U.S. Department of Transportation

Office of the Secretary (OST)

Privacy Impact Assessment (PIA)
Electronic Document Management System (EDMS)

Responsible Official

Angela Knight
EDMS System Owner
Office of the Chief Digital and Information Officer
angela.knight@dot.gov

Ashleigh Schofield
EDMS Business Owner
Office of the Secretary of Transportation
Ashleigh.Schofield@dot.gov

Approving Official

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

Executive Summary

The Electronic Document Management System (EDMS) is an application used to control and manage official correspondence (mail, email, fax) to and from the U.S. Department of Transportation (DOT or the Department) Office of the Secretary (OST), Deputy Secretary, Chief of Staff, and members of Congress, the administrators and senior management of the DOT operating administrations, state and local elected officials, associations and organizations, private companies, and members of the public.

This Privacy Impact Assessment (PIA) is conducted in accordance with the E-Government Act of 2002 as the correspondence maintained in the system may contain Personally Identifiable Information (PII) on members of the public.

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;*

[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).

- *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 Department developed the EDMS web-based application to reduce the time and labor required to manage Executive Correspondence for documents requiring the signature of the Secretary, the Deputy Secretary or an Operating Administration's Administrator or Executive. The system is managed by the Executive Secretariat and is used by Operating Administrations (OAs) and other offices within the Office of the Secretary engaged in responding to Executive Correspondence. The OST Executive Secretariat and the executive secretariats of each of the DOT operating administrations (e.g., Federal Aviation Administration (FAA), Federal Transit Administration (FTA), et. al.) are charged with receiving the correspondence and routing it to appropriate DOT personnel for preparing, reviewing, and approving a response.

Through EDMS, authorized users (typically administrative assistants) may upload incoming correspondence and route the correspondence to appropriate parties within DOT to prepare a response and to circulate that response for comments and concurrence from appropriate DOT organizations, such as legal counsel and policy.

Correspondence may arrive at DOT via physical mail, electronic mail, or fax, or other means, including hand-delivery. Physical correspondence is scanned and saved to the correspondence intake analyst's computer and then uploaded into the system. The following information from the correspondence is manually entered and stored: Name, Last Name, Job Title, Email, Address, Organization, Phone Number, and Country.

Correspondence that arrives electronically, via email, is forwarded to the correspondence intake analyst's email box. EDMS facilitates the upload of the content of the email message along with all attachments into EDMS. The correspondence intake analyst then manually enters the correspondent's Name, Last Name, Job Title, Email, Address, Organization, Phone Number, and Country. EDMS does not incorporate optical character recognition capabilities.

EDMS is not publicly available and does not solicit information from the public; however, correspondence maintained in the system may include some PII of the correspondent, which has been volunteered by the correspondent. In this case, the information is saved in EDMS.

The PII provided is, as appropriate, used to develop the response to requestors and to facilitate correspondence with the requestors. EDMS houses PII on:

- Individuals who write or are referred to in writing by a second party, to the Secretary, Deputy Secretary, Deputy Under Secretary, and their immediate offices as well as to the administrators and deputy administrators of the DOT operating administrations.
- Individuals who are the subject of an action requiring approval or action by one of the forenamed, such as appeal actions, training, awards, foreign travel, promotions, selections, grievances, and discipline may have their PII.

Once the out-going correspondence is signed by the appropriate DOT official, the entire correspondence package is archived for future reference and reviewed in accordance with approved Privacy Act notices and records disposition schedules.

The records housed in EDMS are maintained by the Executive Secretariat on behalf of the Secretary, Deputy Secretary, Associate Deputy Secretary, Chief of Staff, Director of the Executive Secretariat, and officials in similar roles in the DOT operating administrations. The EDMS platform is maintained by the DOT Office of the Chief Digital and Information Officer.

At the time of publication of this PIA, there are no standing, automated exports of data from EDMS, however plans for EDMS include an automated transfer of correspondence to the U.S. National Archives and Records Administration (NARA) in accordance with records retention schedules of DOT and DOT operating administrations regarding executive correspondence.

The DOT Office of the Chief Digital Information Officer (OCDIO) is the responsible organization for this system.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template 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

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

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.

EDMS does not require any PII from the public. The PII voluntarily sent to the DOT by mail, email, or fax is saved in EDMS for sole purpose of preparing a response and corresponding to the same party requesting answers. The Department provides general notice to the public of this records collection through its Privacy Act System of Records Notice (SORN), DOT/OST 041 – Correspondence Control Mail (CCM), 70 FR 19554, April 11, 2000, which provides general notice to the public. Records created after January 1, 1974, are indexed by name of correspondent, referring individual, and subject category (e.g., ''employment'' for applicants). Records created prior to that date are indexed by name of correspondent.

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 should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Under the provisions of the DOT's Privacy Act/Freedom of Information Act (FOIA) procedures, individuals may request searches of EDMS to determine if any records have been added that may pertain to them. The Freedom of Information Act (FOIA) is a federal law that gives you the right to access any DOT records unless DOT reasonably foresees that the release of the information in those records would harm an interest protected by one or more of the nine exemptions (such as classified national security, business proprietary, personal privacy, investigative documents) or release is prohibited by law. The DOT will review all

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

Privacy Act requests on an individual basis and may waive exemptions if the release of information to the individual would not cause harm to applicable exemptions such as law enforcement or national security.

Notification procedure: Individuals wishing to know if their records appear in this system may inquire in writing to the system manager:

EDMS System Manager
1200 New Jersey Avenue, SE
Washington, DC 20590
Email: DOTCIO@dot.gov
Fax: (202) 366-7373

Included in the request must be the following:

- Name
- Mailing address
- Phone number or email address
- A description of the records sought, such as the subject matter of the correspondence, addressee of incoming correspondence, and date(s) and author(s) of the response(s), and if possible, the location of the records.

Contesting record procedures: Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons for 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:

EDMS System Manager
1200 New Jersey Avenue, SE
Washington, DC 20590
Email: DOTCIO@dot.gov
Fax: (202) 366-7373

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 its collects, uses, maintains, or disseminates PII.

EDMS is integral to the operations of the Department in furtherance of its responsibilities to ensure a safe and reliable transportation system as authorized by 49 CFR. The purpose of the system is to support the preparation of a response to correspondence addressed to and to be signed by the Secretary and Deputy Secretary of Transportation and the officials of the DOT OAs. The PII voluntarily sent to DOT by mail, email, or fax is saved in EDMS is maintained solely for purposes of responding to the correspondent who provided the information. 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. DOT should retain PII for only if necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

EDMS only collects the information necessary to accomplish EDMS's stated purpose. EDMS does not require any PII from the public. The PII voluntarily sent to the Office of the Secretary by mail, email, or fax is saved in EDMS for sole purpose of providing a response to the same party requesting answers.

EDMS also collects basic user contact information about DOT employees and contractors tasked with managing correspondence, including user role and organizational assignment to establish access authorization. User contact information is used to identify the user and to send responses to letters or emails of the enquiring public. Responses are sent via postal mail or email.

Records are maintained in accordance with approved NARA records disposition schedule, see Appendix A.

Hard-copy records for 1967 to 1969 and duplicate microfilms for 1974 to 1989 are in the custody of (NARA). Records reside on the system as defined by DOT policies and as disk space on the system allows prior to conversion to Microfilm at an approved schedule by the DOT. Microfilm Records from 1990 through the present are retained in the Departmental headquarters building.

Computer microfilm records, and remote reader terminals, which permit access to the system records, are locked after office hours. During office hours computer is accessible only

through terminals operated by, and under the surveillance of, authorized employees of the Executive Secretary.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

The PII that is collected in EDMS is not used in any manner that is not specified in notices and is only used for the purposes collected. Consistent with the Privacy Act system of records notice for this system, data entered and stored in EDMS is used for communications and referral to the appropriate office within as well as outside the DOT for actions involving matters of law or regulation such as the Civil Service Commission for employee appeals, the Department of Justice in matters of law enforcement. Additionally, the Department may share PII maintained in EDMS for purposes stated in the Department's Prefatory Statement of General Routine Uses.

EDMS does not automatically nor routinely send data nor documents electronically to any other system. All data housed within EDMS is retained within EDMS except as necessary to comply with federal records retention schedule.

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).

Authorized users are DOT employees or contractors whose responsibilities include tracking, drafting, reviewing, routing, and approving responses to correspondence directed to DOT officials.

Authorized users enter data into EDMS manually via the application's screens and upload incoming correspondence and the outgoing drafts and final signed version into the document repository. Over the lifecycle of the correspondence, from initial data entry through reviews and revisions of the draft as well as the final approval of the outgoing response, data and documents housed within EDMS undergo several iterations of quality checks to ensure the data entered is accurate and complete.

To preserve data quality and integrity in the event that data in the system becomes corrupt or needs to be restored, system backups are made nightly. The backups securely housed in an off-site location.

OST and the DOT operating administrations ensure that the collection, use, and maintenance of information collected for operating EDMS is relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, it is accurate, complete, and up to date.

The redress process described in the Individual Participation and Redress section is a mechanism to maintain and improve accuracy of information.

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.

EDMS takes appropriate security measures to safeguard PII and other sensitive data. EDMS applies FedRAMP and DOT security standards, including but not limited to performing routine scans and monitoring, backing EDMS data, and through performing background checks of technical employees and contractors.

The platform used for implementing EDMS is the Microsoft Dynamics 365 Online Government. Microsoft has achieved an authority to operate (ATO) as certified by the Federal Risk and Authorization Management Program, or FedRAMP, which is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based products and services. This software-as-a-service offering was independently assessed by a third party to ensure the required security controls are in place and operating as intended. In addition to the FedRAMP security assessment, the DOT has performed an additional security assessment to authorize EDMS.

The EDMS system is categorized as a Moderate security impact system and adheres to all moderate baseline security controls. All DOT personnel and contractors are required to take annual security awareness training. EDMS requires user identification and authentication prior to allowing access to the system. Access to the system is tightly controlled and no access can be granted without the approval of the EDMS account manager. When approving access, the concept of least privilege is implemented, which means that users are only granted the access rights they require for their positions. EDMS employs role-based access control.

All data is encrypted, in transit using TLS 1.2 and at rest using Microsoft DKM protocol. Microsoft provides intrusion detection and security monitoring of the EDMS platform. The application has robust auditing controls in place to ensure security relevant events are captured and recorded. Audit logs are reviewed to detect any suspicious activity. The

application is hosted at Microsoft datacenters which have multiple layers of physical protection.

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.

OST is responsible for identifying, training, and holding OST employees and contractors accountable for adhering to DOT/OST privacy and security policies and regulations. OST follows the Fair Information Practice Principles as best practices for the protection of PII associated with the EDMS. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records.

Federal and contract employees are given clear guidance in 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 as well as the DOT Rules of Behavior.

Users with greater responsibilities with respect to EDMS's operation, are required to take additional, specialized security and privacy training, appropriate to their roles.

The OST Information System Security Officer and OST Privacy Officer will conduct periodic security and privacy compliance reviews of the EDMS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Responsible Official

Angela Knight
EDMS System Owner
Office of the Chief Digital and Information Officer
angela.knight@dot.gov

Ashleigh Schofield
EDMS Business Owner
Office of the Secretary of Transportation
Ashleigh.Schofield@dot.gov

Approving Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2025.11.20 08:23:29 -05'00'

Appendix A: EDMS Retention Schedules

OA	Current Record Schedule	Record Schedule Status			Item Nos.
		Approved	Pending	Not Started	
OST	DAA-0398-2024-0004		X		1, 2, 3, 6
FAA	NC1-74-227				1, 7, 10
FHWA	N1-406-08-5				1, 2
FMCSA	N1-557-05-11 N1-557-05-001 N1-557-05-007				2, 3, 11 4, 8, 9, 11 1, 2, 4 ,7
FTA	N1-408-05-1				1000, 2500
MARAD	NC1-357-81-2				27, 28, 43, 44, 45, 47, 54, 56, 57, 58, 59, 60, 72, 76, 77, 78, 87, 422
NHTSA	N1-416-86-001/11 & N1-416-86-001 & N1-416-09-4/2	X			1, 16, 17, 18
FRA	DAA-0399-2015-0001 DAA-0399-2013-0004 DAA-0399-2013-0003				1 1 1
PHMSA	DAA-0571-2018-0008				1, 2
GLS	N/A*				

*GLS does not store any GLS records in the EDMS repository.