U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Flight Standards Automation System/Technical Analysis Program (FSAS/TAP)

Responsible Official

Lawrence Wade
Email: helpdesk@faa.gov
Phone Number: 844-FAA-MYIT

Reviewing Official

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

Executive Summary

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 developed the Flight Standards Automation System/Technical Analysis Program (FSAS/TAP) to comply with the Federal Aviation Act of 1958, as Amended. FSAS/TAP is a web-based application that is used by Flight Standards Service (AFS) Managers, Aviation Safety Inspectors (ASIs), and support personnel in all Flight Standards District Offices (FSDO) to run data quality reports related to FAA safety inspector functions and verify the accuracy of aviation safety data including airmen and aircraft information. Authority to operate the system is governed by 14 CFR Part 39 and 49 U.S.C § 44701.

The FAA is publishing this Privacy Impact Assessment (PIA) for the FSAS/TAP in accordance with Section 208 of the E-Government Act of 2002 because the system receives Personally Identifiable Information (PII) from airman, aircraft owners, employees of airlines, air operators, or air agencies. The system also collects and maintains the PII of FAA employees and FAA contractors.

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

[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).

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.

FSAS/TAP is an internal, web-based application, available on the FAA intranet.

AFS Managers, ASIs and support personnel in all FSDOs use FSAS/TAP to run data quality reports related to FAA safety inspector functions and verify the accuracy of aviation safety data including airmen and aircraft information.

Users, who consist of FAA employees and contractors, access FSAS/TAP at https://analysis.avs.faa.gov/analysisnet using their Personal Integrated Verification (PIV) card. Once users are logged into FSAS/TAP, the homepage displays a wealth of options for

the user to explore. The user selects the subject area they are analyzing to conduct a query. FSAS/TAP through the Aviation Safety (AVS) Replication Server[2] receives replicated information from Federal Aviation Administration Management Information, Enhanced Flight Standards Automation System and the Enforcement Information System to generate reports that pertains to the subject area being analyzed. FSAS/TAP only displays the reports, and the reports are not saved in FSAS/TAP. The reports generated through this system are used to prepare data quality reports related to FAA safety inspector functions and verify the accuracy of aviation safety data, including airmen and aircraft information. The reports contain the following information:

Members of the Public

- Airman's full name
- Airman's Unique ID
- Airman Certificate Number
- Type of Certificate
- Airman's Social Security Number
- Aircraft Owner name and personal address
- Violator name, personal address and telephone number
- Doing Business As Name
- Aircraft Registration Number

FAA Employee and Contractors

- AVS User ID
- Inspector Name
- Inspector Code
- Inspector Specialty
- Inspector Type
- Assigned Office
- Business Phone

[2] The AVS Replication Server, a component of AIT Enterprise Data Centers (AIT EDC). PIAs for AIT EDC and other systems who information is transfer through the AVS Replication Server, will be published at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments for a full discussion of the system process. The AVS Replication Server at some point will be decommissioned and functions will be taken over by the Enterprise Management System Platform.

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[3], 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[4].

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.

FSAS/TAP does not collect information directly from individuals but displays read-only data that it receives from the AVS Replication Server. Therefore FSAS/TAP is not Privacy Act System of Records. Individuals are notified when the source systems initially collect the information, to the extent the source system is a Privacy Act system of records and if the FAA collects information directly from the individual.

System access records that the FAA maintains on FAA employees and contractors are considered Privacy Act records; therefore, the Department of Transportation has published the System of Record Notice DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002).

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the FSAS/TAP.

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

[3] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[4] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

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.

FSAS/TAP does not collect information directly from individuals but displays read-only data that it receives from the AVS Replication Server. For an individual to correct or amend their records, they must go back to the original point of collection.

Under the provisions of the Privacy Act, individuals may request searches of their information maintained in the source systems to determine if any records have been added that may pertain to them and if such records are accurate.

For all inquiries related to the information contained in the source system, the individual may appear in person, send a request via email (privacy@faa.gov), or in writing to:

Privacy Office

800 Independence Avenue, SW

Washington, DC 20591

The request must include the following information:

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

If you have comments, concerns, or need more information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.

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 FAA's central mission is to promote safety in civil aeronautics. To achieve this, the agency establishes regulatory standards and requirements, found in 14 Code of Federal Regulations (C.F.R.) parts 14 CFR Part 39 and 49 U.S.C § 44701. The PII in FSAS/TAP is

used to query information for the purpose of running aviation safety inspection reports and verifying the accuracy of aviation safety data, including airmen and aircraft information.

FSAS/TAP receives information from the AVS Replication Server which is discussed in the Overview section of this PIA. In addition, FSAS/TAP sends the FAA Directory Service (DS) user's name and receives an access token from FAA DS to grant users access to FSAS/TAP.

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.

FSAS/TAP receives read-only information discussed in the Overview section of this PIA. Those records are maintained in accordance with *GRS 5.1, Item 20, "Non-recordkeeping copies of electronic records"* and records are 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 *GRS 3.2, Item 30 "System Access Records"* 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.

The PII in FSAS/TAP is used only to query information for the purpose of running aviation safety inspection reports and verifying the accuracy of aviation safety data, including airmen and aircraft information. The FAA does not use the PII for any other purpose, and any PII disclosures that might appear in this system are in fact in the source system.

System access records maintained about FAA employees and contractors are managed in accordance with SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002).

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).

FSAS/TAP only displays read-only data that is received from the AVS Replication Server but does not save the information. The accuracy of the information is dependent on the source system that the information is retrieved from.

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 Federal Information Security 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 the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* dated September 2020 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of the FSAS/TAP to test security processes, procedures and practices. The system operates on security guidelines and standards established by NIST and only FAA personnel with a need to know are authorized to access the records in FSAS/TAP. All data in-transit is encrypted and access to electronic records is controlled by PIV and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessment to test and validate security process, procedures and posture of the system.

Based on the security testing and evaluation in accordance with the FISMA, the FAA issues FSAS/TAP an on-going authorization to operate. The Authority to Operate was issued August 25, 2023.

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.

DOT implements 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.

In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with FSAS/TAP 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 awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of FSAS/TAP as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Lawrence Wade

System Owner

Product Support Manager (PSM)

ADE-540, Solutions Delivery Service

Prepared by: Barbara Stance, FAA CPO

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer