U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Office of Finance and Management-
Franchise Funds Organization (AFN-FFO)
Electronic Document Management Tool (EDMT)

Responsible Official

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

Reviewing Official

Karyn M. Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Electronic Document Management Tool (EDMT) supports the electronic storage and indexing of documents, as well as search, retrieval, annotation, and updates. EDMT is comprised of multiple systems constituting an Electronic Document Management Solution (EDMS) for governmental accounting records managed and maintained by the Financial Services Division of the Federal Aviation Administration (FAA). Systems within EDMT include Enterprise Data Delivery Solutions (EDDS) Enterprise Content Management Solution (ECS), and the Payroll Imaging Process Services (PIPS).

This Privacy Impact Assessment (PIA) was developed in accordance with Section 208 of the E-Government Act of 2002 because EDMT maintains personally identifiable information (PII) on members of the federal workforce and members of the public within the PIPS archive. While PIPS does not directly collect information from the public, DOT components provide paper copies of their financial and accounting and security and/or government travel records that may include PII from members of the public as incidental information about the collection and payment of funds.

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*

[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).

- *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 is managed by the Office of Finance and Management-Franchise Funds Organization (AFN-FFO) at Mike Monroney Aeronautical Center (MMAC), in Oklahoma City Oklahoma. EDMT is a set of data management tools, including the PIPS application, which is an archive system that supports scanning and storage of images of hardcopy documents for seven active DOT Agency/departments, and one former customer with archived documents. The images are not searchable on information within the documents. These images are retrieved by the agency/department using predetermined data fields. In some instances, search indexes use a unique identifier such as an individual name to retrieve records.

The scanned paper documents are generally government agencies accounting and financial transaction records, and government travel records that are ready to be archived from the following seven DOT agency/departments:

1. Federal Aviation Administration (FAA): Accounts receivable, administrative orders on consent (AOC), reimbursable agreements, and employee clearance records.

2. Federal Highway Administration (FHWA): Accounts receivable, reimbursable agreements, accounts receivable daily deposit forms, accounts receivable debit vouchers, accounts receivable debt letters, accounts receivable miscellaneous, accounts receivable do- it-yourself (DIY) Credit Cards, accounts receivable Fed Wire, accounts receivable Freedom of Information Act (FOIA), accounts receivable Intra-Governmental Payment Collection (IPAC) and accounts receivable National Highway Institute Bill Collection.

3. Federal Motor Carrier Safety Administration (FMCSA): Accounts payable contracts, accounts payable invoice register, accounts receivable reimbursable agreements, accounts receivable civil fines, accounts receivable daily deposit, accounts receivable debit voucher, accounts receivable debt letters, accounts receivable DIY Credit Cards, accounts receivable Fed Wire, accounts receivable FOIA, accounts receivable IPAC, accounts receivable miscellaneous documentation, accounts receivable delinquency notice, and notice of claims.

4. National Highway Traffic Safety Administration (NHTSA): Accounts receivable reimbursable agreements, accounts receivable daily deposit, accounts receivable debit voucher, accounts receivable debt letters, accounts receivable FOIA, and accounts receivable IPAC.

5. Surface Transportation Board (STB) (archive until end of retention period, no active user): Accounts receivable daily deposit, accounts receivable debit voucher, accounts receivable debt letters, accounts receivable IPAC, accounts receivable fees and billing collection.

6. Bureau Transportation Statistics (BTS): Reimbursement agreements, accounts receivable daily deposit forms, accounts receivable debit voucher forms, accounts receivable debt letters, and accounts receivable IPAC forms.

7. Enterprise Services Center: Reimbursable agreements, accounts payable contracts

8. GovTrip: former EDMT customer which has no active users. EDMT continues to store GovTrip documents but no longer collects them. GovTrip records will be removed as soon as they are no longer needed per National Archives and Records Administration (NARA) requirement. The forms contained within the archive are previous requests for New GovTrip User Requests, GovTrip User Change Requests, and Direct Deposit Sign-Up Forms.

EDMT consists of the following:

- **Payroll Imaging Process Services (PIPS)** is an application that supports the electronic storage of documents and was created to follow the paperwork reduction policies of the federal Government Paperwork Elimination Act (GPEA) P.L. 105-277 XVII to reduce the storage costs of any existing legacy documents. It is a collection of the following Commercial-Off-the-Shelf (COTS) software:
    - Ascent Capture is used to define the document processing instructions also used to support the document scanning and indexing. The Ascent Capture then passes this information to ApplicationXtender.
    - ApplicationXtender is used to store the processed documents indexing information and the associated electronic images.
        - ApplicationXtender provides a web interface, which allows search and retrieval of the scanned documents based on metadata entered during the scanning process.
- **Enterprise Data Delivery Solutions (EDDS)** is a COTS software for data visualization that allows specified users a virtual view of data across platforms based on Memorandums of Understanding (MOU) or a Service Level Agreements (SLA). The MOU or SLA describes the information that will be provided with the virtual view.

  Users can also browse across defined relationships between data entities and search for specific data enabling business users to search the actual data using an intuitive interface without being able to change the data at the data source. Users can access any enterprise information regardless of its location, format, or protocol, using the methods that best suit their work needs such as data discovery and search, based on the MOU/SLA that is in place. These working documents are durative in nature and not maintained within the system.
- **Enterprise Content Management Solution (ECS)** is an OpenText content solution that can integrate content management across the four required environments (Dev, Test, Prod, and Disaster Recovery (DR)), and establish a meta-data integration and deduplication for record reference. ECS can store any format of digital data and provides a NARA approved records management platform.

Access

Federal government employees and contractors access the system with their Personal Identity Verification (PIV) card. Members of the public do not have access to the EDMT system or its components.

Document Storage

EDMT staff gets shipments of documents that are ready to be archived. Documents are sent via registered mail, Federal Express, or United Parcel Service (UPS). Once the records are received, the scanning and imaging staff prepares the files for scanning (making sure staples are removed, print orientation is uniform, etc.). The documents are then placed in batches based on the originating agency, separated by the type of form and the information it captures. The documents are scanned and saved in folders created by EDMT Application Administrators based on the agencies and type of form on a server with Federal Information Processing Standard (FIPS) 140-2 encryption in a sequential number format in which they are scanned (ex., 5534, 5535, 5536, etc.). The Ascent Capture application automatically places the scanned information into the retrieval database for storage. The retrieval database (encrypted storage location) allows authorized EDMT staff members to retrieve documents immediately once they are scanned. After the documents are scanned and indexed, the hardcopies of the scanned documents are then stored in locked bins until they are picked up to be destroyed by an authorized commercial service vendor contracted by EDMT or repackaged for return shipment to the owning agency depending on the SLA requirements.

Document Retrieval

ECS is accessible by authorized users through the EDMT website for requests for documents stored in PIPS by authorized administrators using only agency predetermined metadata. To obtain access to the website and documents, customers contact an EDMT staff member by email. The EDMT staff then forwards the request to the data owner of the requested data to ensure the requestor has the proper requirements for access to receive the data. Once approved the data request is emailed to the requestor.

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

[2] http://www.cio.gov/documents/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

information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

DOT agency/departments may provide documents to be scanned that may contain financial, accounting, security and/or government travel records that can include PII such as name, social security number (SSN), date of birth (DOB), home address and/or employee's work address, cell phone number, 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, employer identification number (EIN), taxpayer identification number (TIN), gender, personal email address and/or employee's email address, and tax information (ex. W-4 information). The EDMT systems support the electronic storage, indexing, searching and retrieval of these records. In some instances, search indexes use a unique identifier such as an individual name to retrieve records.

A Privacy Act Statement discussing the Department's privacy practices, regarding the collection, use, sharing, maintenance, and disposal of PII, is provided by the agency/department at the initial point of collection.

The Department also provides general notice to the public of these records collection through the following Privacy Act System of Records Notices (SORN):

- DOT/All 7 - Departmental Accounting and Financial Information System (DAFIS) and Delphi Accounting System - 65 FR 19481 - April 11, 2000;
- DOT/ALL 10 - Debt Collection File - 65 FR 19483 - April 11, 2000;
- DOT/ALL 11 - Integrated Personnel and Payroll System IPPS - 65 FR 19485 - April 11, 2000;
- DOT/ALL 13 - Internet/Intranet Activity and Access Records - 67 FR 30757 - May 7, 2002;
- DOT/ALL 19 - Federal Personnel and Payroll System (FPPS) - 73 FR 66285 - November 7, 2008;
- GSA/GOVT-3 – Travel Charge Card Program – May 3, 2013 78 FR 20108;
- OPM/GOVT-1 – General Personnel Records – (December 11, 2012 77 FR 79694.

In addition, this PIA, published on the Department's Privacy Program website (www.dot.gov/privacy) provides additional information on the privacy risks and mitigation strategies for the 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.

DOT will review all Privacy Act requests on an individual basis and may, as appropriate, waive exemptions if the release of information to the individual would not detrimentally impact the law enforcement or national security purposes for which the information was originally collected or is subsequently being used.

Notification procedure: Requests should be submitted to the attention of the official responsible for the record at the address below:

DOT Chief Privacy Officer
Department of Transportation
1200 New Jersey Ave, SE
E31-312
Washington DC, 20590

Email: privacy@dot.gov
Fax: (202) 366-7024

Individuals should include in their requests the following information:

- Name and title of the system of records from which you are requesting the search.
- Name of individual
- Mailing address
- Phone number or email address; and
- Description of the records sought, and if possible, location of records.

Contesting record procedure: Individuals wanting to contest information about them, that is contained in this system, should make their requests in writing, detailing the reasons for and why the records should be corrected. Requests should be submitted to the attention of the OST Official responsible for the record at the address below:

DOT Chief Privacy Officer
Department of Transportation
1200 New Jersey Ave, SE
E31-312
Washington DC, 20590

Email: privacy@dot.gov
Fax: (202) 366-7024

Additional information about the Department's privacy program may be found at: https://www.transportation.gov/privacy-program/about-us. Individuals may also contact the DOT Chief Privacy Officer at: privacy@dot.gov. For questions relating to DOT's Privacy Program please go to http://www.dot.gov/privacy.

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 integral to the operations of the Federal Aviation Administration in furtherance of its responsibilities to ensure aviation safety under 49 USC 40103. The EDMT system may store in archive (images) form, PII such as name, social security number (SSN), date of birth (DOB), home address and/or employee's work address, cell phone number, 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, employer identification number (EIN), taxpayer identification number (TIN), gender, personal email address and/or employee's email address, and tax information (ex. W-4 information). The data elements listed above were collected by the customers in support of their mission and business processes. EDMT is the archive for data collected by these customers EDMT does not use, collect or manage the data; instead, it stores the documents as an archive for the customers. EDMT archives the documents in accordance with approved record retention schedules to meet federal requirements.

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 individual agency/department organizations are responsible for ensuring the data scanned into the EDMT system contains only the required PII. EDMT does not use or collect SSNs, including truncated SSNs. However, FAA security clearance records, which are stored as pictures, may contain SSNs. EDMT is a records management system for these documents, and the SSNs within the scanned records are not used as a retrievable identifier.

EDMT does not directly collect information from, or about, the public. Instead, EDMT maintains documentation that contains members of the public's information. EDMT is the archive for its federal customers, who have previously collected the required information. Documents are scanned into the PIPS system and stored as images of the records. The paper copies are returned to their owners or destroyed once it is determined, by scanning staff, that documents have been scanned correctly. The electronic records stored in the EDMT system and their retention periods are as follows:

- Debt Collection information supports activities associated with the collection of money owed to the United States government from both foreign and domestic sources. Payment information includes disbursements of Federal funds via a variety of mechanisms to Federal agencies, state, local and international Governments, and the private sector, to effect payment for goods and services, or distribute entitlements, benefits, grants, subsidies, loans, or claims. Payment management provides appropriate control over all payments made by or on behalf of an organization, including but not limited to payments made to vendors in accordance with contracts, purchase orders and other obligating documents; state governments under a variety of programs; employees for salaries and expense reimbursements; other Federal agencies for reimbursable work performed; individual citizens receiving Federal benefits and recipients of Federal loans. Debt collection and payment records are maintained in accordance with approved National Archives and Records Administration (NARA) schedule N1-237-09-023, FAA Financial Records Disposition Schedule, December 20, 2009, Payments and Receivables Records, Item 4. Electronic records may be retained as long as needed for business purposes and no longer than seven years after the cut off period the cut off period is at the end of the fiscal year if the payment is made, or debt is satisfied.

- Collections and receivables information includes deposits, fund transfers, and receipts for sales or service. Receivable management supports activities associated with recognizing and recording debts due to the federal government, performing follow-up actions to collect on these debts, and recording cash receipts. These records are maintained in accordance with approved NARA schedule N1-237-09-023, FAA Financial Records Disposition Schedule, December 20, 2009, Accounting and Cash Management Records Item 2. Electronic and hard copy records may be retained as long as needed for business purposes and no longer than 7 years.

  Security Management information supports the processes associated with ensuring employees, contractors, and others have been approved to enter Federal buildings, utilize Federal services, and access sensitive information. This includes eligibility determination, badge issuance, clearance tracking, and security verification services.

- Employee clearance records includes The Official Personnel Folder (Standard Form 66) or its approved electronic equivalent documents an individual's employment history. GENERAL RECORDS SCHEDULE 2.2, Employee Management Records, April 2020, Official Personnel Folder (OPF)/electronic OPF (eOPF) item 040.

- GRS 3.2 Information System Security Records 050/051: Backups of master files and databases. Electronic copy, considered by the agency to be a federal record, of the master copy of an electronic record or file and retained in case the master file or database is damaged or inadvertently erased. File identical to permanent records scheduled for transfer to the National Archives. Destroy immediately after the identical records have been captured in a subsequent backup file or at any time after the transfer request has been signed by the National Archives, but longer retention is authorized if required for business use.

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.

EDMT does not use or collect SSNs, including truncated SSNs. However, FAA security clearance records, which are stored as images, may contain PII such as name, social security number (SSN), date of birth (DOB), home address and/or employee's work address, cell phone number, 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, employer identification number (EIN), taxpayer identification number (TIN), gender, personal email address and/or employee's email address, and tax information (ex. W-4 information). Records maintained in the EDMT system supports the electronic storage, indexing, searching, and retrieval of financial and accounting, security and/or government travel records for several DOT agency/departments. EDMT is the archive for data collected by these customers EDMT does not use, collect or manage the data; instead, it stores the documents as an archive for the customers. EDMT archives the documents in accordance with approved record retention schedules to meet federal requirements.

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 information stored within the EDMT system is the responsibility of the agency/department that provides the paper copies to be scanned. Quality checks are conducted on the scanned images to ensure:

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

Records maintained in the EDMT system support the electronic storage, indexing, searching and retrieval of financial and accounting, security, and/or government travel records for several DOT agency/department. Authorized FAA employees and contractors upload records and the records are then searchable by the agency/department using pre-determined indexes to retrieve their specific agency/department records from the EDMT system.

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.

EDMT resides in a government owned building on the Mike Monroney Aeronautical Center (MMAC) Oklahoma City, OK. The entire campus is occupied by government and contractor personnel and is not open to the public. PIPS scanners are located in the HQ building room 272-F. EDMT application is housed within the Systems Management Facility (SMF). The SMF is located on the 1st floor of the Multi-Purpose Building (MPB) on the MMAC campus. The P2000 Security Management System and a turnstile provide physical security to the SMF. EDMT servers are setup to encrypt data in transit and in storage that meet federal standards using encryption according to FIPS 140-2. The system employs the TLS 1.2 AES 256 using RSA (2048 Bits) encryption technology to prevent unauthorized disclosure of information.

Paper documents are either destroyed or returned to the customer after quality check verification is conducted. The system is only available to users on the internal network.

The EDMT system utilizes role-based access to ensure personnel are allowed the minimum access required to perform their assigned duties.

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 Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division is responsible for governance and administration of the following:

- FAA Order 1370.121 FAA Information Security and Privacy Program Policy (as amended)
- E-Government Act of 2002 (Public Law 107-347,)
- Federal Information Security Modernization Act (FISMA)
- DOT privacy regulations
- Office of Management and Budget (OMB) mandates
- Other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, additional policies and procedures are consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance in their duties as related to collecting, using, and processing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior.

The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of the EDMT system as related to the requirements of OMB Circular A-130 requirements.

Responsible Official

Murty Pullela
Information System Owner
Manager, Implementation and OPS Transition

Approval and Signature

Karyn M. Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer