U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration

Federal Aviation Administration Management Information System

FAAMIS

Responsible Official

Brenda Bailey
Email: Brenda.Bailey@faa.gov
Phone Number: (717) 712-1018

Reviewing Official

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

Executive Summary

The Federal Aviation Administration Management Information System (FAAMIS) serves as a central repository and is used by Aviation Safety Inspectors (ASIs) and support personnel to conduct queries to retrieve reports on results of inspections related to aviation safety for air carriers, air agencies, aircraft incidents, and other aviation entities and activities. FAAMIS is also used to gather information when responding to internal and external requests such as Freedom of Information Act (FOIA), background and statistical information to Federal Aviation Administration (FAA) Office of the Chief Counsel for their use in litigation procedures, and background and statistical information for Congressional inquiries or in support of the U.S. General Accounting Office (GAO) audits. FAAMIS is owned and operated by the FAA Office of Aviation Safety (AVS) System Approach for Safety Oversight (SASO) Program Office, Automation and Policy Team (AFS-910) and operates under Title 49 United States Code (U.S.C.) § 40101, 49 U.S.C. § 40113, 49 U.S.C. § 44701, and 49 U.S.C. § 44702.

This Privacy Impact Assessment (PIA) was conducted pursuant to the E-Government Act of 2002 because FAAMIS maintains exact copies of records that are received from FAA systems discussed in the Overview section of this PIA. FAAMIS maintains Personally Identifiable Information (PII) about air carriers, air agencies, designated airmen, and check airmen that include name, address, airmen certification number, date of birth, and other PII discussed in the PIA.

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 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]

[1]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).

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;*
- *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, as amended, gives the Federal Aviation Administration (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 System Approach for Safety Oversight (SASO) Program Office has been given the responsibility to carry out safety programs to regulate the aviation industry. FAAMIS supports Flight Standards Service (AFS) to conduct job functions by maintaining information on entities such as air carriers[2], air agencies[3], designated airmen[4], and check airmen. The three main components of FAAMIS are as follows:

- National Vital Information System (NVIS) is the official repository for information about air operators, fractional ownership programs, air agencies, designees, check airman, Organizational Designation Authorization (ODA), and other certified and non-certified activities.

[2] An air carrier is a person who undertakes directly by lease, or other arrangement, to engage in air transportation.
[3] An air agency is a company or agency authorized to sell and arrange air transportation of persons and cargo.
[4] A flight engineer designated to conduct certification within a specifically approved Aircrew Designated Examiner (ADE) program.

- National Program Tracking and Reporting (NPTRS) is a repository of data resulting from the many different job functions and activities performed by ASIs. It provides:
    - An automated method of collecting data resulting from inspector work activities;
    - A structured means of entering observations, evaluations and opinions into NPTRS;
    - A data-storage method that permits pattern detection or identification of problem areas; and
    - An efficient method of data distribution, an automated, flexible capability to retrieve data, and an analysis capability to identify system problem areas that affect aviation safety.

  NPTRS has various retrieval and reporting features that allows users managers to compile and plan work programs, prioritize activities and specific job tasks, and analyze the safety and compliance status of various elements throughout the air transportation industry. Reporting includes responding to FOIA requests, providing background and statistical information to FAA's Office of the Chief Counsel for their use in litigation procedures, and providing background and statistical information for Congressional inquiries or in support of the U.S. GAO audits.

  NPTRS uses FAA Form 8000-36 Program Tracking and Reporting System Data Sheet to record the inspector's work activities. This form has spaces for entering information that describe the type of job function performed, personnel involved (if pertinent to the job function), and the results of that activity, including any inspector comments and opinions. The following PII is entered:

    - Airman Certificate Number
    - Name
    - Examiner Number
    - Applicant Number
    - Current Personnel Field (name, position, and base)
    - Recommending Instructor

- Complexity is a pay grade calculation tool that is used to determine ASI's pay level. Complexity creates reports by using the information in the NVIS to compute the value of aviation organizations assigned to a certificate management inspector as it relates to the position grade level classification. Complexity reports can be on an inspector, job specialty, field office, or region and the report may contain the full name of the ASI, job title, office designator, mailing address, airman certificate number, work assignments, job specialty, office, region, and work product.

FAAMIS does not collect data from individuals but receives the following PII from Enhanced Flight Standards Automation System (eFSAS)[5] and Safety Analysis System

[5] eFSAS is schedule to be decommission around November 2024 and the functionality of this system will be replaced by SAS.

