the United States.

[2] See Appendix B, AFSP data flow diagram. An applicant's candidate category will determine in each case what information is collected and may slightly vary the flow of information. See Appendix A. As discussed above, Category 4 candidates will not undergo a security threat assessment at all, although TSA must collect their information at the outset to confirm that they meet the requirements for Category 4 status.

For candidates in categories 1, 2, and 3, TSA will then conduct a name-based security threat assessment by running the names through law enforcement, immigration, terrorist-related, and intelligence data sources both classified and unclassified. Most of the databases will be accessed directly by either DHS employees or cleared TSA contractors; however, some databases, including the classified databases, will be accessed by providing candidate information to the federal agency maintaining or using the database. All candidates must submit passport information (see Appendix A). Passport information will be sent to TSA via a clearinghouse run by a TSA contractor. All classified material will be handled commensurate with federal guidelines for storing, accessing, sharing, copying, and transmitting classified information. Although these guidelines are for security purposes, they also add another layer of privacy protection to the candidate information. TSA and/or TSA contractors will review the results and will make a preliminary determination as to whether a candidate poses or is suspected of posing a security threat. If TSA makes a determination that a candidate poses or is suspected of posing a security threat, TSA will notify the training flight school that the candidate may not receive or continue to receive flight training. TSA will also share information about such candidates with the appropriate governmental, law enforcement and intelligence agencies.

The second step of the security threat assessment is a fingerprint-based check of appropriate law enforcement, intelligence, immigration, and terrorist-related databases. After the name-based threat assessment, candidates have the choice of submitting their fingerprints through several secure options described in Appendix A. Regardless of the method the candidate chooses, all fingerprints will be sent to TSA via a clearinghouse run by a TSA contractor. The clearinghouse assists in the collection and processing of candidate fingerprints and tracking and processing of applicant fees. Additionally, for candidates who choose to submit their fingerprints to an entity that does not collect them in an electronic format, the clearinghouse scans the fingerprints and converts them into an electronic format for TSA. Once the fingerprints are received, they are run through the appropriate Department of Justice and Department of Homeland Security databases. The results become part of the candidate's electronic file, which is analyzed by TSA and TSA contract analysts. If TSA determines that a candidate poses or is suspected of posing a security threat, the training flight school will be notified that the candidate may not receive or continue to receive flight training. Additionally, the candidate information will be shared with the appropriate governmental, law enforcement and intelligence agencies.

- **What opportunities for consent are provided to individuals regarding the collection of their personal data and information?**

TSA's website located at www.flightschoolcandidates.gov provides a written privacy policy, including a Privacy Act statement as required by the Privacy Act of 1974 (5 U.S.C. 552a (e)(3)). The Privacy Act statement informs candidates of the reasons why their personal information is being collected, the authority for the collection, and how it will be used. The notice also informs the candidates that the collection of the information is voluntary, but those who decline to provide it will not be eligible for the requested flight training. Candidates who are not willing to provide the required information may choose not to apply for flight-training or withdraw their application.

- **Does this program create a new system of records under the Privacy Act?**

No. The information collected for the AFSP will become part of an existing TSA Privacy Act system of records known as the Transportation Workers Employment Investigation System (DHS/TSA 002). The collection, maintenance, and disclosure of information will be in compliance with the Privacy Act and the system of records notice for DHS/TSA 002, which was published in the Federal Register on August 18, 2003. *See* 68 Fed. Reg. 49496, 49498.

- **What is the intended use of the information collected?**

Because the AFSP system is primarily a risk assessment tool, the information being collected will be used to establish a flight-training candidate's identity, and to conduct a security threat assessment on the candidate in compliance with legislative mandates set forth in ATSA and the Vision 100--Century of Aviation Reauthorization Act. These purposes will be effective for querying candidates' names and biometrics against databases. Additionally, however, the information collected will be used to ensure all required program fees have been collected from the candidate through www.pay.gov.[3] Please note that in the case of candidates who seek recurrent training in a specific aircraft (Category 4 candidates), TSA simply verifies that the candidate is current and qualified to fly the aircraft; no risk assessment is performed.

- **With whom will the collected information be shared?**

Personal information collected and stored in the AFSP system will be shared with the appropriate government, law enforcement, intelligence authorities, and government contractors involved in processing the security threat assessments and analyzing the results. If a candidate is determined to pose or is suspected of posing a security threat, then the information will be shared with appropriate government and international intelligence and law enforcement agencies depending on the nature of the threat.

- **How will the information be secured against unauthorized use?**

Personal information will be protected at various system access points. TSA uses Secure Socket Layer (SSL) 128-bit encrypted sessions between the end users 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 employees and contractors with proper access privileges will have access to this information to conduct the security threat assessment. TSA follows all security practices as found in the DHS IT Security Program Handbook.

As discussed below, all DHS/TSA and assigned contractor staff will receive appropriate privacy and security training, and have any necessary background investigations and security clearances for access to sensitive, privacy or classified information or secured facilities.

Personal information collected from candidates will be used for the purposes of the AFSP as stated in this document and the AFSP IFR, and in conformance with the Privacy Act and the system of records notice for DHS/TSA 002. TSA ensures this via legal agreements with its contractors and internal privacy policy enforcement with all DHS entities involved in processing the security threat assessments.

Finally, TSA's Privacy Officer is responsible for ensuring that the privacy of all candidates is respected and responding to individual concerns about the collection and retention of personal information in the AFSP program. The TSA Privacy Officer will review privacy issues related to this program to ensure privacy concerns are considered in all aspects of this program.

- **Will the information be retained, and if so, for what period of time?**

TSA intends to retain these records for a sufficient period of time to permit affected individuals an opportunity to pursue appropriate redress or appeal measures, as well as to permit TSA to retain

[3] Pay.gov is a secure website where the candidate can use either check or credit card to pay the required program fees. The candidate can either submit his or her credit card number through the site or obtain an address by which he or she can mail a check. For those candidates who choose to mail a check for their fees, please allow up to five business days for the check to clear once it is received.

adequate records of its actions under this program. TSA does not yet have a record retention schedule approved by the National Archives and Records Administration (NARA) for records pertaining to this program. TSA is in the process of developing a records retention schedule that will dictate the retention period for these records. Once the records schedule is approved, TSA will amend this document to include the retention period for AFSP records. Until a records schedule is identified, all records will be retained.

- **Will the information collected be used for any other purpose other than the one intended?**

Information is being collected in order to conduct and track the status of security threat assessments for flight-training candidates. Information may be shared with appropriate government, law enforcement, intelligence authorities, to identify potential threats to transportation security, uphold and enforce the law, and ensure public safety. Additionally, information will be used to track the collection of fees incurred to conduct a security threat assessment. Information collected will be used only for the purposes and manner described herein.

- **What databases will the names be run against?**

Information collected for purposes of conducting a security threat assessment will be processed against various systems and databases, to include but not limited to intelligence, law enforcement, immigration, and terrorist-related databases maintained or used by the U.S. Department of Homeland Security, the U.S. Department of Justice, and the intelligence community.

- **What technical safeguards are in place to secure the data?**

The AFSP program secures information and the systems on which that information resides by complying with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules, which are applied to component systems, communications between component systems, and at interfaces between component systems and external systems. In addition, DHS and DOJ databases have been individually certified and accredited as satisfying applicable security requirements by their legacy organizations.

One aspect of the DHS comprehensive program to provide information security involves the establishment of rules of behavior for each major application, including AFSP. These rules of behavior require users to be adequately trained regarding the security of their systems. These rules also require a periodic assessment of physical, technical, and administrative controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. In addition, the rules of behavior already in effect for each of the component systems on which AFSP draws will be applied to the program, adding an additional layer of security protection.

Privacy Threats and Mitigation Measures

The table below provides an overview of the privacy risks associated with AFSP and the types of mitigation measures that address those risks.

Table 1: Overview of Privacy Threats and Mitigation Measures

Type of Threat	**Description of Threat**	**Type of Measures to Counter/Mitigate Threat**
Unintentional threats from insiders[4][4]	Unintentional threats include flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians (i.e., personnel of organizations with custody of the information). These threats can be physical (e.g., leaving documents in plain view) or electronic in nature. These threats can result in insiders being granted access to information for which they are not authorized or not consistent with their responsibilities.	These threats are addressed by (a) developing a privacy policy consistent with Fair Information Practices, laws, regulations, and OMB guidance; (b) defining appropriate functional and interface requirements; developing, integrating, and configuring the system in accordance with those requirements and best security practices; and testing and validating the system against those requirements; and (c) providing clear operating instructions and training to users and system administrators.
Intentional threat from insiders	Threat actions can be characterized as improper use of authorized capabilities (e.g., browsing, removing information from trash) and circumvention of controls to take unauthorized actions (e.g., removing data from a workstation that has been not been shut off).	These threats are addressed by a combination of technical safeguards (e.g., access control, auditing, and anomaly detection) and administrative safeguards (e.g., procedures, training).
Intentional and unintentional threats from authorized external entities	Intentional: Threat actions can be characterized as improper use of authorized capabilities (e.g., misuse of information provided by AFSP) and circumvention of controls to take unauthorized actions (e.g., unauthorized access to systems). Unintentional: Flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians	These threats are addressed by technical safeguards (in particular, boundary controls such as firewalls) and administrative safeguards in the form of routine use agreements which require external entities (a) to conform with the rules of behavior and (b) to provide safeguards consistent with, or more stringent than, those of the system or program
Intentional threats from external unauthorized entities	Threat actions can be characterized by mechanism: physical attack (e.g., theft of equipment), electronic attack (e.g., hacking, interception of communications), and personnel attack (e.g., social engineering).	These threats are addressed by physical safeguards, boundary controls at external interfaces, technical safeguards (e.g., identification and authentication, encrypted communications), and clear operating instructions and training for users and system administrators.

For each life-cycle stage—collection, use and disclosure, processing, and retention and destruction—key issues are assessed, privacy risks identified, and mitigation measures discussed. Risks are related to fair information principles—notice/awareness[5], choice/consent,

[4] Here, the term “insider” is intended to include individuals acting under the authority of the system owner or program manager. These include users, system administrators, maintenance personnel, and others authorized for physical access to system components.

[5] Includes limitation of collection, use, disclosure, and retention to that which is consistent with the stated purposes.

access/participation, integrity/security, and enforcement/redress—that form the basis of many statutes and codes.

- **Will the staff working with the data have appropriate training and security clearances to handle the sensitivity of the information?**

All TSA and assigned contractor staff working on AFSP will or have completed mandatory security training commensurate with their role and responsibility. They also receive privacy training on the use and disclosure of personal data prior to the transfer of the program from DOJ to TSA. Additionally, government and contract operators will receive training that relates to the handling of personal data specifically related to the AFSP security threat assessment. Staff assigned to handle classified threat assessment information will be required to obtain appropriate security clearances.

Additionally, all staff must hold appropriate credentials for physical access to the sites housing the security threat assessment databases and management applications. Physical access safeguards include the use of armed or unarmed security guards at sites; hard-bolting or fastening of databases, servers, and workstations; and credential readers for internal and external site access. The DHS contractors also hold appropriate facility security clearances.

Appendix A – AFSP Candidate Data Requirements

Below are the information requirements for candidates in each of the four AFSP categories.

Category 1 Candidates (Regular Processing)

Prior to the start of flight training, a Category 1 candidate is required to provide the following information to TSA:

(1) The candidate's full name, including any aliases used by him or her, or variations in the spelling of his or her name;

(2) A unique student identification number as a means of identifying records concerning the candidate;[6]

(3) A legible copy of the candidate's current, un-expired passport and visa;[7]

(4) The candidate's passport and visa information, including all current and previous passports and visas held by the candidate and all the information necessary to obtain a passport or visa;[8]

(5) The candidate's country of birth, current country or countries of citizenship, and each previous country of citizenship, if any;

(6) The candidate's actual date of birth or, if the candidate does not know his or her date of birth, the approximate date of birth used consistently by the candidate for his or her passport or visa;

(7) The dates and location of the candidate's requested training;

(8) The type of training for which the candidate is applying, including the aircraft-type rating the candidate would be eligible to obtain upon completion of the training;

(9) The candidate's current u.s. pilot certificate, certificate number, and type rating, if any;

(10) The candidate's fingerprints;

(11) The candidate's current address and telephone number, as well as each address for the five years prior to the date of the candidate's application; and

(12) The candidate's gender.

This information is either required under Section 612 of Vision 100, is necessary for TSA to determine the identity of the candidate, or is necessary for TSA to determine what type of training a candidate is applying to receive.

