U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

Enforcement Management Information System (EMIS)

Responsible Official

Barbara Baker

Application Development Team Lead | IT Development Division

(202) 366-3397

Barbara.Baker@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 11:55:38 -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 Enforcement Management Information System (EMIS) web-based system that monitors, tracks, and stores information related to FMCSA enforcement actions. EMIS collects Personally Identifiable Information (PII) in order to track safety-related data in the hopes of recognizing trends that can be useful when making policy and other changes. Data is collected to identify individuals involved in enforcement actions, and to track and manage enforcement actions.

This Privacy Impact Assessment (PIA) update is necessary to addresses risks associated with migrating the EMIS 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.

[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).

Introduction & System Overview

EMIS Online is a web-based system that supports FMCSA's overall mission of keeping unsafe drivers and trucks off of the nation's highways. EMIS manages and tracks enforcement actions associated with notifying the carrier, monitoring the carrier's response, determining whether further compliance action is required, and generating reports for various FMCSA Headquarters, FMCSA Service Center, and FMCSA Division staff. It is an authoritative source for FMCSA enforcement data. EMIS imports census files, investigatory files, driver/vehicle safety violations and inspection data, and crash data from MCMIS for the purpose of automatically initiating UNFIT/UNSATISFACTORY cases within EMIS resulting from Safety Rating letters generated by MCMIS. The EMIS application has a limited scope and neither addresses compliance reviews nor makes the initial determination that an enforcement action is required.

Further, EMIS supports FMCSA enforcement of Federal laws and regulations designed to ensure the safety of commercial motor carriers and shippers engaged in interstate operations within the United States. This system maintains a comprehensive record of FMCSA enforcement actions taken against interstate carriers, hazardous materials shippers, and individuals subject to the Federal Motor Carrier Safety Regulations (FMCSRs) and Hazardous Materials Regulations (HMRs).

Personally Identifiable Information (PII) and EMIS

EMIS records include information on enforcement cases initiated by FMCSA against companies and drivers of commercial motor vehicles (i.e. trucks with a gross combination weight of 10,001 pounds or more, buses used to transport more than nine passengers, including the driver), and vehicles transporting hazardous materials. It also includes information on cases against shipping and freight forwarding companies registered with FMCSA. Specific information related to individuals is maintained on:

- Drivers associated with enforcement actions resulting from vehicle inspections and crashes investigated by Federal and state motor carrier enforcement officials;
- Officials associated with the motor carrier companies and/or drivers who are the subject of enforcement actions recorded in the system; and
- FMCSA and state officials authorized access to EMIS via assigned user accounts.

Records and reports in this system are referenced by a unique Enforcement Case Number. Each Enforcement Case Record may include:

1. **Subject Identification Information:** USDOT Number, subject's name, address, phone numbers, type of operation, Employer Identification or Social security number, etc. The subject of an enforcement action may be a company or an individual.
2. **General Case Information:** Information related to the persons and organizations initiating and managing the action, which may include originating Division and/or Safety Investigator, managing Service Center and/or Enforcement Specialist, etc.
3. **Contact Information:** Names, addresses and phone numbers of persons with an interest in the case, including subject's point of contact, legal advisor, etc.
4. **Violation and Fine Information:** Specific federal laws and regulations for which the subject is being prosecuted and the counts and fines being assessed for each.

5. **Fine Payment Information:** Data associated with the subject's payment of fines assessed as a result of an enforcement action.
6. **Actions Taken Information:** Chronological list of activities associated with management of the case with comments and users inputting the data.
7. **Document References:** Link to electronic documents associated with management of the case.

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 EMIS, 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.

EMIS contains PII for only drivers of commercial vehicles, contacts for commercial carriers and shippers, and State and local officials requiring access to the system. Drivers and commercial carrier representatives are required by law to provide PII as part of the inspection and crash data collection process and EMIS does not provide additional notice or options for consent.

Notice is also provided to individuals through the Privacy Act System of Records Notice (SORN) for EMIS (DOT/FMCSA 002 - Motor Carrier Safety Proposed Civil and Criminal Enforcement Cases - 65 FR 83124 - December 29, 2000). The EMIS SORN is available to the public on the DOT Privacy Office website and from the Federal Register (http://www.gpo.gov/fdsys/pkg/FR-2000-12-29/pdf/00-33365.pdf). The EMIS web interface also provides notice, via the DOT Privacy Policy, to all individuals who enter their own PII into EMIS.

FMCSA informs the public that their PII is stored and used by EMIS through this Privacy Impact Assessment published on the DOT website. This document identifies the information collection's purpose, FMCSA's authority to store and use the PII, and all uses of the PII stored and transmitted through EMIS. The EMIS PIA is available at https://www.transportation.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 the EMIS system through its Motor Carrier Information Management system (MCMIS) and DataQs system.

EMIS imports data, some of which is PII, from the MCMIS database on a nightly basis. The uploaded data is not altered in any way once it enters the system. The MCMIS system obtains information, including PII, from commercial motor carriers when they apply for, or update, their USDOT Number information. Carriers apply using the MCSA-1 form or the Unifed Registration System (URS) and modify their records using the MCS-150 form and/or the MCMIS website.

At any time, a motor carrier can log into the MCMIS website using their PIN number, and update the information that is stored, including any PII data. Motor carriers also currently have the option of filling out an updated MCS-150 form and mailing it to FMCSA-HQ for data entry.

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 EMIS. 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. EMIS will receive the changed information through 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 EMIS 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 primary purpose of EMIS is to provide FMCSA personnel with the information to make enforcement decisions and to maintain historical documents in the case of an appeal. EMIS records include information on enforcement cases (including SSN) initiated by FMCSA against companies and drivers of commercial motor vehicles (i.e. trucks with a gross combination weight of 10,001 pounds or more, buses used to transport more than nine passengers, including the driver,) and vehicles transporting hazardous materials. It also includes information on cases against shipping and freight forwarding companies registered with FMCSA.

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 that data that are relevant and necessary for the purpose of EMIS. EMIS 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).

EMIS tracks and stores FMCSA enforcement information, such as FMCSA enforcement actions taken against motor carriers, hazardous materials shippers, and drivers of commercial motor vehicles. EMIS also monitors motor carrier payments of FMCSA-ordered civil penalities, motor carrier responses to FMCSA, and FMCSA notifications to motor carriers.

Retention and disposal of EMIS records is managed in accordance with the NARA-approved records disposition schedule for the EMIS system (N1-557-10-1) Item 1. The length of retention time for EMIS documents depends on whether the information falls under inputs, master data files, documentation, or outputs. For any information entering EMIS, the data is destroyed or deleted, regardless of media, 10 years after information is imported into the EMIS 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 only by FMCSA employees and authorized contractors to perform functions according to the business needs of the Federal Motor Carrier Safety Administration. Access to the EMIS system is not available to the public.

Records maintained in the system are used for two purposes: enforcement decisions and historical documentation for appeals. This data is used by FMCSA personnel to monitor carrier and driver enforcement cases, monitor payment data, and track historic carrier performance.

Designated FMCSA staff members and designated and approved State and local compliance officials and data entry representatives have direct access via the FMCSA Portal to EMIS data. Different individuals receive different rights to access information in EMIS according to their job role and business need.

FMCSA may also share with other federal agencies PII in EMIS to assist with national security or other compliance activities. FMCSA evaluates each request on an individual basis and oversees the process to ensure all procedures are followed pursuant to the Privacy Act of 1974.

The following groups have access to EMIS:

- FMCSA and State Enforcement 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 the L&I to perform their assigned roles and responsibilities (development and maintenance of the system).

EMIS 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 EMIS 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 EMIS system provides internal data quality and completeness checks. Sources of information, such as State police departments or other officials, are responsible for inputting correct information. The EMIS system's functionality provides internal data quality and completeness checks. For example, uploads to the system from the CaseRite

application validate against the violation table in EMIS and ensure that correct violations are cited. In addition, for the PII that has been collected through the Motor Carrier Management Information System (MCMIS), please refer to the MCMIS PIA for additional elements in place.

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 EMIS 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 EMIS 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 EMIS system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the EMIS system is logged and monitored.

Logical access controls restricts users of the EMIS. 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 EMIS 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 EMIS 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 EMIS. 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 EMIS.

The EMIS maintains an auditing function that tracks all user activities in relation to data including access and modification. Through technical controls including firewalls, intrusion detection, encryption, access control list, and other security methods; FMCSA prevents unauthorized access to data stored in the EMIS system. 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 EMIS prior to receiving the necessary clearances and security and privacy training as required by DOT/FMCSA. All users at the federal and state level 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 EMIS.

A security authorization is performed every year to ensure that EMIS meets FMCSA and federal security requirements. EMIS also undergoes an additional security authorization whenever a major change occurs to the system. EMIS 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 EMIS 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 EMIS was last authorized in June 30, 2015.

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 EMIS 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 is 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 EMIS 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 EMIS 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 EMIS.

Responsible Official

Barbara Baker
Application Development Team Lead | IT Development Division
(202) 366-3397
Barbara.Baker@dot.gov

Approval

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