U.S. Department of Transportation

Federal Aviation Administration (FAA)
Office of Aviation Safety (AVS)
Privacy Impact Assessment
FAA Safety Team Website (FSTW)

Responsible Official

Anthony D'Angelo
System Owner
Phone Number: 1-631-383-7261
faasafety@faa.gov

Reviewing Official

Karyn Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Federal Aviation Administration (FAA) Safety Team Website (FSTW) is a web-based system developed by the FAA that provides a central portal to online information regarding training and safety courses. Airmen (pilots, including remote pilots[1], mechanics and other certificated airmen) and any member of the public that is interested can access the website to complete training/safety relate courses, receive credit for completion of training/safety-related courses, register for safety events and seminars, and receive email notifications about upcoming safety seminars and events in the aim of lowering the nation's aviation accident rate. Training is provided by industry volunteers to include Training Providers, FAA Safety Team (FAASTeam) Representatives, Lead Representatives, Certified Flight Instructors (CFIs) and FAA personnel. The type of training offered include seminars, webinars, ground and flight training, and online courses.

The FAA is publishing this Privacy Impact Assessment (PIA) for the FSTW in accordance with Section 208 of the E-Government Act of 2002 because the FAA collects Personally Identifiable Information (PII) from airmen, remote pilots, Aviation Maintenance Technician (AMTs), and any member of the public (hereafter refer to as Individuals) that are interested in attending training, seminars or reviewing content available on the website.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[2]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's

[1] An individual who pilots an Unmanned Aircraft System.

[2]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The Federal Aviation Act of 1958 gives the FAA the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. The FAA is responsible for:

- Regulating civil aviation to promote safety;
- Encouraging and developing civil aeronautics, including new aviation technology;
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- Regulating U.S. commercial space transportation.

The FSTW is located at https://www.faasafety.gov/ and provides a central portal to online information regarding safety training events and courses. Individuals do not have to create an account to view information available at this website. However, individuals need to create an account to take full advantage of the website's benefits, including participating in the WINGS Pilot Proficiency Program[3], AMT Awards Program[4], completing training, receiving credit for completion of safety-related courses, registering for safety events and seminars, and receiving email notifications about safety information, and upcoming seminars and events.

[3] This program promotes air safety and encourages general aviation pilots to continue training and maintain proficiency. Information about this Program is available at https://www.faasafety.gov/WINGS/pub/learn_more.aspx.

[4] This program encourages AMTs and employers to take advantage of initial and recurrent training by issuing awards based on training received in one calendar year. The AMT Awards Program was developed when the FAA recognized the need for an incentive program that would encourage technicians and employers to participate in maintenance training. The FAA recognizes these technicians and employers by issuing awards for receiving, promoting, and fostering initial and recurrent maintenance training.

Create an Account

To create an account, individuals provide their name, zip code, airman certificate number (airman only[5]), Civil Air Portal (CAP) identification (United State Air Force CAP personnel only), email address which serves as their username, and password recovery questions and answers which may include PII such as mother's maiden name. Upon submission, FSTW sends an email notification that include a temporary password that individuals must change upon initial login.

Once the account is created, individuals may then select the type of email notifications they would like to receive based on their interests. Examples include general information, repair station, FAA job opening announcements, and Safety Stream – Pilots. Individuals will be able to browse a list of upcoming training to include on-demand courses and live events such as seminars and webinars. They will also be able to enroll in on-demand courses and register for live events. The individual name that is associated with account is used for enrollment in online course and seminars.

FAA Safety Team (FAASTeam)

The FAA established the FAA Safety Team (FAASTeam) with the premise that general aviation accidents can be reduced by improving the knowledge and proficiency of pilots, AMTs, and other involved in the aviation community. FAA employees and representatives from all segments of the aviation industry, such as airmen, air carriers, repair facilities, flight and mechanic schools, and other aviation entities and individuals, can become a FAASTeam member. Individual that would like to become a FAASTeam member are required to submit an application available on the FSTW and manually enter the following information:

- ***FAASTeam Representatives, (includes Lead Representatives)*** are volunteers who conduct safety events, validate completion credits, and create event announcements in the Safety Program Airmen Notification System (SPANS).
    - Full name;
    - Mailing address;
    - Region and district office;
    - Published name (name of user to be displayed in system);
    - Contact telephone number(s);
    - Additional email addresses (optional);
    - Airman certification types;
    - Airman certificate number;
    - Country of origin;
    - Total flight time;
    - Full name of person who recommended user to join FAASTeam;
    - Open-comments box that user can explain for reasons to join FAASTeam;

[5] FSTW uses the AVS Registry to validate the airman certificate number.

- Specialties;
- Areas of expertise (open-comments box);
- List of facilities available for FAA seminars and events;
- Facility name and type; and
- An uploadable self-portrait image (optional).

- ***FAASTeam Service Providers (FSP)*** are volunteers who assist at safety events or provide a service that is valuable to the FAASTeam. These individuals do not have elevated permissions on the website and do not enter information into SPANS or validate credits.

  - Full name;
  - Mailing address;
  - Region and district office;
  - Published name (name of user to be displayed in system);
  - Contact telephone number(s);
  - Additional email addresses (optional);
  - Airman certification types;
  - Airman certificate number;
  - Country of origin;
  - Total flight time;
  - Full name of person who recommended user to join FAASTeam;
  - Open-comments box that user can explain for reasons to join FAASTeam;
  - Specialties;
  - Areas of expertise (open-comments box);
  - List of facilities available for FAA seminars and events;
  - Facility name and type; and
  - Self-portrait image that must be uploaded (optional).

- ***FAASTeam Industry Members (FIM)*** are business entities, such as aircraft and pilots' associations that assist the FAASTeam by sponsoring events in conjunction with the FAA. These entities do not conduct any training or events.

  - Company name;
  - Region;
  - Company address;
  - Authorized company representative's full name (optional);
  - Company representative's job title (optional);
  - Company's website address;
  - Company telephone number;
  - Additional email addresses (optional);
  - Open-text comments box to list areas of expertise (optional); and
  - Facility location(s).

- ***Training Providers*** are individuals or organizations that conduct training under the WINGS – Pilot Proficiency Program and AMT Awards Program.

    - Training provider name;
    - FAA-issued designator code (optional);
    - Mailing address along with country (optional);
    - Training provider website address (optional);
    - Telephone number (optional);
    - Fax number (optional);
    - Training provider contact name; and
    - Training provider contact email address.

- ***Course Authors*** are individuals or organizations that host e-learning courses under WINGS – Pilot Proficiency Program and AMT Awards Program.

    - Organization Point of Contact;
    - Address to include city, state, and zip code;
    - Phone number; and
    - Email address.

Once the application is submitted, it is reviewed by the Program Manager and then sent to the Safety Liaison Team Lead or Site Administrator for approval or denial. Applications are denied for applicants that are not in good standing; for example, they have not completed the required training. FSTW generates an email notification to all individuals informing them of the final decision. All applications follow the same approval process.

FAASTeam members consent to include their contact information in a directory that is publicly available[6]. This directory allows users of FSTW to locate FAASTeam members in their area. This information listed includes the name, position, city, state, zip code, email address, and phone number. Individual members can opt out and in those instances; their information will not be included in the directory.

Safety Program Airmen Notifications System (SPANS)

SPANS is a tool within FSTW that allow FAASTeam Representatives to login and create event announcements or notices detailing upcoming online course, safety seminars and webinars, or safety advisories and alert. The notification provides information such as the location of upcoming events; or advisories or alerts that identity safety concerns. The notification does not include PII. All notices are reviewed by the FAASTeam Program and a Safety Liaison Team Lead or Site Administrator prior to publication on the FSTW. SPANS then disseminates the notification by email to individuals that have sign up to

[6]The directory is available at https://www.faasafety.gov/FAASTApp/directory/default.aspx.

receive the notice. Individual can then register to attend the safety seminar or upcoming event.

Enrollment

The individual name that is associated with account is used for enrollment safety seminars or upcoming event. No additional PII is required for internal course enrollment. Account email address is provided to external course providers during course enrollment for some courses to enable credit validation as part of the Application Programing Interface (API) process.

To enroll or register, the individual selects the online safety course or seminar that they would like to attend. The individual name that is associated with account is used for enrollment in online course and seminars. FAASTeam volunteers and FAA personnel administer the training. Upon completion, the Training Provider, Course Author, Representative, CFI or Program Manager enters the information into a web form or uploads a CSV file containing the activity/course number, account email address of attendees, and the date of completion of individuals that completed the course or attended the seminar or training. This upload can be completed directly within the website or via API. A record of training is listed in the activity history for each attendee. A certificate of completion is generated when an internal course is completed on FSTW. FSTW does not issue certificates for external courses, seminars, webinars, or activities.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[7], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[8].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of

[7] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[8] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

FSTW collects the name, certification number (airmen only), zip code, email address and answers to security question that could be PII from individuals when creating an account. In addition, individuals seeking to become FAASTeam members must complete an application and enter information discussed in the overview section of this PIA. FSTW presents individuals with a Privacy Act Statement that provides notice of the purpose, information being collected, and use of their information prior to collection.

The FAA retrieves system access records in FTSW by name and other identifiers and protect Privacy Act records in accordance with Department published a System of Records Notice (SORN) DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002). The FAASTeam member applications records are also retrievable by name and DOT/FAA 847, *Aviation Records on Individuals* 75 FR 68849 ((November 9, 2010) provides notice to the public of its privacy practices regarding the collection, use, sharing, safeguarding, maintenance and disposal of information.

The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency about its privacy practices to those who use the FSTW.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Individuals voluntarily provide FSTW with their name, zip code, airman certificate number (airman only), CAP ID (United States Air Force CAP personnel only), email address which serves as their username, and password recovery questions and answers which may include PII such as mother's maiden name to create an account. Individuals can navigate to https://www.faasafety.gov to correct or amend their name, zip code, email address and answers to their security questions.

Individuals that would like to become a member of the FAASTeam voluntarily provide the information listed in the overview section of this PIA. FAASTeam industry volunteer members include Representatives, Lead Representatives, FAASTeam Service Providers, Training Providers, Course Authors and FAASTeam Industry Members.

Under the provisions of the Privacy Act, individuals my request searches to determine if any records have been added that may pertain to them. Individuals wishing to know if their records appear in a system may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue (Ave), SW
Washington DC 20591

Included in the request must be the following:

- Name
- Mailing Address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records

Contesting record procedures:

Individuals wanting to contest information about themselves that is contained in FSTW should make their requests in writing, detailing the reasons for why their records should be corrected, to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Avenue (Ave), SW
Washington, DC 20591

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

The following legal authorities authorize FAA's collection of PII belonging to airmen, industry members, and other members of the public:

- *Promotion of civil aeronautics and safety of air commerce:* 49 U.S.C. § 40104 empowers the Administrator to "take action that the Administrator considers necessary to establish, within available resources, a program to distribute civil aviation information in each region served by the Administration."

- *Safety Considerations in the Public Interest:* 49 U.S.C. § 40101 empowers the Administrator of the FAA to "consider the following matters, among others as being in

the public interest…..assigning, maintaining, and enhancing safety and security as the highest priorities in air commerce."

- *Safety-Related Training and Operational Services:* 49 U.S.C. § 44701(a)(5) empowers the Administrator (of FAA) to "promote safe flight of civil aircraft in air commerce by prescribing . . . regulations and minimum standards for other practices, methods, and procedure the Administrator finds necessary for safety in air commerce and national security."

FSTW collects an individual name, zip code, airman certificate number (airman only), CAP ID (United States Air Force CAP personnel only), email address which serves as their username, and password recovery questions and answers which may include PII such as mother's maiden name to create an account. The email address is used to send notification that they have selected to received. The name is used to enroll in upcoming training, online courses, and seminars or webinars they would like to attend. Individuals that would like to become a FAASTeam member provide PII listed in the overview section of the PIA and used in the scope of their duties that include sending out notifications and providing upcoming training, online courses, and seminars & webinars. FAASTeam members can consent to their name, position, city, state, zip code, email address, and phone number made available in a publicly available directory that allow individuals to locate FAASTeam members in their area. Individuals can opt out and in those instances their information will not be included in the directory.

The Civil Aircraft Registry (AVS Registry) provides FSTW the Airman certificate number and ratings, name, email address, airman mailing address and country of origin and that information is used to validate the certification number when an airman creates an account.

Course Authors send FSTW course number (ALC-XXX), email address of attendees, and date individuals completed the course. Training Providers send FSTW the activity number, email address of attendees and date of completion for attendees to allow individual to receive credit for training they have attended. User agreements are in effect for the exchanges of data with the external course providers that use the API process.

FSTW shares the CAP ID, email address, type of activity and activity name, activity number, activity completion date, and latest flight review date to allow safety education and training for their accreditation in the CAP organization. The CAP member must opt in or provide consent for USAF CAP to receive this information otherwise the information is not provided. A CAP member is opted in and provides consent when they provide their CAP ID, listed in their account preferences. A Memorandum of Understanding (MOU) place for this sharing.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

FSTW collects the minimum amount of information that is relevant and necessary to create an account and from individuals wanting to become a FAASTeam member. System access records are maintained in accordance with National Archives and Records Administration (NARA) GRS 3.2, *Information Systems Security Records, Item 30 and* destroyed when business use cease. The FAA Records Office is developing a records retention schedule for airmen and AMT's training records that consist of registration, course names, completion credits and status, completion dates, and hours completed. The records will be maintained as permanent until NARA approves the retention schedule

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

FSTW shares with the Civil Air Portal the CAP ID, email address, type of activity and activity name, activity number, activity completion date, and latest flight review date to allow safety education and training for their accreditation in the CAP organization. The sharing of user account information in the FSTW is conducted in accordance with Department SORN DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002 67 FR 30758. In addition to other disclosures generally permitted under 5 U.S.C. §552(a)(b) of the Privacy Act, all or a portion of the records or information contained in the system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C § 552a(b)(3) as follows:

- To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.
- To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings.
- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records.
- To other government agencies where required by law.

FSTW maintains training records for airmen in accordance with DOT/FAA 847, *Aviation Records on Individuals* . In addition to other disclosures generally permitted under 5 U.S.C. §552(a)(b) of the Privacy Act, all or a portion of the records or information contained in the system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C § 552a(b)(3) as follows:

- Use contact information to inform airmen of meetings and seminars conducted by the FAA regarding aviation safety;

The Department has also published 15 additional routine uses applicable to all DOT Privacy Act systems of records. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, and 77 FR 42796, July 20, 2012, under "Prefatory Statement of General Routine Uses" (available at http://www.transportation.gov/privacy).

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Individuals are responsible for ensuring the accuracy of their information when creating an account and completing an application to become a FAASTeam member. Individuals can navigate to https://www.faasafety.gov to make changes to their name, zip code, email address and answers to their security questions. In addition, that information is validated with airman information received from the AVS Registry into FSTW.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The FAA protects PII by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for Federal Information Systems under the Federal Information System Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, dated September 2020.

The FSTW system has met all requirements and has been certified with an Authority to Operate (ATO) by DOT/FAA. FSTW was granted its ATO on July 21, 2021, after undergoing the National Institute of Standards and Technology (NIST) security assessment and authorization (SA&A). The FSTW system is audited by FAA Security Personnel to ensure FISM compliance through an annual assessment according to NIST standards and guidance.

The FAA has implemented security and privacy controls that fully incorporate administrative, technical, and physical measures to protect users' PII against loss, unauthorized access, and disclosure. Specifically, FSTW takes the following steps to safeguard PII: identification and authentication, physical security, user roles and permissions, and encryption. All users gain access in FSTW by logging in with their account email address and password in the login portal. Passwords are at least eight (8) characters in length, must contain at least one character from all four of the following: Upper case letter, lower case letter, number, and special character, e.g., @, #, %, or *. Passwords must be changed every 90 days. Passwords expire after 90 days of inactivity. User accounts are deactivated upon termination.

Physical security includes physical access and environmental controls in the controlled server center within a secure facility (MMAC) that houses FSTW. Physical access to the FSTW system is limited to designated personnel through photo badges, building key cards, and room-access keypads. FSTW's security measures also included encryption to safeguard PII and other sensitive data both at rest and in transit between FSTW and AVS Registry and USAF CAP as well with other systems with which FSTW connects. FSTW limits access to the data it maintains through user roles and permissions, based on the need to know according to job function. Write access in FSTW is available only to privileged users with approved accounts. All FAA government and contract personnel must complete privacy and security training and must agree to the Rules of Behavior (ROBs), which emphasize privacy protective practices.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FAA Order 1370.121B, FAA Information Security and Privacy Program & Policy, implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, the FAA will implement additional policies and procedures as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with the FSTW are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy training awareness training, as well as FAA Order 1370.121B. The FAA will conduct periodic privacy compliance reviews of the FSTW as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Anthony D'Angelo
System Owner
National Administrator, FAAST Team

Prepared by: Barbara Stance

Approval and Signature

Karyn Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer