U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

Electronic Document Management System (EDMS)

Responsible Official

Richard Kim

EDMS System Owner

(202) 366-6830

Richard.Kim@dot.gov

Reviewing Official

Claire W. Barrett

Chief Privacy & Information Asset Officer

Office of the Chief Information Officer

privacy@dot.gov

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=CLAIRE W BARRETT
Date: 2017.03.21 09:27:23 -04'00'

Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is an Operating Administration within the U.S. Department of Transportation (DOT) with a core mission to reduce commercial motor vehicle-related crashes and fatalities. To further this mission, FMCSA created the Electronic Document Management System (EDMS) web-based system (https://edms.fmcsa.dot.gov/) to provide FMCSA personnel with a centralized document repository application for the purpose of storing, archiving and retrieving documents relevant to FMCSA business processes.

This Privacy Impact Assessment (PIA) update is necessary to addresses risks associated with migrating the EDMS system to the FMCSA Cloud Enviornment.

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.*

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

Electronic Document Management System (EDMS) is a web-based, commercial, off-the-shelf software program (emVision360) that was customized for FMCSA. EDMS facilitates the storage, retrieval, and management of documents

[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 M-03-22 dated September 26, 2003).

from any authorized system throughout FMCSA Headquarters (HQ), service centers, divisions, and remote offices. EDMS has been enhanced to automatically upload compliance reviews and safety audits from the Motor Carrier Management Information System (MCMIS) and download Certified Roadside Inspection Reports to SAFETYNET. There is a daily scheduled job in EDMS that extracts updates of census information (Company Name, Trade or D.B.A. [Doing Business As] Name, phone number, etc.) from MCMIS, if MCMIS has a change dated after the corresponding EDMS Carrier Folder was last updated. It also creates new DOT Carrier Folders if a new DOT number was created in MCMIS and is active. EDMS also currently manages enforcement cases and general documentation related to motor carriers, FMCSA personnel, and FMCSA policies.

EDMS collects, stores, and transmits Personally Identifiable Information (PII), including the sole proprietors of active or inactive interstate motor carrier operations, operators of licensed or unlicensed interstate commercial motor vehicles (CMVs), and FMCSA employees and contractors.

EDMS uses emVision360—a software program developed by Global 360, Inc.—to store, retrieve, and manage all documents concerning motor carriers, FMCSA personnel, and FMCSA policies. EDMS manages the large volume of electronic files and images ("objects") produced by FMCSA via multi-threaded object servers and a data repository. The current functionality of EDMS does not include the use of heavy client workstations. EDMS operates behind the FMCSA AWS firewall, which requires all users to authenticate with a valid user identifier and password to gain access to the FMCSA Cloud Environment.

Personally Identifiable Information (PII) and EDMS

EDMS collects, stores, and transmits Personally Identifiable Information (PII) regarding sole proprietors of active or inactive interstate motor carrier operations, operators of licensed or unlicensed interstate commercial motor vehicles (CMVs), and FMCSA employees and contractors.

The input of information into EDMS is discretionary. Field users upload compliance review, inspection and enforcement documents related to motor carriers. Use of the administrative (non-carrier related) sections of EDMS are also at the discretion of the Division/Field Administrator and may or may not contain certain types of information including, but not limited to, sensitive personnel documents such as Travel Vouchers (which include Social Security Numbers). Therefore, there is the potential for the following categories of documents to reside in this system:

- Carrier-Related Documents include, but are not limited to:
  - Carrier Enforcement Case Documents
  - General Carrier Documents, including, but not limited to:
    - Compliance Reviews
    - Correspondence (including e-mail)
    - Crash Reports
    - Out of Service Orders
    - Safety Audits
  - Carrier Receipt Documents
  - Driver Enforcement Case Documents, including, but not limited to:
    - Notice of Claim
    - Receipts
    - Correspondence (including e-mail)

        - Enforcement Cases
        - Exhibits
        - Final Agency Orders
    - Roadside Inspection Certification
    - Roadside Inspection Report
- Administrative Documents including, but not limited to:
    - Delegations of Authority
    - Non-personnel related Employee Documents
    - Federal Programs
    - Rules of Conduct
    - Employee Work Schedules
    - Time and Attendance Records
    - Congressional Correspondence
    - Suspicious Activity Reports
- Management and Financial Management Documents including, but not limited to:
    - Budgets and Invoices

As a result of the potential for the aforementioned categories of documents residing in the EDMS system, the following categories of PII may also be collected, stored, or transmited: Name, Address, Social Security Number, Employer, Pay Grade, Email Address, Telephone Number, Business Address, Family Members (dependents), Birth Date, and Marriage Date.

