



U.S. Department of Transportation
Privacy Impact Assessment
Federal Aviation Administration (FAA)/
Air Traffic Organization (ATO)

Future Flight Services Program (FFSP)

Responsible Official

John Hudy
In-Service Group Manager, AJR-B2
202-267-6447

Reviewing Official

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





Executive Summary

The FAA's Future Flight Services Program (FFSP) system promotes safety by facilitating the filing of flight plans, providing weather briefings, and receiving safety notifications and alerts relevant to the flight plans filed by the General Aviation (GA) pilot.

The FAA developed this Privacy Impact Assessment (PIA) in accordance with Section 208 of the E-Government Act of 2002 because FFSP collects and processes Personally Identifiable information (PII) such as the pilot's name, address, email address, phone number, flight plan information, aircraft identifier, username/login name, password, home airport location, emergency contact information, pilot certification type (student, commercial, etc.), call detail records including date, time, and caller ID, and voice recordings via NICE voice recording system. PII may also be included from incoming preflight calls, outgoing emergency services calls, connecting pilots or other external users and specialists.

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.¹

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

¹Office 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).



- *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](#) outlines the authority given to the FAA to carry out safety programs under the FFSP to ensure the safest, most efficient aerospace system in the world. The FAA is responsible for the following:

- 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.

Description of System:

FFSP is a National Airspace System (NAS) support system under FAA/Air Traffic Organization's Flight Service. FFSP, previously named the Flight Service for the Twenty-First Century (FS21) system, is operated by Leidos, an FAA contractor. The primary role of FFSP is to provide weather data, aeronautical information, and flight planning services to general aviation (GA) pilots, which enables pilots to readily have the information available to make better decisions and improve aviation safety. Future Flight Service provides these services through:

- a) Direct voice-services contact, by either telephone or radio, with a certified FAA flight service specialist that translates weather and aeronautical data into critical and comprehensible information tailored for flight.



- b) Automated online web portals provides GA pilots access to weather and aeronautical data and the ability to file flight plans without speaking to a flight specialist.

FFSP maintains pilot profile information for system user validation, as well as to contact the pilot in the event of an emergency (i.e., if a pilot does not reach their destination within 30 minutes of the expected arrival time, Flight Service will begin attempting to call the pilot and contact authorities if necessary). Filing a flight plan for Visual Flight Rules (VFR) flights is optional. Filing a flight plan is required for Instrument Flight Rule (IFR) flights.

There are two methods of communicating with Flight Service: contacting the call center by phone or radio, or self-assisted via the online portal. To contact Flight Service, a pilot can log onto <https://www.1800wxbrief.com> or call 1-800-WXBRIEF.

If a pilot decides to log onto the online portal, <https://www.1800wxbrief.com> to communicate with Flight Services, the pilot is required to create an online account. To create an account and receive a username and password, the pilot must provide an email address, last name or organization, Aircraft ID (optional), phone number, and home base phone number. Once a username and password are provided and the pilot has access to the online portal, the pilot must enter their name, address, email address, phone number, flight plan information, aircraft identifier, username/login name, password, home airport location, emergency contact information, pilot certification type (student, commercial, etc.), call detail records including date, time, and caller ID, and voice recordings (via [NICE](#) voice recording system). Recordings may include Aircraft Identification (N-Number), Specialist Operating Initials and may contain other PII included at the speaker's discretion from members of the public comprising the GA community, such as pilots.

If a pilot decides to use the call-in option at 1-800-WXBRIEF, the pilot is greeted by an FAA certified flight service specialist. The same information must be provided to the FAA certified flight service specialist. The specialist then enters the information into FFSP directly.

PII from incoming preflight calls, outgoing emergency services calls, connecting pilots or other external users and specialists are recorded, and these recordings could include PII. PII contained in recordings could include the Aircraft Identification (N-Number) and specialist operating initials, as well as other PII at the speaker's discretion.

When a pilot contacts Flight Service via voice or online, the following flight plan information is requested: aircraft ID, flight rules (VFR/IFR), flight type, number of aircraft, aircraft type, wake turbulence, aircraft equipment, departure airport, departure date & time, cruising speed, altitude, surveillance equipment, route of flight, destination airport, expected flight duration, fuel endurance, persons on board, emergency radio type, survival equipment, jackets, and pilot contact information.



A pilot's PII is entered into the FFSP system by an FAA Flight Specialist over the telephone, or the individual creates a Pilot Web account and enters their information manually.

FFSP collects information to facilitate the GA pilot to file flight plans, receive weather briefings, and/or receive safety notifications and alerts relevant to the flight plans filed by the pilot. The pilot's name and certificate type are collected to verify the individual's identity and match the correct flight plan with the individual. The pilot's contact information, such as telephone number and address, are also used to provide communications updates and safety-related services to the pilots.

Information in FFSP is used internally by Flight Service for data metrics (i.e., pre-flight call patterns to determine future staffing levels) and search and rescue.

At any time, individuals registered with the FFSP system may request changes to their user profiles by calling 1-877-377-3721 or logging into their Pilot Web account.

Information that pilots receive when communicating with Flight Service includes airmen's meteorological information (AIRMET) reports, pilot reports (PIREPs), Notices to Air Missions (NOTAMs), temporary flight restrictions (TFRs), radar and satellite weather reports, current weather conditions, weather forecast, recommended altitude, and winds aloft.

FFSP is a distributed system comprised of two operational facilities (Ashburn, VA & Fort Worth, TX) distributed within the contiguous U.S. (CONUS), interconnected by a Wide Area Network (WAN). Each facility hosts approximately 100 Flight Service Specialists that provide telephone or radio-based support to pilots. The provision of flight services is accomplished by employing three major functions of the FFSP system:

- Flight planning and weather briefing
- Voice and data communications
- Data management

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)



v3², 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 Organizations³.

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 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.

The FAA takes steps to ensure transparency to the general aviation community and ensure that pilots are aware that FFSP maintains pilot profile information for system user validation and to contact the pilot in the event of an emergency.

FAA utilizes a self-assisted online portal at [Flight Service](#), where pilots can update their information. FAA also maintains the phone line at 1-800-WXBRIEF that pilots can use to contact Flight Services to update their information in FFSP. FFSP system provides automated notice and consent, and Flight Service specialists are required to ask for and receive a pilot's verbal consent before including the pilot's PII in a flight plan. The recordings are specific to the facility and are not maintained by Flight Service personnel or within the FFSP system boundary. The voice recordings are a part of the overall system boundary.

The DOT/FAA 847, [Aviation Records on Individuals](#), 75 FR 68849 (November 9, 2010) System of Records Notices (SORN) provides transparency as to how the FAA processes and maintains pilot information, while the DOT/ALL 13, [Internet/Intranet Activity and Access Records](#), 67 FR 30757 (May 7, 2002) SORN provides transparency as to how the FAA processes and maintains information related to FFSP access.

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.

² <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

³ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf



FFSP collects information to facilitate a GA pilot's filing flight plans, receiving weather briefings, and/or receiving safety notifications and alerts relevant to the flight plans filed by the pilot. To do so, FAA affords pilots two mechanisms through which they can submit their information or correct their information. First, FAA Flight Specialists collect PII directly from pilots over the telephone and manually enter it into FFSP. FAA Flight Specialists must request and be granted consent from a pilot before including the pilot's PII in the flight plan information in FFSP. In addition, a pilot may create their own Pilot Web account and enter their information manually into FFSP at any time. Pilots can update their profile information via the self-assisted online portal or calling Flight Service.

Under the provisions of the Privacy Act, individuals may request searches of the FFSP flight plan database to determine if any records pertain to them by sending a written request directly to the Flight Service Program Office containing the requestor's name, verification information, and information regarding the request. They may also request amendment of records they believe are not timely, relevant, accurate, or complete.

As described in DOT/FAA 847, [Aviation Records on Individuals](#), 75 FR 68849 (November 9, 2010), individuals with questions about privacy and Flight Service should contact the FAA directly. For inquiries, a letter should be sent to the System Manager at the address specified below:

John Hudy
Flight Service Program Operations
Federal Aviation Administration
800 Independence Avenue, SW
Washington, DC 20591

Individuals with concerns about privacy regarding Flight Service may also email the FAA Privacy Officer via the contact information provided in the privacy policy on the FAA's website (www.faa.gov/privacy).

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 authority for the collection of the information within the FFSP system is 49 U.S. Code §§ 40102 and 40103, which provides the FAA authority to ensure safety in the National Airspace.

The FAA is responsible for maintaining records on individuals in connection with FAA's oversight and enforcement of safety regulations as described in DOT/FAA 847. To that end,



FFSP collects information necessary to identify individuals for search and rescue and accident investigation purposes. Information will be used consistent with the purposes for which it was collected.

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.

DOT requests the minimum amount of information necessary to meet the statutory requirements FFSP is designed to fulfill. FFSP collects and retains information from the pilot such as name, basic contact information, emergency contact information, flight plan information, and other information described previously in the Introduction & System Overview section.

Flight Service records are scheduled under National Archives and Records Administration (NARA) Schedule Reference Number DAA-0237-2020-0027. The disposition for this schedule is three years after the cutoff of the end of the contract. The flight plans in FFSP containing PII data are maintained for the required three (3) years to perform services to registered pilots operating with the system. Voice recordings are retained for 45 days.

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.

The use of PII in FFSP records is limited to Search and Rescue (SAR) and accident investigation purposes and the routine uses identified in DOT/FAA 847, [Aviation Records on Individuals](#), 75 FR 68849 (November 9, 2010). Specifically, records are shared by the FAA Flight Services Quality Assurance Specialist upon formal request from law enforcement, SAR agencies, and/or the DOT/FAA organization responsible for accident investigations.

Routine uses include:

- a. Provide basic airmen certification and qualification information to the public upon request
- c. Disclose information to the National Transportation Safety Board (NTSB) in connection with its investigation responsibilities.
- d. Provide information about airmen to Federal, State, local and Tribal law enforcement agencies when engaged in an official investigation in which an airman is involved.
- n. Provide information about airmen to Federal, State, local, and Tribal law enforcement, national security or homeland security agencies whenever such agencies are engaged in the performance of threat assessments affecting the safety of transportation or national security.



Unless there is a formal data request from law enforcement personnel, the information is needed for a SAR, quality assurance, or an accident investigation, the PII contained in the FFSP flight plan is not used by other applications or systems or included in any reports unless there is a trouble-ticket issue.

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).

The PII required in FFSP flight plans is provided verbally by the pilot and entered into the system by the Flight Service Specialist or by obtaining an account on the 1800wxbrief.com website. Voice recordings (VRs) of pilot-specialist interaction are stored for 45 days. When flight plan PII is changed, FFSP maintains a copy of the flight plan and records which Flight Service Specialist made the changes. FFSP stores flight changes to the flight plan as amended flight plans. Amended flight plans can be retrieved from the FFSP database by the LFS specialist if required. The accuracy of the PII data is dependent on both the pilot and the LFS specialist. Flight Service personnel can retrieve stored VRs to review pilot information; however, there is no means available to validate the accuracy of the data.

At any time, individuals registered with the FFSP system may request changes to their user profiles by calling 1-877-377-3721 or logging into their Pilot Web account.

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). The safeguards 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.

FFSP received its authority to operate 03/05/2021. Access to FFSP is limited to authorized personnel only. Access to Flight Service facilities is restricted using a combination of physical and logical access controls (e.g., fences, badge/card readers with keypads, visitor



control, closed-circuit TV). In addition to physical and logical access control, FFSP limits access to PII according to job function.

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 FFSP 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 FFSP as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

John Hudy
In-Service Group Manager, AJR-B2
Federal Aviation Administration

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer