U.S. Department of Transportation

# Privacy Impact Assessment

## Federal Aviation Administration (FAA)

## Office of Information & Technology Services (AIT)

## FAA-Enterprise Document Management System (FAA-EDMS)

### Responsible Official

Ashley S. Sherrod
Email: Ashley.s.sherrod@faa.gov

### Reviewing Official

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

## Executive Summary

Federal Aviation Administration (FAA) offices and programs leverage the FAA-Enterprise Document Management System (FAA-EDMS) business platform as a document storage repository. This repository enables more efficient storage and retrieval of governmental records and promotes greater access to data, which is consistent with the FAA's Policy 49 U.S.C. 40101 and 49 U.S.C. 322. Under the E-Government Act of 2002, the FAA developed this Privacy Impact Assessment (PIA) because FAA-EDMS maintains Personally Identifiable Information (PII) on individuals affiliated with airports, sponsors, or their consultants.

## 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;*
- *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.*

[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).

*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 Administration-Enterprise Document Management System (FAA-EDMS) business platform provides a variety of technical services for customers and offices that utilize the platform via tenant applications. Services provided by the FAA-EDMS include:

- Repository Service - Provides the capability to organize and manage the life cycle of the content and enforce security for access.
- Search Service - Provides content and metadata indexing and full text search capability.
- Transformation Service – Provides conversion services for different file formats.
- Content Modeling - Provides the capability to model hierarchical information to meet specific business needs.
- EDMS Share - Provides a collaboration environment to provide out of the box capability for end users to collaborate on the content creation, editing, versioning through the concept of a site.
- Administrative Console - Provides various tools for system administrator to manage and configure the FAA-EDMS system settings and to monitor system health.
- Content Service Representational State Transfer (REST) Application Programming Interface (API) – Provides management of content nodes, sites, users, and groups.
- Process Designer – Provides a web-based visual editor that allows business analysts to create and modify business process models.
- Admin Application - Manages the FAA-EDMS process server activity.
- Process Service User Interface (UI) - Provides a general user interface for the users to perform activities within the platform.
- Process Service REST API - Provides endpoints used to perform various FAAEDMS services.
- Process and Rule Engine – Provides a process and rule engine to control the process flow and tasks.

Most customers who maintain tenant applications that reside within FAA-EDMS maintain their own privacy compliance documentation, including any applicable PIA. However, several customers are considered within the FAA-EDMS security authorization boundary, and as such, are included within FAA-EDMS' security and privacy compliance documentation, as described below.

Users of the FAA-EDMS include FAA employees and contractors as well as external users (other government organizations/federal agencies). The external user access only pertains to Interagency Group on International Aviation (IGIA) application (see below). Requesting access for new users is done by an FAA-EDMS designated customer point of contact sending an initial request for access to the FAA-EDMS System Owner. The user access request must be reviewed and approved by the FAA-EDMS System Owner before a user account is created. Requests for access are generated by the FAA-EDMS customer points of contact via a Jira ticket. The Jira ticket must contain the name of the user requesting access, their business email address, location, organization, phone number and the business purpose for requesting access. For a denied request, the FAA-EDMS System Owner sends an email to the user stating that the request is denied and the reason for denial. Upon creation of the user account the user will be instructed to navigate to the FAA-EDMS Uniform Resource Locator (URL) and use their FAA Active Directory username and password, or for external users, their newly created Alfresco user account and password to log in.

The following customers maintain documentation in tenant applications within FAA-EDMS:

*The Airports Document Management System (ADMS)*

The FAA's Office of Airports (ARP) utilizes the Airport Document Management System (ADMS) tenant application within FAA-EDMS as a repository for final ARP documentation. ARP documentation is received by ADMS via an interface with the FAA's System of Airport Reporting (SOAR). SOAR is the FAA system used by the FAA to track grant applications and funding transfers between the FAA and the Department of Transportation (DOT) and by the FAA and air carriers, airports, and sponsor/public agencies across the United States (U.S.) to facilitate the Airport Improvement Program (AIP) and the Passenger Facility Charge (PFC) program. SOAR documentation present in ADMS relates to airport grants and includes information on entities and airports that have received FAA grants. PII could be present within this documentation; specifically, PII on members of the public who are individuals affiliated with airports, sponsors or their consultants who support grant processes in their business capacity. SOAR[2] documentation is present within ADMS for long-term storage purposes.

[2] The SOAR PIA is available here.

*Acquisition & Business Services (ACQ) eDocs*

FAA-EDMS stores records that were previously held in a now-decommissioned system, eDocs. FAA-EDMS now stores eDocs records including acquisition-related documents such as contracts, statements of work, responses from vendors, and other supporting documents that relate to contracts. There are three different forms that were stored in eDocs, and now are present in FAA-EDMS including the Business Declaration, Electronic Funds Transfer Waiver, and Intra-Agency Agreement. Data within these forms include names/signatures, company name, email address, Taxpayer Identification Number (TIN), phone number, DUNS number, yes/no boxes for ethnicity, and business controlling interest (economically/socially disadvantaged, disabled veteran, woman-owned). Records within eDocs pertains to contract companies supporting the FAA, and not specifically to individuals.

*Interagency Group on International Aviation (IGIA)*

FAA-EDMS stores records that were previously held in a now-decommissioned system, IGIA. The IGIA was used to store materials (such as conference papers) for the International Civil Aviation Organization (ICAO) clearinghouse and was used by several different federal agencies, including: the Department of Defense, Department of Commerce, Department of State, Department of Justice, National Transportation Safety Board, Environmental Protection Agency, Department of Homeland Security, and the Transportation Security Administration. IGIA contained draft conference materials, version control documents, comments, and workflow information for papers. PII could include the name and business contact information of non-FAA federal employees of the above-referenced agencies.

## 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].

[3] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

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

## 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 FAA-EDMS. The FAA also provides notice of its collection, use, and disclosure of PII within this system via the publication of this PIA.

FAA-EDMS 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.

FAA-EDMS is not a Privacy Act system of records for the substantive records within the system, and therefore does not provide notice to individuals at the point of PII collection. Records within FAA-EDMS are not subject to the Privacy Act and are not about individuals or are not searched for by a unique identifier. ADMS is not subject to the Privacy Act because, while the system does contain information about individuals, the information is not searched using unique identifiers. It is instead searched using airports or other company names. Electronic document (eDocs) records contain information about vendors including contracts, statements of work, responses from vendors, and other supporting documents that relate to contracts pertaining to business and not in an individual capacity and are therefore not subject to the Privacy Act. IGIA records include only business contact information for users from other federal agencies that participate in ICAO matters, and relate to conferences and agendas, and not individuals.

## 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.*

FAA-EDMS is not the source system for records that contain PII within ADMS, eDocs and IGIA. Users seeking access to records within ADMS, would make their request for access through the SOAR system, and not FAA-EDMS. FAA-EDMS is the historical repository for eDocs and IGIA, and as such is the only source for them. ADMS, eDocs and IGIA do not contain records protected by the Privacy Act.

## 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.*

As described in the overview, FAA-EDMS is a document storage repository. This repository enables more efficient storage and retrieval of governmental records and promotes greater access to data. The FAA uses the FAA-EDMS 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.

Records within FAA-EDMS were initially created and authorized pursuant to separate legal authorities. FAA-EDMS is merely the historical repository that holds these records.

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.*

FAA-EDMS is a historical repository for documentation initially collected in SOAR, eDocs and IGIA. All data owners are allowed read-only access to records.

Information technology operations and maintenance records for FAA-EDMS are maintained pursuant to General Records Schedule (GRS) 3.1, *General Technology Management Records*, and are destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use. System access records maintained under GRS 3.2, *Information Systems Security Records*, and are destroyed when business use ceases.

SOAR records are maintained in accordance with a variety of retention schedules, as follows:

NC1-237-77-02

Item 1 Airport project case files:

(a) Airports service. Destroy five years after financial completion of project
(b) Regional Airports division. Destroy after micro-filming and film is determined to be adequate substitute for paper records.
(1) Destroy five years after financial completion of project.
(c) Airport District Offices. Destroy five years after financial completion of project.

Item 2 Airport project plan files:

(a) Preliminary plans. Destroy upon receipt of approved construction plans.
(b) Approved construction plan. Destroy upon receipt of as constructed plans.
(c) As constructed plans. Destroy after microfilming and the film is determined to be adequate substitute for paper records.
(1) Destroy microfilm when 50 years old.

NC1-237-77-03

Item 47: Airport project program data files. Destroy when twenty years old. Transfer to Federal Records Center when ten years old.

NC1-237-77-04

Item 1: Airport project case files

(a) Office of Airports Programs. Destroy five years after completion of project.
(b) Regional Airports Division.
(1) Case files. Destroy twenty years after financial completion of the project.
(2) Airport Drawings/Layouts. Destroy fifty years after financial completion of the project. If microfilm is available, the original paper record may be destroyed after the film is determined to be an adequate substitute. Microfilm to be made in accordance with FPMR 101-11.5. Destroy microfilm after 50 years after completion of project.
(c) Airport District Offices. Destroy 5 years after financial completion of project.

Item 3: Airport project plan files.

(a) Preliminary plans. Destroy upon receipt of approved construction plans.

(b) Approved construction plan. Destroy upon receipt of as constructed plans.
(c) As constructed plans. Destroy fifty years after financial completion of project. If microfilm is available, the original paper record may be destroyed after the film is determined to be an adequate substitute. Microfilm to be made in accordance with FPMR 101-11.5. Destroy microfilm fifty years after completion of project.

Item 4: Airport project specification files. Destroy upon financial completion of project.

NCI-237-79-03

Item 5. Airport project case files.

(a) Transfer to Federal Records Center. Destroy 5 years later.
(b) Regional Airports Division/Airports District Offices. Transfer to Federal Records Center upon financial completion. Destroy 20 years later.

Item 6: Airport project plan files.

(a) Preliminary plans. Destroy upon receipt of approved construction plans.
(b) Approved construction plan. Destroy upon receipt of as constructed plans.
(c) As constructed plans.

(1) Paper (if not filmed). Transfer to FRC when volume warrants. Destroy 50 years after financial completion of the project or sooner if as-constructed plans for subsequent projects include all modifications.
(2) If microfilm is available, the original paper record may be destroyed after the film is determined to be an adequate substitute.
(3) Microfilm is to be made in accordance with FPMR 101-11.5. These film records may be forwarded to the FRC for retention when volume warrants. Destroy film 50 years after financial completion of project.

Records within eDocs are maintained under GRS 1.1, *Financial Management and Reporting Records* and are destroyed 6 years after final payment or cancellation, but longer retention is authorized if required for business use. DAA-GRS-2013-0003-0001.

Records within IGIA are maintained permanently pursuant to NCI-237-77-03, *External Relations Records*, and are offered to the National Archives and Records Administration when 40 years old.

## 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.*

FAA-EDMS is not a Privacy Act system of records for the substantive records within FAA-EDMS. Records within FAA-EDMS are not subject to the Privacy Act and are not subject to use limitations per the Privacy Act.

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.S. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed as a routine use under 5 U.S.C. 552a(b) as follows: (1) to provide information to any person(s) authorized to assist in approved investigations of improper access or usage of DOT computer systems; (2) 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 information discovery proceedings; (3) to contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working 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 (4) 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 records that they have been authorized to access by the FAA data owner. Data that is ingested into FAA-EDMS comes directly from the source systems. The information that FAA-EDMS receives from other systems is assumed to be accurate. The source systems are responsible for ensuring the quality of the data it provides to FAA-EDMS.

## 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. FAA-EDMS 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 FAA-EDMS logs. The FAA-EDMS is accredited as a Moderate confidentiality system. As FAA-EDMS could contain TINs within its historical documentation, which for some vendors could be their personal Social Security Number (SSN), FAA-EDMS is being tracked as part of the FAA'S Social Security Number Reduction Elimination Plan. TINs are protected via encryption and limited access.

## 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 the FAA-EDMS 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

Ashley S. Sherrod
System Owner

## Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN

Digitally signed by KARYN MARIE GORMAN
Date: 2024.11.07 11:31:04 -05'00'