A candidate is required to submit his or her fingerprints to TSA as part of the identification process. The candidate's fingerprints must be collected either: (1) by, or under the supervision of, a U.S. Federal, State, or local law enforcement agency; (2) by U.S. Government personnel at a U.S. embassy or consulate, where available; or (3) by another entity, such as a contractor[9] who would follow guidelines approved by the Federal Bureau of Investigation (FBI) or TSA. In order for TSA to match the candidate's information with his or her fingerprints, the candidate must complete the online TSA form and submit it to TSA electronically prior to the submission of fingerprints.

[6] When a candidate or flight school (in the case of category 4 candidates) completes the TSA form on the website and submits it to TSA, the website generates a unique identification number for that candidate.

[7] A candidate may either scan his or her complete passport and submit it to TSA electronically, or copy his or her complete passport and fax it to TSA via a clearinghouse using the fax number provided on the website.

[8] More detail on the type of visa and passport information required is available on the website.

[9] This option is available in those regions of the U.S. where no other approved entity has the ability to take fingerprints.

The candidate must show his or her passport (if a non-resident alien), or resident alien card or U.S. driver's license (if a resident alien), in order to confirm his or her identity to the entity collecting the fingerprints.

Category 2 Candidates (Expedited Processing aircraft more than 12, 500 pounds)

Some candidates may be eligible for expedited AFSP processing. Submission of information for these candidates is identical to candidates in Category 1, set forth above) These are candidates who:

(1) Hold an airman's certificate from a foreign country that is recognized by the FAA or a U.S. military agency, and that permits the candidate to operate a multi-engine aircraft that has a certificated takeoff weight of more than 12,500 pounds;

(2) Are employed by a foreign air carrier that operates under 14 CFR part 1546;

(3) Have unescorted access authority to a secured area of an airport under 49 U.S.C. 44936(a)(1)(A)(ii), 49 CFR 1542.209, or 49 CFR 1544.229;

(4) Are flight crew members who have successfully completed a criminal history records check in accordance with 49 CFR 1544.230; or

(5) Are part of a class of individuals to whom TSA has determined providing flight training poses a minimal threat to aviation or national security because of the flight training already possessed by that class of individuals.

TSA requires Category 2 candidates to provide all of the information collected of Category 1 candidates, in addition to documentation, such as a copy of the candidate's security identity display area (SIDA) badge, necessary to establish their eligibility for expedited processing. TSA will provide on the AFSP website a list of acceptable types of documentation that establish a candidate's eligibility for expedited processing.

Category 3 Candidates (aircraft 12,500 pounds and less)

Category 3 candidates are required to submit the same information required of Category 1 candidates, including their fingerprints.

Category 4 Candidates (Recurrent training)

TSA requires flight schools, prior to beginning a candidate's recurrent training, to notify TSA that a candidate has requested recurrent training. Either the candidate or the flight school is required to submit to TSA the following information:

(1) The candidate's full name, including any aliases used by the candidate or variation in the spelling of the candidate's name;

(2) Any unique student identification number issued by the doj or tsa that would help establish a candidate's eligibility for the recurrent training exemption;

(3) A copy of the candidate's current, un-expired passport and visa;

(4) The candidate's current u.s. pilot certificate, certificate number, and type rating(s);

(5) The type of training for which the candidate is applying;

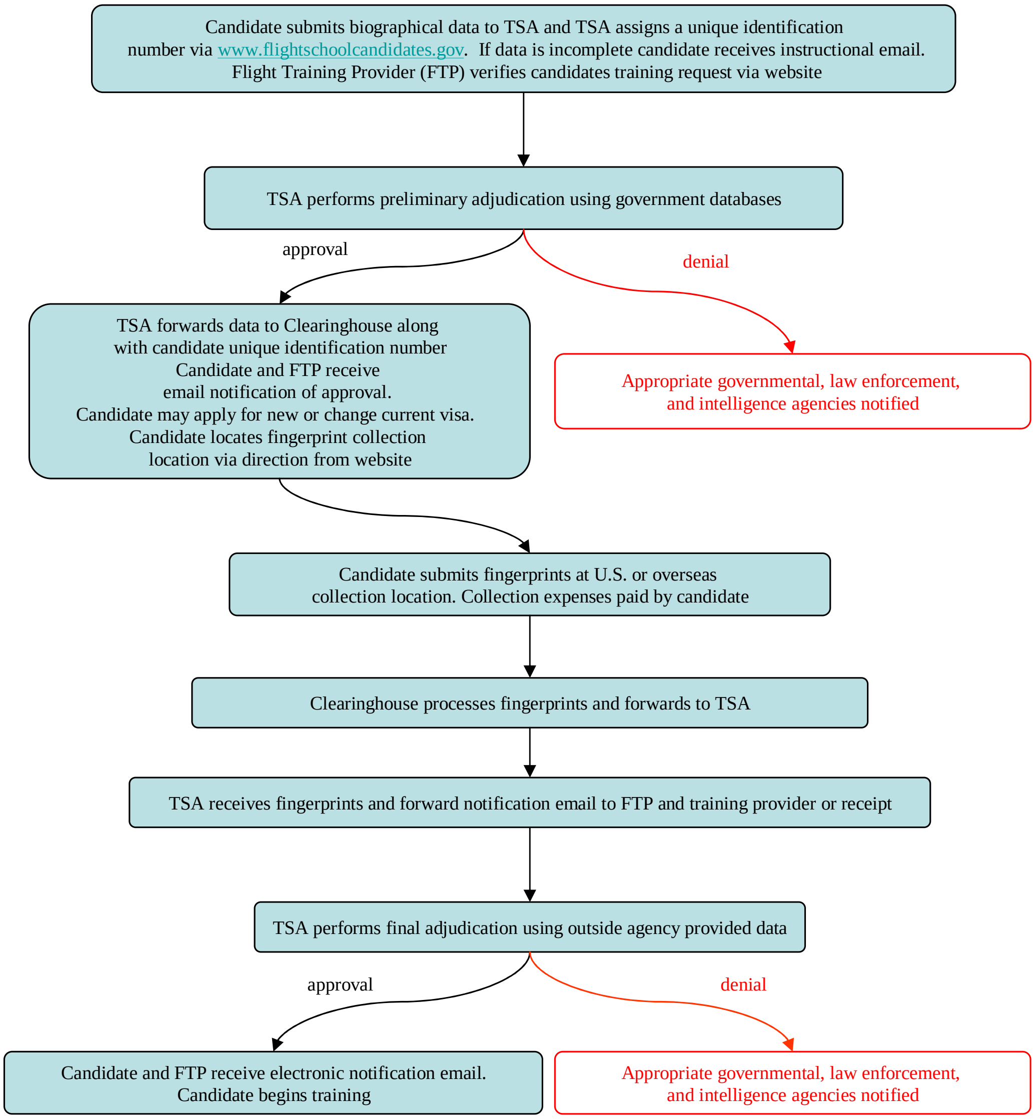
(6) The date of the candidate's prior recurrent training, if any, and a copy of the training form documenting that recurrent training; and

(7) The dates and location of the candidate's requested training.

This information is necessary to establish a candidate's identity and determine whether he or she is applying for recurrent training and thus exempt from the security threat assessment requirements.

Appendix B

AFSP Data Flow*



Candidate submits biographical data to TSA and TSA assigns a unique identification number via www.flightschoolcandidates.gov. If data is incomplete candidate receives instructional email. Flight Training Provider (FTP) verifies candidates training request via website

TSA performs preliminary adjudication using government databases

TSA forwards data to Clearinghouse along with candidate unique identification number
Candidate and FTP receive email notification of approval.
Candidate may apply for new or change current visa.
Candidate locates fingerprint collection location via direction from website

Appropriate governmental, law enforcement, and intelligence agencies notified

Candidate submits fingerprints at U.S. or overseas collection location. Collection expenses paid by candidate

Clearinghouse processes fingerprints and forwards to TSA

TSA receives fingerprints and forward notification email to FTP and training provider or receipt

TSA performs final adjudication using outside agency provided data

Candidate and FTP receive electronic notification email.
Candidate begins training

Appropriate governmental, law enforcement, and intelligence agencies notified

*This chart accurately reflects the data flow for all categories of candidates with the following exceptions: There is no preliminary approval for Category III Candidates, and Category IV Candidates receive only notification of application receipt and will not undergo a security threat assessment.