U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

FMCSA Portal

Responsible Official

James L. Vasser
Application Development Team Lead
(202) 493-0215
jamie.vasser@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
Date: 2019.07.10 09:57:34 -04'00'

Executive Summary

The U.S. Department of Transportation's (DOT) Federal Motor Carrier Safety Administration (FMCSA) core mission is to reduce commercial motor vehicle-related crashes and fatalities. To further this mission, FMCSA created the FMCSA Portal (https://portal.fmcsa.dot.gov/login) to provide the industry motor carriers, federal employees and contractors, state and local employees, with single sign-on capability to several critical FMCSA information systems. The FMCSA Portal integrates new technologies with FMCSA business practices and allows FMCSA to quickly and efficiently respond to evolving business requirements, significantly expand IT delivery capabilities, and reduce IT operation and maintenance costs. This Privacy Impact Assessment (PIA) update is necessary to address risks associated with migrating the FMCSA Portal system to the FMCSA Cloud Environment.

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*
- *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 of M-03-22 dated September 26, 2003).

Introduction & System Overview

The FMCSA Portal (https://portal.fmcsa.dot.gov/login) is a web-based system that supports most FMCSA information technology capabilities.[2] By optimizing FMCSA's business processes and improving IT functionality, the FMCSA Portal provides FMCSA, State enforcement personnel, and the motor carrier industry with resources needed to improve the safety of U.S. roadways. The FMCSA Portal, enables FMCSA to respond quickly to evolving business requirements, significantly expand IT delivery capabilities, and reduce IT operation and maintenance costs. The FMCSA Portal provides a single-entry point to multiple FMCSA information systems for internal and external users in compliance with the E-Government Act of 2002.

The FMCSA Portal allows individuals to request a FMCSA Portal account, as well as make modifications to these requests. Motor carriers use the FMCSA Portal to access crash, inspection, reviews, and census information contained on them in various FMCSA IT systems through a single interface.

In addition to providing single sign-on access to the systems referenced above, the FMCSA Portal also provides:

- Direct web access to the FMCSA Portal; allowing FMCSA enforcement users[3] to access crucial data during roadside inspections and when working from other remote locations;
- FMCSA enforcement users with the proper roles the ability to make assignments for compliance reviews, safety audits and corrective action plans to federal and state field personnel. Assignments can be viewed and managed by enforcement users via the Portal or from Excel spreadsheet reports downloaded from the portal;
- Users with the ability to request FMCSA Portal accounts and modify requests directly from the FMCSA Portal. Users were previously required to submit paper-based forms to the Technical Support Hotline to request and modify accounts. Administrative users can run advanced user searches, disable or enable users, verify user accounts annually, and transfer administrative roles. Individual users can request a forgotten User ID, unlock a locked account, and receive automatic notifications when their passwords are getting ready to expire; and
- Enforcement with access to all company data in the same format as that seen by Motor Carriers.

The FMCSA Portal is an aggregated information management system that was created with the express purpose of allowing law enforcement and motor carriers to manage carrier safety information and address safety concerns. As a result, one of the portal's primary purposes is to make safety information available to the user in a very clear manner. The FMCSA Portal contains three types of information:

- Information provided directly by the individual or motor carrier company;
- Information acquired from external sources pertaining to safety compliance; and
- Information on the road safety performance of motor carriers so that FMCSA can identify unsafe carriers, prioritize them for intervention, and monitor if a motor carrier's safety and compliance problem is improving.

[2]The systems and applications accessible via the FMCSA Portal are: Motor Carrier Management Information System (MCMIS), Enforcement Management Information System (EMIS), Licensing and Insurance (L&I) System, DataQs, Query Central (QC), Analysis and Information (A&I) Online, Safety and Fitness Electronic Records (SAFER), Electronic Document Management System (EDMS), National Consumer Complaint Database (NCCDB), and FMCSA Information Systems Website (InfoSys).

[3]FMCSA enforcement users - Field Safety Investigators, Safety Auditors, Division personnel, Service Center Personnel, HQ and State partners

Personally Identifiable Information (PII) and FMCSA Portal

The FMCSA Portal collects and stores only the PII necessary to enable authorized users to sign into the Portal. Through the electronic registration process users submit specific information to complete the process of signing up for an account. As a result, the FMCSA Portal contains PII of employees of industry motor carriers, federal government employees and contractors, and state and local employees and contractors. The following information is collected from users through the electronic application process:

- Username;
- Password;
- Last, First, and Middle Name;
- Business Email address;
- Business Telephone number;
- Business Address;
- USDOT Number; and
- User-chosen personal security questions and responses (such as Mother's Maiden Name, Maternal Grandmothers Name, or the City where the user was born).

This PIA addresses only the FMCSA Portal; and not the underlying FMCSA IT systems that are accessible via the FMCSA Portal. PIAs specific to those systems are published on the DOT privacy website: (https://www.transportation.gov/privacy).

Move to the FMCSA Cloud Environment

As part of FMCSA's on-going plans to modernize and enhance IT tools that support FMCSA mission processes for registration, inspection, compliance monitoring and enforcement, the FMCSA Portal has been migrated from a private in-house 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 AWS Cloud. In following this technical migration approach, FMCSA enterprise applications were not redesigned or modified.

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 Flipped 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[4], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information

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

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[5].

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.

FMCSA clearly discloses its policies and practices concerning the collection and maintenance of PII by the FMCSA Portal in this PIA. The Information is collected directly from the user with the user's clear and explicit participation and consent. Data provided by the user is not submitted until the user has read and consented to the FMCSA Rules of Behavior. The Rules of Behavior provides expected privacy related behaviors require user to acknowledge and accept them. Authorized users of the FMCSA Portal have access to the information that they submitted about themselves as part of the user registration process.

The FMCSA Portal also provides users with training designed to inform the user of how to operate the FMCSA Portal, as well as the individual user's responsibilities when accessing the system. In addition, the FMCSA Portal provides clear links to the DOT privacy policy. DOT has provided generalized notice to the public of its use of login/access records through the System of Records Notice (SORN), DOT/ALL – 13 (67 FR 30757 - May 7, 2002) Internet/Intranet Activity and Access Records Systems of Records. Additionally, FMCSA informs the public of how their PII is collected, stored, and used by the FMCSA Portal through this Privacy Impact Assessment (PIA), published on the DOT website. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the PII, as well as all uses of the PII collected and stored by the FMCSA Portal. The Privacy Policy, SORN, and FMCSA Portal PIA are available at https://transportation.gov/privacy.

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 ensures that an individual has the right to: (a) obtain confirmation of whether FMCSA has records containing PII relating to him or her; (b) access the record related to him or her within a reasonable time, at little if any cost, and in a form, that is easily understood; (c) obtain an explanation if a request is denied, and challenge such denial; and (d) challenge records relating to him or her and, if the challenge is successful, have the record amended. Individuals may request access to their records that are maintained in a system of records in the possession and under the control of DOT by complying with DOT Privacy Act regulations, 49 CFR Part 10. Privacy Act requests for access to an individual's record must be in writing either handwritten or typed, may be mailed, faxed or emailed. DOT regulations require that the request include; a description of the records sought, the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or include a

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

statement that the information submitted is accurate. The statement must be attested to under penalty of perjury. Additional information and guidance regarding DOT's Privacy program is located on the DOT website www.transportation.gov/privacy.

FMCSA obtains consent for records created in the FMCSA Portal through the process of account creation. That is, all personal data maintained by the FMCSA Portal is collected directly from the user to establish a user account. Before the user submits the data, they are required to consent to a Rules of Behavior form which addresses both privacy and proper handling of the information contained in the system. At any point of the collection process, the user can cancel the process if concerns arise. In addition, all information provided by the user is directly accessible and modifiable by the user, so errors in the information may be corrected by the user at any time. Users may also contact the Service Provider Help Desk at FMCtechsup@dot.gov or 617-494-3003 to request that information be corrected or updated.

Under the provisions of the Privacy Act, individuals may request searches of the FMCSA Portal to determine if any records in the Portal 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.

Title II, section 207 of the E-Government Act of 2002 requires Government agencies to improve the methods by which government information, including information on the Internet, is organized, preserved, and made accessible to the public. The FMCSA Portal is the agency wide initiative to improve its business processes, integrate them with the Agency's information systems, and make them more seamless, secure, and supportive of the Agency's mission of saving lives by providing single sign-on access to the systems listed in the Introduction and System Overview section.

The FMCSA Portal also provides Carriers a single location where they can view their data. The Portal queries directly from the authoritative sources, MCMIS, EMIS, L&I, SAFER, EDMS, NCCDB, and InfoSys. This allows carriers to have access to data that is uploaded within 24 hours, which is more current data than what was previously available to them through A&I or SAFER. A&I and SAFER upload carrier data monthly. The that may be downloaded by carriers includes compliance reviews, safety audits, inspections, crashes and closed enforcement case information. It also includes safety performance of a motor carrier, Census information, and operation type. The data does not include PII. Carriers can also generate their own safety profiles within the FMCSA Portal at no cost and provide third-party entities with online access to their safety and operational data. The use of PII by the FMCSA Portal is limited to user authentication. There will be no subsequent uses of PII unless individuals are given written notice of the proposed change in use, and individuals provide written consent for its use for such new purpose.

The Introduction and System Overview section of this PIA discusses the PII used to create an FMCSA Portal account. Information is collected to ensure that the username and password match and are valid. The records in this system are used to electronically authenticate users and to prevent unauthorized access to FMCSA IT systems. As part of the security authentication framework, the FMCSA Portal also collects answers to user-chosen personal questions. This

information is used only to identify the user later in the event the primary credentials are corrupt or unavailable, and are never transmitted to the applications that may be accessed through the system.

User contact information is also used to send messages and alerts to the user, as needed. Messages are sent via both postal mail and email. Messaging is a fundamental requirement of the FMCSA Portal to alert the user to critical actions or states, as well as to deliver correspondence necessary to notify and resolve safety issues.

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.

The FMCSA Portal only uses and retains data that are relevant and necessary to authenticate users and provide them with access to their MCMIS, EMIS and L&I data. The Portal collects basic user contact information, security information, organizational information to establish authorization capacities and provide driver/carrier safety statistics that pertain to the specific goal of the FMCSA Portal. Collected information includes:

- Last, First, and Middle Name
- Business Email address
- Business Telephone number
- Business Address
- USDOT Number

The FMCSA Portal requires this information for creating an account. For account security, the Portal prompts users to select from a list of security questions (i.e. – Mother's Maiden Name, Maternal Grandmothers Name, or the City where the user was born) and provide the response. Three security questions are required. The system uses this information only to identify the user later in the event the primary credentials are corrupt or unavailable, and are never transmitted to any other part of the FMCSA Portal or any other system.

The FMCSA Portal uses User contact information to identify the user and to send messages and alerts to the user, as needed. Messages are sent via both postal mail and email. Messaging is a fundamental function of the portal, as it allows FMCSA to alert the user about critical actions or status, as well as to deliver correspondence necessary to notify and resolve safety issues.

Organizational information concerning the user's affiliated company or law enforcement office is used to:

- Establish chains of authority to determine which user(s) can approve certain requests made by the user
- Determine what information the user can access based on what they have authority over

The FMCSA Portal maintains user profile records in accordance with National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.2 Information Systems Security Records, Item 30 (System Access Records). FMCSA deletes User Identification, Profiles, Authorizations, and Password files when the agency determines the business uses ceases.

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 restricts the collection of data to that necessary to meet the authorized business purpose in support of Agency mission. The FMCSA Portal collects PII from industry motor carrier employees, federal government employees and contractors, and state and local employees and contractors to grant single sign-on access to several critical FMCSA information systems via the web. Information is collected to initially authenticate users by validating against the user name tables in the database to ensure that the username and password match are valid. Safety inspections, which contain PII about drivers, are viewable via the FMCSA Portal. No PII is transmitted to any third-party or external FMCSA systems.

FMCSA restricts access to the FMCSA Portal to FMCSA enforcement personnel, FMCSA Headquarters (HQ) staff, state agencies, and Motor Carriers. The authentication information in The FMCSA Portal is not shared outside of the agency.

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 information viewed in the FMCSA Portal 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 FMCSA Portal has strict input validation checks on all data supplied during account creation. It will reject all requests that contain invalid data types. If a data type has been rejected, the system displays an error message. FMCSA Portal prohibits users from submitting account information when applying for an account unless all required data fields are completed in a valid format.

The FMCSA Portal provides direct access to systems on which the PII is maintained. Individuals who wish to update their PII in MCMIS, EMIS, L&I, SAFER, EDMS, NCCDB, and InfoSys may use the FMCSA Portal to access those systems. The individuals who submit their personal information are responsible for the accuracy of the information they submit to those systems.

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, and
- Protect against unauthorized access to or use of PII.

FMCSA safeguards the records in the FMCSA Portal in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. FMCSA imposes strict controls to minimize the risk of compromising the information that is being stored. FMCSA also limits access to records in the FMCSA Portal 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 FMCSA Portal are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the FMCSA Portal system is logged and monitored.

The FMCSA Portal restricts users by logical access controls. These controls are guided by the principles of least privilege and need-to-know. FMCSA Portal administrator creates role-based user accounts with specific job functions. These accounts allow only the level of access, necessary to accomplish assigned task. Tasks are assigned in accordance with operational needs and business functions of the FMCSA Portal. Any changes to user roles require approval of the System Manager. FMCSA assigns user account access rights based on the roles and responsibilities of the individual user. Individuals requesting access to FMCSA Portal must submit 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 assigned roles.

Security Assurances Inherited from the AWS Cloud

FedRAMP-approved independent third-party assessment organizations (3PAOs) evaluated and tested the AWS environment. 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 identifies, trains, and holds accountable Agency personnel for adherence 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 FMCSA Portal. In addition to these practices, FMCSA consistently applies policies and procedures, 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 Rules of Behavior. The FMCSA Security Officer and FMCSA Privacy Officer conduct regular security and privacy compliance reviews of the FMCSA Portal consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Audits are completed to ensure that FMCSA Portal 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, acknowledged as understood, and signed by each user prior to being authorized to access FMCSA information systems, including FMCSA Portal.

Responsible Official

James L. Vasser
Application Development Team Lead
IT Development Division

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer