U.S. Department of Transportation

Privacy Impact Assessment
Federal Aviation Administration (FAA)
Office of Finance and Management (AFN)

Enterprise Data Management Tools
EDMT

Responsible Official

Murty S. Pullela
Email: murty.pullela@faa.gov
Phone Number: (405) 954-6786

Reviewing Official

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

Executive Summary

The Electronic Document Management Tool (EDMT) is a Federal Aviation Administration (FAA) Office of Finance and Management (AFN) system. It comprises multiple applications that perform governmental accounting, data visualization, and data management for the Department of Transportation (DOT) and FAA customers. Additionally, it serves as a secure storage for the Enterprise Services Center (ESC).

This Privacy Impact Assessment (PIA) has been updated from the previously published PIA to reflect changes in EDMT's scope. The system now maintains Personally Identifiable Information (PII) on members of the federal workforce and members of the public within the Enterprise Content Services (ECS) component, including financial and accounting documents. EDMT is also used to store the FAA Office of General Counsel (AGC). This update also aligns the PIA with the current Privacy Act System of Records Notices (SORNs) that cover the system.

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;*

[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).

- *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

EDMT functions as an electronic filing system for DOT components, enabling the scanning of documents and recording of accounting transactions. Users can perform data analytics and generate reports without altering source data. Initially launched in 2006 as the Payroll Imaging Process System (PIPS), its security boundary was renamed EDMT in 2021.

EDMT comprises three primary applications:

- **EDDS (Denodo):** Provides a user-friendly, read-only interface for accessing DOT financial databases, allowing users to browse and search specific data. This tool does not store PII beyond user login credentials (email, username). Users can create ad-hoc reports from authorized data collections, with results displayed directly on their computers and no report data stored within EDDS itself.
- **ETRS:** Enables users to view, review, and create dashboards for tracking trends across multiple DOT data sources (e.g., ESC PRISM, DOT Delphi). Like EDDS, ETRS is a read-only data visualization tool that does not store PII beyond user login credentials (username, email). It supports complex analysis via a web portal, generating ad-hoc reports displayed directly on the user's computer.
- **ESC (Enterprise Content Services):** This component is used to scan and store DOT Office of Secretary of Transportation (OST) and FAA Office of the Chief Counsel (AGC) documents for easy searching and retrieval. All scanned documents are stored on an encrypted database with limited administrator access. ESC also receives data from DOT Delphi via a signed Memorandum of Understanding (MOU) for archival and retrieval of departmental financial records. The Delphi system has its own PIA for privacy processes.

PII in ESC: The scanned documents stored in ESC may contain the following Personally Identifiable Information (PII) related to members of the public, FAA employees, and contractors:

- **Personal Identifiers:** Full name, date of birth (DOB), Social Security Number (SSN) (full and partial), gender.

- **Contact Information:** Home address, home phone number, cell phone number, personal email address (alternate contact).
- **Financial Information:** Government travel card number and expiration, bank name, bank account and routing numbers, tax information (e.g., W-4 associated information including full name, SSN, full address, marital status).
- **Other:** Medical information (e.g., insurance selection).

Typical ESC transactions include:

- Scanning and archival storage of OST financial documents.
- Archival and active storage for AGC case files.
- Storage of audit artifacts for OST Statement on Standards for Attestation Engagements.

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, 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.

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.

EDMT is a privacy-sensitive system because its Enterprise Content Services (ECS) component collects, maintains, uses, and disseminates PII as detailed in the "Introduction & System Overview" section. This includes PII found in:

- **DOT Office of the Secretary of Transportation (OST) historical archives and agency budget documents,** which may contain PII for DOT/FAA employees, contractors, and the public, such as names, SSNs, dates of birth, contact information, financial details, and medical/retirement benefit information.

- **FAA Office of General Counsel (AGC) case files,** which may contain PII for DOT/FAA federal and contract workforce members, such as names, SSNs, dates of birth, contact information, medical/retirement benefit information, and case outcome results.

EDMT supports electronic storage, searching, and retrieval of these records, often using individual names as search identifiers. The Department provides public notice of these record collections through the following Privacy Act System of Records Notices (SORNs):

- **DOT/ALL 7, Financial Management Records (90 FR 55335, Dec 2, 2025):** Covers OST historical archives and agency budget documents, including payment, collection, and labor cost records for civilian employees. This SORN covers the PII listed above for public, FAA employees, and contractors within EDMT, including financial and personal identifiers.
- **DOT/ALL 10, Debt Collection Files (65 FR 19483, April 11, 2000):** Covers administrative management and collection of delinquent debt records, including salary-offset and administrative offset provisions.
- **DOT/ALL 13, Internet/Intranet Activity and Access Records (67 FR 30757, May 7, 2002):** Covers FAA access information records used for creating and validating login credentials, audit trails, and security monitoring for EDMT program participants and managers. A Privacy Act Statement is provided at the initial point of collection for access and authentication data.
- **DOT/ALL 19, Federal Personnel and Payroll System (FPPS) (73 FR 66285, Nov 7, 2008):** Covers records for controlling and facilitating salary payments to DOT civilian employees.
- **DOT/FAA 858, Adjudication Docket Records in Aviation Litigation Proceedings (88 FR 78467, Nov 15, 2023):** Covers DOT case records for in-house administrative adjudications and mediations related to aviation safety and acquisition disputes.

The publication of this PIA further demonstrates DOT's commitment to transparency for the EDMT system.

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.

EDMT receives data from the DOT Delphi system via a data exchange. For individuals that may have PII contained in Delphi system, they should review the individual participation and redress procedures listed in the Delphi PIA.[2]

Under the provisions of the Privacy Act, individuals may request searches of the EDMT within the ECS archives 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 EDMT, 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 EDMT system is authorized by the following legal authorities:

- 5 U.S.C. 301, 302, 5101 et seq.
- 23 U.S.C. 504.
- 31 U.S.C. Chapter 37 (Subchapters I & II), Debt Collection Act of 1982, 5 U.S.C. 5514, E.O. 11222 (Sec 206), E.O. 9397, and 49 C.F.R. part 92.
- 40 U.S.C. 1441.

[2] The DOT Delphi PIA is located at https://www.transportation.gov/sites/dot.gov/files/docs/Delphi_PIA_OST_Adjudicated_122914.pdf.

- 49 U.S.C. 106, 301, 322, 40122(g), 40108, 40101, 44701, 40113–40114, 46101–46110, 14 C.F.R. part 13 (Subparts D & G), 14 C.F.R. parts 14 & 17, and the Federal Claims Collection Act of 1966.
- The National Security Act of 1947, as amended; Chapter 3512.
- The Homeland Security Act of 2002; E.O. 12148, as amended; E.O. 12656, as amended; E.O. 13286; and Title 32 C.F.R.

The EDMT system may store in archive (images) form, PII such as citizens or legal permanent residents, visitors, members of the DOT Federal and contract workforce name, SSN, DOB, home address and/or employee's work address, cell and home phone number and/or employee's work phone number, medical, retirement and disability benefit information, credit card numbers or last four of credit card number, bank account information, driver's license number, EIN, TIN, Sex, personal email address and/or employee's email address, and tax information (ex. W-4 information).

EDMT maintains the following PII on members of the public DOT/FAA employee Email Address, DOB, SSN, last four of SSN, Home Address, Home Phone Number, Cell Phone Number, Medical Information, CC Number, Last four of CC Number, CC Expiration Date, Bank Account and Routing Number, Bank Name, DL Number, EIN/TIN (which is sometimes an SSN), Sex, Personal Email Address, Tax Information (W-4 associated information; Full Name, SSN, Address, Employer's Name, Employer's address, and EIN. The purpose of the exchange is to facilitate Delphi archival storage and retrieval for departmental financial records.

EDMT uses this information in accordance with the purposes for which it is collected: The purpose of the exchange is to facilitate Delphi archival storage and retrieval for departmental financial records. This information is used in accordance with the description in the "Purpose" section of the applicable SORN.

In addition, EDMT maintains the following PII on members of the public: email address and name. The FAA uses this access information for purposes of creating and validating login credentials, audit trails, and security monitoring for contractors who are part of the EDMT program and/or manage the system. This use is consistent with the description in the "purpose" section in the applicable system of records notice. The PII in the EDMT system is not routinely used for any other purposes.

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.

EDMT's ECS component stores PII contained within scanned documents, as detailed in the "Introduction & System Overview" section. While EDMT does not directly collect or use

SSNs, it stores scanned records that may contain full or partial SSNs, which can be used as retrievable identifiers within the records management system.

EDMT does not directly collect PII from the public. Instead, it maintains documentation (scanned as images) from OST and AGC, which are the original collecting entities. Paper copies are destroyed or returned to the owners after scanning staff verify correct scanning.

Electronic records in EDMT are retained according to the following National Archives and Record Administration (NARA) approved General Records Schedules (GRS):

- **Financial Records (GRS 1.1, Item 010, approved April 2020):** Temporary records related to governmental accounting and financial transactions. Retained for at least six years, with longer retention authorized for business use. Disposition Authority: DAA-GRS-2016-0013-0001.
- **Information Technology Operations and Maintenance Records (GRS 3.1, Item 020, approved November 2019):** Temporary records for IT operations and maintenance. Retained for at least six years, with longer retention authorized for business use. Disposition Authority: DAA-GRS-2016-0013-0001.
- **Information Systems Security Records (GRS 3.2, Items 050 & 051, approved January 2023):** Temporary electronic copies of master files/databases for security and recovery. Destroyed after identical records are captured in subsequent backups or transferred to NARA, with longer retention authorized for business use. Disposition Authorities: DAA-GRS-2013-0006-0007 and DAA-GRS-2013-0006-0008.
- **Legal Enforcement Files (N1-237-92-004, approved September 1992):** Temporary case files related to legal actions concerning Federal Aviation Regulations. Transferred to Federal Records Center (FRC) two years after case closure, with destruction five years after closure. Disposition Authority: N1-237-92-004.

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 FAA implements controls to limit the use of PII within EDMT. Access is restricted to FAA personnel with a "need-to-know," and system access is reviewed and approved by program management. The PII in EDMT supports governmental accounting, data visualization, data management, and the storage of AGC documents.

Sharing of Privacy Act records from EDMT is governed by the applicable SORNs previously listed in the "Transparency" section. Additionally, the Department adheres to 15 general

routine uses applicable to all DOT Privacy Act systems of records, published in the Federal Register (75 FR 82132, Dec 29, 2010; 77 FR 42796, July 20, 2012; 84 FR 55222, Oct 15, 2019).

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).

The FAA maintains EDMT data quality and integrity through several processes:

- **Encryption:** Data is encrypted both at rest and in transit.
- **Auditing:** EDMT logs are audited as needed, with business owners reviewing audit logs to ensure proper system use.
- **Cybersecurity Policy:** EDMT adheres to DOT Order 1351.37, Departmental Cybersecurity Policy, requiring continuous monitoring of security controls, annual reporting to the Authorizing Official (AO), and AO review of risk posture to determine acceptable operational risk.

Source Data Responsibility: The agency or department providing paper copies for scanning is responsible for the accuracy of the original information.

Scanning Quality Checks: FAA scanning staff conduct quality checks to ensure:

- All pages are scanned correctly.
- Image quality is acceptable.
- Paper copies are scanned in the correct order and rotation.

PII, received through scanned documents, is protected by limiting access to authorized FAA personnel with official duties requiring access. Audit logs are also maintained and periodically reviewed.

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 EDMT system resides in a government owned building on the Mike Monroney Aeronautical Center (MMAC) Oklahoma City, Oklahoma and located within the Systems Management Facility (SMF). The SMF physical security consists of the P2000 Security Management System and a turnstile providing controlled and monitoring of access to specifically approved individuals.

The EDMT encrypts data in transit and in storage. The encryption meets federal standards according to Federal Information Processing Standard (FIPS) 140-2 (or as amended). The system employs the Transport Layer Security (TLS) 1.2 Advanced Encryption Standard (AES) 256 using encryption technology to prevent unauthorized disclosure of information.

The EDMT system utilizes role-based access to ensure personnel are allowed the minimum access required to perform their assigned duties. The system is only available to users on the internal FAA network. Paper documents are destroyed after quality check verification is conducted unless otherwise stated by the Statement of Work.

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 FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and the 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 EDMT system 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 EDMT. All data in-transit is encrypted and access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessments to test and validate security process, procedures and posture of the system. Based on security testing and evaluation in accordance with the FISMA, the FAA issues EDMT an on-going authorization to operate.

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

Responsible Official

Murty S. Pullela
Information System Owner
Manager, Implementation and OPS Transition

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2026.02.20 09:48:02 -05'00'