



U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Information & Technology Services (AIT)

Service Now Information Technology Services

Management System (Service Now ITSM)/ MyIT Service Center

Responsible Official

Christopher Logan

Email: christopher.j.logan@faa.gov

Phone Number: 210-763-7059

Reviewing Official

Karyn Gorman

Chief Privacy Officer

Office of the Chief Information Officer





Executive Summary

The Federal Aviation Administration (FAA) Office of Information & Technology Services (AIT) uses the Service Now Information Technology System Management (Service Now ITSM) platform as a service (PaaS) to provide IT support services to FAA employees, contractors, and members of the public. Service Now ITSM includes the FAA's MyIT Service Center, which supports the FAA's operational mission by enabling the effective use of IT resources, which is consistent with FAA policy pursuant to 49 United States Code (USC) 40101, *Policy* and 49 USC 322, *General Powers*.

Under the E-Government Act of 2002, the FAA developed this Privacy Impact Assessment (PIA) because the MyIT Service Center collects Personally Identifiable Information (PII) on members of the public, such as pilots or designees who request these IT support services. This PIA addresses only the use case of external individuals seeking IT support services from the FAA.

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:

- *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;*

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).



- *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 FAA uses the Service Now ITSM platform as a service (PaaS) to provide internet technology (IT) support services to FAA employees, contractors, and members of the public. Service Now ITSM includes the FAA's MyIT Service Center, which supports the FAA's operational mission by enabling the effective use of IT resources. This PIA addresses the use of the MyIT Service Center by members of the public accessing FAA IT resources.

Members of the public occasionally have a need to access FAA IT resources, such as the FAA's Pilot Records Database (PRD) to view their PRD Airmen Record (PAR) or the MedXPress system that allows airmen to request FAA medical clearances. If these individuals have difficulties with accessing systems or require password resets, they can contact the MyIT Service Center via phone or e-mail. For the FAA to provide these services, the external individuals may provide their name, email address, phone number for call back, and the application the individual has or needs access to. In the case of email, the individual could also voluntarily provide an attachment or information in their email signature.

Once the issue has been expressed, the FAA MyIT Service Center analyst manually types the name, email address, phone number, and application they have access to into the MyIT Service Center electronic interface. A system-generated Request ID is displayed to the analyst via a pop-up box and can be shared via email or verbally to the external user. The Analyst then takes action to resolve the issue, which may include calling or emailing the customer to obtain further details or clarification (such as the numerical name for the customer's computer, or their Internet Protocol (IP) address). Once the issue is resolved, the analyst may email the customer from their own @faa.gov email address. In doing so, PII regarding the analyst may be included, such as their full name, government email address, and any information in their email signature (such as office location, routing code, and government/personal cell phone number). Reports (including call log data such as phone numbers) are saved by the FAA's contractor on a secure Amazon Web Services mid server.



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 employs multiple techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains PII within the MyIT Service Center. Information collected from external users is stored in a guest record and retrieved by ticket number. The FAA does not save external users' information in a specific user record. Therefore, no Privacy Act System of Record Notice (SORN) is required for the external users' functionality provided by the MyIT Service Center. The FAA does not make disclosures of external users' records from the MyIT Service Center.

Computer access records of FAA employees and contractors who staff the MyIT Service Center are maintained in accordance with the Department's Privacy Act System of Records Notice (SORN), [DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30758 \(May 7, 2002\)](#).

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

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



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.

The FAA does not make Privacy Act disclosures of external users' records out of the MyIT Service Center. If an external user calls or emails the MyIT Service Center and provides their ticket number to a MyIT Service Center analyst, they can update the PII on that ticket record.

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.

External individuals provide the FAA with their names, email addresses, and phone numbers for the purpose of receiving requested IT support services. The FAA collects this information in the MyIT Service Center, and the information stored therein under the following authorities:

- 1) Title 49 United States Code (U.S.C.) § 40101, Policy, which covers matters relating to the public interest and consistent with public convenience and necessity.
- 2) 49 U.S.C. § 322, General Powers, which requires the Department of Transportation Secretary to carry out aviation duties and powers.

System access and authentication records of FAA employees and contractors who support the MyIT Service Center are used by the FAA consistent with the purposes for which it was collected as described in DOT/ALL 13, "Internet/Intranet Activity and Access Records", 67 FR 30758 (May 7, 2002). Specifically, to manage IT system services.

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.

The FAA minimizes its data maintenance, use, and retention in the MyIT Service Center to the relevant and necessary information to meet its authorized business purpose of providing IT support services to FAA employees, contractors, and members of the public. Records within the MyIT Service Center are maintained pursuant to [General Record Schedule 5.8, Administrative Help Desk Records](#). Records are temporary and are destroyed one year after resolved, or when no longer needed for business use. System access and authentication records are maintained pursuant to [General Record Schedule 3.2, Information Systems](#)



Security Records. These records are temporary and can be destroyed when business use ceases.

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 external individual seeking IT support services provides their name, email address, and phone number specifically for the purposes of identity verification and the provision of the requested IT services. External users' PII is not maintained pursuant to the Privacy Act. The FAA does not disclose external users' PII from the MyIT Services Center.

Logging information from FAA employees and contractors is used as specified by the DOT's system of records notice, [DOT/ALL 13, Internet/Intranet Activity, and Access Records](#). In addition to other disclosures generally permitted under 5 U.S.C. §552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use under 5 U.S.C. § 552a(b)(3) as follows:

- To provide information to any person(s) authorized to assist in approved investigations 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 negation 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; and
- To other government agencies where required by law.

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).

External individuals seeking IT support are responsible for accurately providing their name, email address, and phone number to the MyIT Service Center analyst via phone. Field restrictions help ensure accuracy for Analysts who manually enter those data elements into the MyIT Service Center. External users who provide information via email are responsible for the accuracy of the data they are emailing.



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 with 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 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 NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated August 4, 2022. The MyIT Service Center implements administrative, technical, and physical measures to protect against loss, unauthorized access, or disclosure. The principle of least privilege is used to grant access to FAA federal employees and contractors, and user actions are tracked in the audit logs.

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.

The FAA's Information Security and Privacy Service (AIS), Security Governance Division is responsible for the administration of FAA Order 1370.121B, "FAA Information Security and Privacy Program & Policy." FAA Order 1370.121B defines the various privacy requirements of the Privacy Act of 1974, as amended (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the Federal Information Security Management Act (FISMA), DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information technology management policies and procedures. In addition to these, other policies and procedures will be consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance on their duties related to collecting, using, processing, and securing privacy data. Guidance is provided through mandatory annual security and privacy awareness training. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of the MyIT Service Center relative to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource OMB Circular A-130, *Managing Information as a Strategic Resource*.



Responsible Official

Christopher Logan
System Owner
Division Manager, Service Optimization Division

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN
MARIE
GORMAN

Digitally signed
by KARYN MARIE
GORMAN
Date: 2026.09.25
15:48:01 -04'00'

DOT Privacy Office - Approved - 09/25/2026



DOT Privacy Office - Approved - 09/25/2026