Move to the FMCSA Cloud Environment

As part of the Administration's ongoing plans and actions to modernize and enhance IT tools that support FMCSA mission processes for registration, inspection, compliance monitoring and enforcement, a number of core FMCSA enterprise applications, including EDMS have been migrated from a private in-house DOT hosting environment and general support services infrastructure to a commercial cloud environment and infrastructure (the Amazon Webservices [AWS] Cloud) known as the FMCSA Cloud Environment.

Initial transition into the FMCSA Cloud Environment followed a lift-and-shift migration approach to replicate the existing application and infrastructure hosting environment directly onto the infrastructure-as-a service (IaaS) platform provided by the AWS Cloud. In following this technical migration approach, FMCSA enterprise applications were not redesigned or modified to accommodate the physical transition to the new AWS Cloud IaaS platform or environment. The risks associated with this migration are discussed in the Security section of this PIA.

For more information on the FMCSA Cloud Environment please refer the the FMCSA Cloud Environment PIA available on the DOT Privacy Office website at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

Fair Information Practice Principles (FIPPs) Analysis

The Fair Information Practice Principles (FIPPs) are rooted in the tenets of the Privacy Act and are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs are common across many privacy laws and provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis DOT conducts is predicated on the privacy control families articulated in the Federal Enterprise

Architecture Security and Privacy Profile (FEA-SPP) v.3i, which is sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council.

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

For both direct access and Intranet access to EDMS, users must read and agree to a warning message that discusses the penalties of unauthorized access before logging in. The EDMS website has a link to DOT Privacy Policy that contains all the protection and advisories required by the E-Government Act of 2002. The Privacy Policy describes DOT information practices related to the online collection and the use of PII.

Notice is also provided to individuals through the Privacy Act System of Records Notice (SORN) for EDMS (DOT/FMCSA 005 - Electronic Document Management System (EDMS) - 71 FR 35727 - June 21, 2006). The EDMS SORN is available to the public on the DOT Privacy Office website and from the Federal Register (http://www.gpo.gov/fdsys/pkg/FR-2006-06-21/pdf/E6-9732.pdf).

FMCSA informs the public that their PII is stored and used by EDMS through this Privacy Impact Assessment, published on the DOT website. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the PII, along with all uses of the PII stored and transmitted through EDMS. The EDMS PIA is available at http://www.dot.gov/individuals/privacy/privacy-impact-assessments.

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.

FMCSA provides redress for individuals whose records may be maintained in various FMCSA systems, including the EDMS system, through its DataQs system.

The DataQs system (https://dataqs.fmcsa.dot.gov/login.asp) is an electronic means for filing concerns about federal and state data released to the public by FMCSA. Individuals can use DataQs to challenge information included in their records. Motor carriers, state agencies, and FMCSA offices can use DataQs to challenge information concerning crashes, inspections, compliance reviews, safety audits, enforcement actions, vehicle registrations, operating authorities, insurance policies, and consumer complaints stored in any FMCSA system, including EDMS. After a challenge has been submitted, DataQs automatically forwards the challenge to the appropriate office for resolution and allows the party that submitted the challenge to monitor its status. If the information is corrected as a result of the challenge, the change will be made in MCMIS. EDMS will receive the changed information through the a refresh from MCMIS.

DataQs cannot be used to challenge safety ratings or civil actions managed under 49 CFR 385.15 (Administrative Review) or 49 CFR 385.17 (Change to Safety Rating Based upon Corrective Actions). Any challenges to information provided by state agencies must be resolved by the appropriate state agency.

Under the provisions of the Privacy Act and Freedom of Information Act (FOIA), individuals may request searches of EDMS or MCMIS to determine if any records have been added that may pertain to them. This is accomplished by sending a written request directly to:

Federal Motor Carrier Safety Administration
Attn: FOIA Team MC-MMI
1200 New Jersey Avenue SE
Washington, DC 20590

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.

The main purpose of EDMS is to provide FMCSA personnel with a centralized document repository application for the purpose of storing, archiving and retrieving documents relevant to FMCSA business processes. EDMS collects, stores, and transmits Personally Identifiable Information (PII) regarding sole proprietors of active or inactive interstate motor carrier operations, operators of licensed or unlicensed interstate commercial motor vehicles (CMVs), and FMCSA employees and contractors (includes SSN).

Legal authorities for EDMS are 49 U.S. C. 31136(e), Motor Carrier Safety Act of 1984, 49 U.S.C. 31315, and the Transportation Equity Act for the 21st Century (TEA–21), which was enacted June 9, 1998 as Public Law 105–178.

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 as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule. Forms used for the purposes of collecting PII shall be authorized by the Office of Management and Budget (OMB)

FMCSA collects, uses, and retains only data that are relevant and necessary for the purpose of EDMS. EDMS retains and disposes of information in accordance with the approved records retention schedule as required by the U.S. National Archives and Records Administration (NARA).

EDMS records are retained and destroyed in accordance with applicable NARA retention schedule N1-557-05-007 Item #4 (http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0557/n1-557-05-007_sf115.pdf). The length of retention time for EDMS documents depends on whether the information falls under inputs, master data files, documentation, or outputs. For any information entering EDMS, the data is destroyed or deleted, regardless of media, after information is imported into the EDMS master data files, backed up, and verified. For master data files and any documentation, the information is destroyed or deleted when the data is superseded or becomes obsolete. For any outputs (reports), the information is destroyed or deleted when the data is no longer needed for reference.

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 FMCSA minimizes its data collection to that necessary to meet the authorized business purpose and mission of the Agency. This information is used by FMCSA personnel according to the business needs of the Federal Motor Carrier Safety Administration in the performance of those functions where access to the documentation stored on EDMS may be required. Only FMCSA employees and authorized contractors have access to information stored on this system; it is not available to the public.

Records maintained in the system are used for two purposes: Carrier documentation is stored as the official record of contact with the carriers. This information may include MCS-150's, Compliance Reviews, Inspection Reports, and other carrier-related documentation for use in cases brought against the carrier, or for historical purposes. Administrative records maintained in this system pertain to FMCSA personnel and FMCSA business processes and projects.

Users of this system are FMCSA personnel and authorized contractors who require access to project information stored on the system. This system gives FMCSA personnel and specified contractors the ability to easily and efficiently search for documents, and eases the burden of manually filing documents. The FMCSA personnel and/or contractors upload documents to EDMS with required index information, and documents are then available to personnel who have access to the individual library where the documents are stored.

Designated and approved compliance officials and data entry representatives have direct access to EDMS data. Designated FMCSA staff members also have direct access to EDMS. Different individuals receive different rights in EDMS according to their job role.

FMCSA may also share PII in EDMS with other federal agencies to assist with national security or other compliance activities. The FMCSA evaluates each request on an individual basis and oversees the process to ensure all Privacy Act procedures are followed.

The following groups have access to EDMS:

- FMCSA Users - Authorized FMCSA users have full access to all of the data to review and monitor the applications. A User ID and password is required to access the system.
- System Administrators and Developers - Federal contractors (System administrators and developers) have full access to EDMS to perform their assigned roles and responsibilities (development and maintenance of the system).

EDMS can be accessed via the single sign-on (SSO) FMCSA. Access through the FMCSA Portal is restricted to FMCSA enforcement personnel, FMCSA Headquarters (HQ) staff, and state agencies.

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 FMCSA ensures that the collection, use, and maintenance of information collected for operating the EDMS system 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 EDMS system itself does not provide internal data quality and completeness checks, as the system is essentially a repository for documents. Individuals inputting information into EDMS are responsible for inputting correct information. As such, checks to ensure that PII in the EDMS system are accurate, relevant, timely, and complete, occur prior to submission to the system.

Individuals who must submit PII in order to obtain direct access to EDMS submit this information directly. These individuals may contact their approving supervisor for any corrections to submitted information. As detailed above in *Individual Participation and Redress*, Individuals can use the FMCSA DataQs system to challenge information included in their records.

Security

DOT shall implement administrative, technical, and physical measures 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.

PII is protected by 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 Federal Information System Management Act (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 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013. FMCSA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII
- Protect against unauthorized access to or use of PII

Records in the EDMS system are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems' security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in the EDMS system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. All records in the EDMS system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the EDMS system is logged and monitored.

Logical access controls restrict users of the EDMS. These controls are guided by the principles of least privilege and need to know. Role-based user accounts are created with specific job functions allowing only authorized accesses, which are necessary to accomplish assigned tasks in accordance with compelling operational needs and business functions of the EDMS system. Any changes to user roles required approval of the System Manager. User accounts are assigned access rights based on the roles and responsibilities of the individual user. Individuals requesting access to EDMS must submit some personal information (e.g., name, contact information, and other related information) to FMCSA as part of the authorization process. Such authorized users may add/delete data commensurate with their requirements.

Users are required to authenticate with a valid user identifier and password in order to gain access to EDMS. This strategy improves data confidentiality and integrity. These access controls were developed in accordance with Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* dated March 2006 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems,* dated April 2013. Regular monitoring activities are also performed annually to provide ongoing oversight of security controls and to detect misuse of information stored in or retrieved by EDMS.

The EDMS maintains an auditing function that tracks all user activities in relation to data including access and modification. FMCSA prevents unauthorized access to data stored in the EDMS system through technical controls including firewalls, intrusion detection, encryption, access control list, and other security methods. These controls meet Federally mandated information assurance and privacy requirements.

FMCSA personnel and FMCSA contractors are required to attend security and privacy awareness training and role-based training offered by DOT/FMCSA. This training allows individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly and securely act in situations where they may use PII in the course of performing their duties. No access will be allowed to the EDMS prior to receiving the necessary clearances and security and privacy training as required by DOT/FMCSA. All EDMS users are made aware of the FMCSA Rules of Behavior (ROB) for IT Systems prior to being assigned a user identifier and password and prior to being allowed access to EDMS.

A security authorization is performed every year to ensure that EDMS meets FMCSA and Federal security requirements. EDMS also undergoes an additional security authorization whenever a major change occurs to the system. EDMS is assessed in accordance with the Office of Management and Budget (OMB) Circular A-130 Appendix III, Security of Federal Automated Information Resources, and the DOT Certification and Accreditation Guidance. The EDMS is approved through the Security Authorization Process under the National Institute of Standards and Technology. As of the date of publication of this PIA, the EDMS was last authorized in September 04, 2014.

Security Assurances Inherited from the AWS Cloud

Use of the AWS Cloud allows FMCSA to re-use and leverage a FedRAMP-compliant cloud system environment and approved Federal cloud service provider (CSP). The AWS FedRAMP-compliant environment consists of the AWS Cloud network and AWS internal data center facilities, servers, network equipment, and host software systems that are all under reasonable control by AWS. The AWS Cloud environment and service facilities are restricted to US personnel, and all AWS Cloud community customers are restricted to US government entities from Federal, state or local government organizations.

The AWS environment had been evaluated and tested by FedRAMP-approved independent third-party assessment organizations (3PAOs). The AWS is designed to meet NIST SP 800-53 minimum security and privacy control baselines for information and/or Federal information systems' risk up to Moderate impact levels. As confirmed through audit, the AWS addresses recent requirements established by NIST SP 800-171 for Federal agencies to protect the confidentiality of controlled unclassified information in non-federal information systems and organizations. AWS provides FIPS Pub 140-2-compliant services to protect data-at-rest with AES-256-based encryption and validated hardware to secure connections to the AWS.

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.

FMCSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to FMCSA privacy and security policies and regulations. FMCSA follows the Fair Information Principles as best practices for the protection of information associated with the EDMS system. In addition to these practices, policies and procedures are 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 data. Guidance will be provided in the form of mandatory annual Security and privacy awareness training as well as DOT/FMCSA Rules of Behavior. The FMCSA Security Officer and FMCSA Privacy Officer conduct regular 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.

Audit provisions are also included to ensure that EDMS is used appropriately by authorized users and monitored for unauthorized usage. All FMCSA information systems are governed by the FMCSA Rules of Behavior (ROB) for IT Systems. The FMCSA ROB for IT Systems must be read, understood, and signed by each user prior to being authorized to access FMCSA information systems, including EDMS.

Responsible Official

Richard Kim
EDMS System Owner
(202) 366-6830
Richard.Kim@dot.gov

Approval

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov