U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Information & Technology Services (AIT)

Enterprise Data Platform (EDP)

Responsible Official

Peter Ingegneri
Email: peter.ingegneri@faa.gov
Phone Number: 609-485-4053

Reviewing Official

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

Executive Summary

Federal Aviation Administration (FAA) programs leverage the Office of Information & Technology Services (AIT) Enterprise Data Platform (EDP) (formerly known as the Enterprise Information Management Platform (EIM Platform)) to collect, store, curate, enrich, access, and analyze FAA data and derived information products to meet their unique business needs. This enables more efficient processing, analysis, decision support, and production use in downstream FAA programs, business applications, and systems. This shared approach reduces operational complexity for both the enterprise and the users by promoting greater access to data and information services, which is consistent with the FAA's Policy under 49 USC 40101 and 49 USC 322.

Under the E-Government Act of 2002, the FAA developed this Privacy Impact Assessment (PIA) because the EDP collects Personally Identifiable Information (PII) on members of the public, including air operator information, airmen certificate numbers, Social Security Numbers (SSN), medical information, contact information, and aircraft registration information. This PIA is being updated to include a new data exchange of PII with the Low Altitude Authorization Capability Automation Platform (LAANC).

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 EDP is a collection of tools and capabilities that provides users the ability to retrieve, manipulate, and analyze data in a single data lake rather than multiple data repositories. The EDP delivers common data and information services that support multiple unique FAA systems but are decoupled from the supported systems so that data and services are available to support programs and users across the FAA. This shared approach reduces operational complexity for both the enterprise and the users by promoting greater access to data and information services.

The EDP enables the agency to move away from silo-centric applications toward a unified, secure, and integrated EDP environment. By hosting and providing common data and information management infrastructure, components, and services that can be reused and leveraged to support systems and business functions across the FAA, the EDP capability will grow in content and services while reducing duplicate capabilities and functions. The EDP is a Federal Information Security Modernization Act (FISMA) High environment accredited to process High-level and sensitive information.

The EDP's cloud-based, big data platform consists of two key items: (1) A Data Mall – this is a large repository for FAA data. It is organized and cataloged for easy access but safeguarded to preserve its integrity and to protect data from unauthorized access, and (2) an "App Mall" – this is a collection of curated technologies and tools to enable FAA personnel to transform data into information.

The EDP is updated quarterly to add new FAA data and new data-related technologies and tools, and to improve functionality. Currently, the EDP contains hundreds of data sources from across the Agency. Non-PII data present within the EDP could include air surveillance data, flight/flow/aeronautical data, weather data, and air safety data. The EDP's current PII data could include SSN, pilot medical information, operator/pilot name, aircraft registration

number/serial number, airmen certificate number, gender, date of birth (DOB), contact information (including home address, phone number, username, and email address). PII present in the EDP is not searchable by a personal identifier, such as a name or address. PII data elements on government employees, contractors, and members of the public currently come from the following upstream systems: Metrics ATC (Future Flight Services Program (FFSP) Workload Data Collection Report (WDCR)), Accident Incident Data System (AIDS), Service Difficulty Reporting System (SDRS), Low Altitude Authorization and Notification Capability (LAANC), Extended Operations Database, Airworthiness Directives, Designee Management System (DMS), Enforcement Information System (EIS), Intune (Microsoft 365), the National Wireless Program, Medical Support System (MSS) Document Imaging Workflow System (DIWS), FAA Recognized Identification Areas (FRIA) and Waiver Programs, and Airworthiness Directives.

FAA employees and contractors access the EDP with their Personal Identity Verification (PIV) credentials, via MyAccess. Each user has specific Rules Based Access Controls (RBAC) restrictions which are established when the data owners/stewards approve adding the user's names to the Active Directory Group for the specified data. Each specific application requires specific permission from an administrator. Because data within the EDP may be flagged as "sensitive," permissions adhere to the least privilege control, and therefore users are given the minimum level of permissions necessary to perform their duties. Unless a user has the administrator role, granted by the data owner or the Program Management Officer, the only other permission for a user is read-only.

Once within an App, the user can view data fields in different visualizations, such as structured data, including columns and rows, create maps, scatter plots, and pie charts, and can view geographic information, including runway surface data. Apps can also perform statistical analysis and visualizations and specify parameters for metrics.

The Integrated Safety Assessment Model (ISAM) is a web-based application within the EDP that provides FAA and Contractor staff the ability to create models of aviation safety risks in the National Airspace System (NAS). A *risk model* in this context means a diagram comprising elements that represent the causal, contributory, and circumstantial factors that lead to aviation accidents. Risk models in ISAM are expressed as *fault trees*. Fault trees are standard diagrams used in safety engineering.

Aviation safety analysts use the risk models in ISAM to represent a holistic view of risk in the NAS. Analysts and risk managers use the information contained within the risk models to make risk-informed decisions about operations (both present and future) in the NAS. The risk models also support both safety assurance (SA) and safety risk management (SRM) 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[2], 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[3].

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 their PII within the EDP. EDP access-related records about FAA users 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), which covers computer access records.

The EDP is not a Privacy Act system of records for the substantive records, reports, or data analytics within its system. However, the EDP pulls data from systems that have an associated SORN. All SORNs are listed on the Department of Transportation (DOT) Privacy webpage. EDP only maintains convenience copies of these records. Convenience copies of records are duplicate copies of official records that are used by employees or contractors in completing their job duties. An individual whose record is maintained in the EDP would need to make a Privacy Act request of the official system of record, not the EDP. The FAA does not make disclosures out of the EDP. Disclosures must be made from the originating system according to that system's applicable SORNs.

[2] https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

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

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.

The EDP only maintains convenience copies of records. An individual whose record is maintained in the EDP would need to make a Privacy Act request of the official system of record, not the EDP. The FAA does not make disclosures out of the EDP. Disclosures must be made from the originating system according to that system's applicable SORN(s).

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 uses EDP 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.

As described in the overview, the EDP pulls in data from various systems to perform analytics. Some of that data may come from Privacy Act systems of records. Site owners are responsible for ensuring that all data within the EDP that is subject to the Privacy Act is used only in accordance with the original purpose for the information's collection, consistent with the applicable SORN. System access data is 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 plan and manage system services in the performance of official duties, and to monitor and investigate improper computer use.

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 EDP to the relevant and

necessary information to meet its authorized business purpose, providing a data lake and visualization mechanism for various FAA employees and contractors in furtherance of their job duties. All data owners and data stewards are allowed read-only access to PII data. The EDP Program Management Office maintains access control audit logs to track access to PII.

Records within EDP are maintained in accordance with General Record Schedule 5.1, Common Office Records, item 020, approved July 2017. Records within EDP are considered non-record-keeping copies of electronic records and 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 General Records Schedule 3.2, Information Systems Security Records, item 030, approved January 2023. These records are temporary 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.

EDP is not a Privacy Act system of records for the substantive records, reports, or data analytics within its system. However, EDP may pull data from systems, such as AIDS, SDRS, MSS, EIS, DMS, and LAANC which may contain information associated with a SORN and covered by applicable routine uses. All SORNs are listed on the Department of Transportation (DOT) Privacy webpage. All use of data within EDP is in accordance with the applicable SORNs that cover the source system of the data.

Profile and logging PII collected by the FAA 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 pursuant to 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).

Users are allowed access only to specific data sets that they have been authorized to by the data owner. Data that is ingested into EDP comes directly from the source system; in some cases, such as LAANC, the exchange of individual's name, phone number and email address come via database replication. The information EDP receives from other systems is assumed to be accurate. The source system is responsible for ensuring the quality of the data it provides to EDP.

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. EDP 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 EDP audit logs. EDP is accredited as a High System and is authorized to store sensitive data.

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 as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of EDP 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

Peter Ingegneri
System Owner
FAA

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2025.06.13 13:32:21 -04'00'