(SAS) to conduct queries and to gather information when responding to internal and external requests:

• Airmen's name, certificate number[6], certificate type, rating type, business and home address, business and personal telephone number, business and personal email address and status (active/inactive)
• Instructor name
• Designator examiner number
• Designee number
• Flight Inspector number
• Pilot training records (type of training the pilot has completed)
• Account Manager's name, work contact information (phone number, address and email address)
• Chief Executive Officer's (CEO) work contact information (phone number, address and email address)
• Company Authorized Point of Contact (POC) full name, job title and telephone number
• Name of Company/Doing business as (DBA), business address and telephone number
Aircraft owner full name and address
• Previous aircraft owner full name and address
• Aircraft serial number
• Aircraft manufacturer name
• Aircraft make/model/series
• Engine manufacturer name
• Engine make/model/series

FAAMIS also receives from eFSAS and SAS witness statements from ASI reports pertaining to an aircraft accident or incident. The witness statement may contain personal contact information that includes names, telephone numbers, email addresses, mailing addresses, and airman certificate numbers.

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

[6] In some instance this may be an airmen social security number. The Civil Aviation Registry discontinued the practice of using the SSN as a certificate number for original or new certificates in June 2002. A small number of airmen have kept their SSN as their certificate number for their convenience.
[7] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

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 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.

FAAMIS maintains copies of records from source systems that are subject to the Privacy Act. eFSAS and SAS systems, the source systems, are subject to the DOT's published system of record notice (SORN) DOT/FAA 847, Aviation Records on Individuals, November 9, 2010, 75 FR 68849 which provides notice of the privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal. Therefore, the copies maintained in FAAMIS are protected in accordance with DOT/FAA 847, Aviation Records on Individuals, November 9, 2010, 75 FR 68849. The FAA retrieves system access records in FAAMIS by name and protects those Privacy Act records in accordance with Department's published SORN DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002 67 FR 30757.

The publication of this PIA demonstrates DOT's commitment to provide additional transparency into FAAMIS.

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.

FAAMIS maintains copies of records received from eFSAS and SAS. Individuals have rights of correction, amendment, or deletion of their Privacy Act information. Under the provisions of the Privacy Act, individuals may 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:

[8] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

Federal Aviation Administration
Privacy Office
800 Independence 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

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

Federal Aviation Administration
Privacy Office
800 Independence 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 FAA uses the copies of records maintained in FAAMIS pursuant to the following legal authorities:

Title 49 United States Code (U.S.C.) § 40101, Policy, (a) Economic Regulation – "the Secretary of Transportation shall consider the following matters…(1) assigning and maintaining safety as the highest priority in air commerce, (2) before authorizing new air transportation services, evaluating the safety implications of those services, (3) preventing deterioration in established safety procedures, recognizing the clear intent, encouragement, and dedication of Congress to further the highest degree of safety in air transportation and air commerce, and to maintain the safety vigilance that has evolved in air transportation and air commerce and has come to be expected by the traveling and shipping public." FAAMIS allows AFS to maintain aviation safety through supporting information sharing related to the certification and oversight of the individuals and organizations described in this document.

49 U.S.C. § 40113, Administrative, (a) General Authority – "(…with respect to aviation safety duties and powers designated to be carried out by the Administrator) may take action the Secretary, Under Secretary, or Administrator, as appropriate, considers necessary to carry out this part, including conducting investigations, prescribing regulations, standards, and procedures, and issuing orders." FAAMIS allows AFS to promote aviation safety through supporting information sharing related to the certification and oversight of the individuals and organizations described in this document.

49 U.S.C. § 44701, General requirements, (a) Promoting Safety – "The Administrator of the Federal Aviation Administration shall promote safe flight of civil aircraft in air commerce by prescribing...(2) regulations and minimum standards in the interest of safety for (A) inspecting, servicing, and overhauling aircraft, aircraft engines, propellers, and appliances; (B) equipment and facilities for, and the timing and manner of, the inspecting, servicing, and overhauling; and (C) a qualified private person, instead of an officer or employee of the Administration, to examine and report on the inspecting, servicing, and overhauling." Information within FAAMIS is used to track and manage designees and aviation safety-related inspections, including monitoring renewal dates and training requirements.

49 U.S.C. § 44702, Issuance of certificates, (a) General Authority and Applications – "The Administrator of the Federal Aviation Administration may issue airman certificates, design organization certificates, type certificates, production certificates, airworthiness certificates, air carrier operating certificates, airport operating certificates, air agency certificates, and air navigation facility certificates under this chapter." FAAMIS supports AFS's ability to track activities related to the certification of these entities.

49 U.S.C. § 44702, Issuance of Certificates, (d) Delegation – "Subject to regulations, supervision, and review the Administrator may prescribe, the Administrator may delegate to a qualified private person, or to an employee under the supervision of that person, a matter related to— (A) the examination, testing, and inspection necessary to issue a certificate under this chapter; and (B) issuing the certificate." FAAMIS supports AFS's ability to track the activities of designees and ODAs who perform these functions.

FAAMIS receives information from eFSAS and SAS as discussed in the Overview section of this PIA. FAAMIS shares all information with the AVS Replication Server, a component of AIT Enterprise Data Centers (AIT EDC). The sharing of the information provides a central service for the control and of these records to other authorized FAA systems. See the AIT EDC PIA published at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments for a full discussion of this process.

AVS Registry[9] sends FAAMIS unique identification, optional social security number, full name, date of birth, height, weight, hair color, eye color, gender, citizenship, region, medical identification number, medical path number, medical application identification number, business email address, mailing address, designated examiner number, FAA inspector number, flight instructor number, physical address, N-Number, and serial number. FAAMIS stores the information on the FAAMIS server for validation purposes only. This information is not available to FAAMIS users, and not shared with other systems.

Federal Aviation Administration Directory Services receives from FAAMIS FAA employee and contractor email address via Hyper Text Transfer Protocol Secure (HTTPS). The purpose of this data exchange is to authenticates FAA employees and contractors for access to FAAMIS.

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 FAAMIS to the information that is relevant and necessary to meet its authorized business purpose. Records are maintained in accordance with National Archive and Records Administration Records Schedule DAA-0237-2022-0005 approved November 7, 2022. NVIS records are destroyed 3 years after cutoff. NPTRS records are destroyed 30 years after the last activity of the certificated entity to which they are related. All other records maintained in FAAMIS are records copies from other FAA systems and are maintained in accordance with General Records Schedule (GRS) 5.1, *Common Office Records,* approved July 2017. Records can be destroyed immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use. System access records are maintained in accordance with NARA General Records Schedule (GRS) 3.2, approved January 2023 and are 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.

FAAMIS does not share information with external systems. DOT discloses information with the source systems eFSAS and SAS outside DOT in accordance with DOT/FAA 847, "Aviation Records on Individuals," 75 FR 68849 (November 9, 2010). In addition to other

[9] PIA for this system is available at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

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 FAAMIS may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) to:

- Disclose information to the NTSB in connection with its investigation responsibilities.
- 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.
- Make airman, aircraft and operator record elements available to agencies relating to aviation events including the Department of Defense, the Department of Homeland Security, the Department of Justice and other authorized government users, for their use in managing, tracking and reporting aviation-related security events.

The sharing of user account information in the FAAMIS is conducted in accordance with SORN DOT/ALL 13, "Internet/Intranet Activity and Access Records", 67 FR 30758 (May 7, 2002). 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.

DOT may also disclose information outside DOT pursuant to 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), 77 FR 42796 (July 20, 2012).and October 15, 2019, under "DOT General Routine Uses" (available at http://www.transportation.gov/privacy/privacyactnotices).

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).

FAAMIS receives copies of records from eFSAS and SAS systems and it is the responsibility of each source system to ensure the accuracy of the data being transferred to FAAMIS. The information in FAAMIS is overwritten by the information in the source systems on a regular basis.

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.

FAAMIS has met all requirements and has been certified with an Authority to Operate (ATO) by DOT/FAA. FAAMIS was granted its ATO on April 25, 2023, after undergoing the National Institute of Standards and Technology (NIST) security assessment and authorization (SA&A). FAAMIS is audited by FAA Security Personnel to ensure Federal Information Security Management Act of 2002 (FISMA) compliance through an annual assessment according to NIST standards and guidance.

Access to FAAMIS is limited to authorized staff members and support personnel. Physical access to the FAAMIS system is limited to authorized personnel. FAA and support personnel with physical access have all passed DOT background checks.

In addition, FAAMIS audits domain account changes (creation, modification, disabling, and termination) and changes to data, office codes, date ranges, and time stamps. Authorized users review the Errors/Audit File function on a regular basis to find discrepancies. In cases

of suspicious activity, FAAMIS personnel can support investigative activities through review and analysis of the audit log files. Through audit log file review, FAAMIS System Owners can also support investigative requests coming from FAA's Legal or Security Departments, U.S. Congress, and other organizations. FAAMIS is responsible for identifying, training, and holding FAAMIS users accountable for adhering to privacy and security policies and regulations.

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

Responsible Official

Brenda Bailey
System Owner
IT Specialist, ADE-540

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer