OCIO Office of the DOT Chief Information Officer

U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)
Motor Carrier Management Information System (MCMIS)

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 12:55:29 -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 Motor Carrier Management Information System (MCMIS), a system used to collect and maintain records on commercial vehicle safety as well as a national inventory of motor carriers and shippers subject to the Federal Motor Carrier Safety Regulations and Federal Hazardous Materials Regulations (FHMRs). This system is used by Federal and state users as well as the motor carrier industry, law enforcement, and the general public.

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

The Motor Carrier Management Information System (MCMIS) is the computerized information system supporting FMCSA in monitoring the safety of commercial motor carriers and shippers engaged in interstate operations within the United States. This system provides for the collection, storage, maintenance, analysis, and dissemination of comprehensive safety performance records for approximately 2.5 million registered commercial carriers and hazardous material shippers subject to the FMCSRs or FHMRs. The MCMIS database assembles data at the Federal and state levels from numerous state-based systems and other information sources, providing comprehensive information for interstate carriers that would otherwise be unavailable to individual states or FMCSA service centers. While the primary role of MCMIS is to manage information pertaining to interstate carriers and shippers, an increasing amount of information has been collected since 1995 for intrastate non-hazardous material carriers. MCMIS also collects information on approximately 10,000 cargo tank manufacturers.

MCMIS supports the DOT strategic goals of Safety, Homeland Security, and Organizational Excellence. In support of Safety and Homeland Security goals, the MCMIS system provides multiple agencies—namely the Bureau of Customs and Border Protection (Department of Homeland Security), and Federal and State roadside commercial vehicle inspectors, who conduct commercial motor vehicle enforcement activities and monitor hazardous materials shipping by motor carrier—with access to a federally based central repository. This central repository maximizes the efficient sharing of current, accurate, and timely information about commercial motor vehicle drivers and motor carriers at the U.S./ Mexican and U.S./ Canadian borders, enabling FMCSA's partners to act quickly in times of possible security breaches.

MCMIS supports the FMCSA Safety goal by providing data on the New Entrant Program, which is used to monitor new motor carriers applying for a USDOT registration. The carriers are monitored 18 months before permanent USDOT registration is issued. This program also monitors FMCSA performance on the number of motor carriers that are educated about Federal Motor Carrier Safety Regulations (FMCSR) and Hazardous Materials Regulations (HMR).

MCMIS also supports Organizational Excellence by improving government-to-government, government-to-business, and government-to-citizen services. MCMIS is built to increase system reliability and customer satisfaction (through ease of use and reducing customer complaints/inquiries), improve data quality by maintaining accurate data, reduce repetitive manual data entry (by increasing the number of online filings of the MCSA-1 and MCS-150 forms for biennial updates), and provide a data warehouse of information needed by FMCSA employees who strive to meet agency goals and protect our highways. This investment supports future changes to the 49 Code of Federal Regulations (CFR) regulations that produce the information requirements that MCMIS supports.

Personally Identifiable Information (PII) and MCMIS

The MCMIS system uses both personally identifiable information (PII) and non-personally identifiable information within the Registration (census), Crash, Inspection, safety audit, and compliance review files. MCMIS provides two sets of data files, one with PII, and one without.

The MCMIS dataset that includes PII may contain PII such as truck/bus driver name, truck/bus driver social security number, driver and company contact information, registration number, and EIN. Only designated individuals, such as insurance companies, carriers, safety consultants, can obtain access to this data, through a written request that the

FMCSA, Enforcement office, reviews and approves. In order to fulfill these requests, FMCSA collects requestor PII, such as name, telephone number, mailing address, and organization.

The MCMIS dataset that does not include PII is available to any individual on request through a Web-accessible, or by mail-in form. FMCSA requires some PII from individuals requesting copies of reports such as name, phone number, and mailing address.

FMCSA also provides direct access to MCMIS for some designated users who may have a need to have multiple accounts/user profiles based on their job responsibilities. In order to control access, FMCSA maintains name, contact information, user ID, password, and organization information on these users. FMCSA uses this PII to authorize or deny access, determine and set permissions, enable access, and contact users if concerns arise.

Move to the FMCSA Cloud Environment

As part of the Administration's on-going 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 MCMIS 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 direct access and or Intranet access to MCMIS, users must read and agree to a warning message that discusses the penalties of unauthorized access before logging in. The MCMIS 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 MCMIS (DOT/FMCSA 001 - Motor Carrier Management Information System (MCMIS) - 78 FR 59082 - September 25, 2013). The MCMIS SORN is available to the public on the DOT Privacy Office website and from the Federal Register (http://www.gpo.gov/fdsys/pkg/FR-2013-09-25/pdf/2013-23131.pdf). The MCMIS web interface also provides notice, via the DOT Privacy Policy, to all individuals who enter their own PII into MCMIS.

FMCSA informs the public that their PII is stored and used by MCMIS 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 MCMIS. The MCMIS 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 MCMIS system through MCMIS itself and the DataQs system.

At any time, a motor carrier can log into the MCMIS website using a 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 to FMCSA-HQ for data entry.

In addition, MCMIS includes a link to the 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 submit a request for data review of the 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 MCMIS. 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.

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 A&I 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

If an individual believes more than one Operating Administration maintains Privacy Act records concerning him or her, the individual may submit the request to:

Departmental Freedom of Information Act Office
ATTN: FOIA request
U.S. Department of Transportation, Room W94–122
1200 New Jersey Avenue SE
Washington, DC 20590

When seeking records about yourself from MCMIS or any other Departmental system of records, the request must conform with the Privacy Act regulations set forth in 49 CFR Part 10. The request must be signed, and the requestor’s signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Freedom of Information Act Officer, http:// www.dot.gov/foia or 202.366.4542. In addition, the requestor should provide the following:

- An explanation of why the requestor believes the Department would have information on him/her;
- Identify which component(s) of the Department the requestor believes may have the relevant information;
- Specify when the requestor believes the records would have been created;
- Provide any other information that will help the Freedom of Information Act (FOIA) staff determine which DOT component agency may have responsive records; and if the request is seeking records pertaining to another living individual, the requestor must include a statement from that individual certifying his/her agreement for the requestor to access his/her records. Without this bulleted information the component(s) may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

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 purpose of MCMIS is to provide a central collection point for records on intrastate motor carriers, interstate motor carrier, hazardous material shipper, freight brokers and freight forwarders in order to facilitate the analysis of data required to administer and manage the agency's safety and commercial enforcement programs.

MCMIS collects PII in order to track safety-related data in the hopes of recognizing trends that can be useful when making policy and other changes. MCMIS provides some or all of this information to companies, agencies, individuals, and other organizations in order to help facilitate communication needed to enhance motor carrier safety.

In addition, in order to process requests for reports, FMCSA collects PII such as name, mailing address, and telephone number from requesting individuals. For individuals with direct access to MCMIS, FMCSA also collects necessary PII to authenticate users and restrict permissions, and MCMIS associates these individuals with users IDs and passwords.

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 MCMIS. MCMIS 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). Records in MCMIS may be retrieved by; individuals' name, Social Security Number, Employer Identification Number, company name, trade name, and geographical location.

MCMIS records are retained and destroyed in accordance with applicable NARA retention schedule N1-557-05-07 Item #5. The master backup tape is designated for deletion under this retention schedule when 5 years old, when no longer needed, or when information is superseded or becomes obsolete, whichever is sooner.

Records in this 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 records in this 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 or permissions.

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 MCMIS system obtains information, including PII, from roadside CMV and CMV driver inspections and crash reports submitted by State and local law enforcement agencies and from investigations performed by State and Federal investigators. Individuals can obtain all or part of MCMIS data through one of several ways. First, Federal and State offices have direct access to the MCMIS. Different individuals receive different rights in MCMIS according to their job role and State. Carrier companies and other individuals can learn about MCMIS information and request data through a publicly-available Web site: http://www.fmcsa.dot.gov/factsfigs/mcmis that provides mail-in forms. Motor carriers can also access the websites http://www.safersys.org or http:// safer.fmcsa.dot.gov to update their motor carrier identification information. To do this, motor carriers must know their USDOT number and their Personal Identification Number (PIN). Individuals can also access MCMIS through the FMCSA Portal. The FMCSA Portal is a web-enabled system designed to authenticate users to various FMCSA IT Systems. User accounts are assigned access rights based on the roles and responsibilities of the individual user. The PIA for the FMCSA Portal is published on the DOT privacy website (www.dot.gov/privacy).

The general public can access these same websites (http://www.safersys.org or http:// safer.fmcsa.dot.gov) to obtain a company safety profile (CSP) on a motor carrier. The CSPs are available to the public under the Freedom of Information Act (FOIA). However, certain information in the CSP, namely Driver Data, contains personal information that is not required to be disclosed by FOIA and will not be included in a CSP that is disseminated to the public. The CSP version available to a motor carrier will also include specific information about crashes and Hazardous Materials BASICS[2] which is not available to the general public user. Of course, a company may have access to its own Driver Data. For this reason, Driver Data will be released only to those who are registered as authorized recipients of that information. To register as an authorized recipient of Driver Data, the motor carrier must fax a request to 1-800-832-5660., the FMCSA Data Dissemination contractor. The requestor must submit the following information: a letter on the official company letterhead; it should include the USDOT number of the company; the letter must be signed by a representative of the company; if the requestor wishes to receive a CSP via e-mail, they must include any e-mail address(es) that they have approved to receive Driver Data information. When ordering online (http://www.safersys.org), the requestor needs to check the box labeled "I am the carrier whose USDOT number was entered above". The requestor then is prompted for the last 4 digits from their company Tax ID (EIN) number to complete the transaction (If no Tax ID is on file, the requestor needs to file an updated MCS-150 form with this information). Motor carriers who access MCMIS through the FMCSA Portal have the ability to request their own CSP through the Portal.

There are several MCMIS reports that do not contain PII and are available to anyone on request through mail-in forms provided on the Web site. FMCSA does not provide driver data to the public: information collected on a driver is ONLY provided to the motor carrier that employs the driver.

FMCSA and other Federal and State Enforcement agencies have direct access to PII data in MCMIS. In order to manage access and appropriate permissions, FMCSA collects name, contact information, organization information and other related information, and maintains user IDs and passwords for all users. Additionally, MCMIS provides reports containing PII to contractors working for FMCSA, government agencies, or contractors of State and Local governments with individual verification of affiliation and need. Recipients of this data must submit a written request form and additionally sign a Non-Disclosure document with privacy provisions. MCMIS staff individually reviews and approve or deny these requests, researching the appropriateness of the requests as needed. In order to obtain direct access to MCMIS, individuals provide PII to a higher-level approval authority within his or her organization and with the MCMIS staff. In most cases, the individual in question fills out a paper-based authorization form and sends that document to his or her supervisor. This supervisor approves or denies the request, and then sends any approvals to the MCMIS Technical Support staff for action. Individuals are also able to request access to MCMIS through the FMCSA Portal. Access through the FMCSA Portal is restricted to FMCSA enforcement personnel, FMCSA Headquarters (HQ) staff, State agencies and Motor Carriers.

[2] BASICs (Behavioral Analysis and Safety Improvement Categories) are the seven categories the FMCSA uses as part of the Safety Measurement System (SMS) to measure safety performance and create monthly scores.)

The MCMIS dataset that does not include PII is available to any individual on request through a Web-accessible, or by mail-in form. An individual must file a written request with FMCSA to obtain copies of data sets with PII information. FMCSA requires some PII from individuals requesting copies of reports. In order to fulfill these requests, FMCSA collects requestor PII such as name, telephone number, and mailing address.

Algorithms such as Safety Measurement System (SMS) make maximum use of MCMIS data (motor carrier performance and compliance data) to assess a motor carrier based on crash, driver, vehicle, and safety management data contained in the BASICs reports. FMCSA field staff use the results of the assessment to determine which carriers need a compliance review. The review information is entered into MCMIS where safety fitness ratings (Satisfactory, Conditional, Unsatisfactory) are assigned to carriers and made available to Federal, State and other requestors. The Inspection Selection System (ISS) is another algorithm that uses MCMIS safety data to prioritize commercial vehicles/drivers for roadside inspection. By targeting the vehicles and drivers most at risk of unsafe practices, crashes are prevented and lives are saved. Both compliance reviews and roadside inspections have been proven by FMCSA to be effective at preventing truck and bus crashes. MCMIS provides the technological strategy to accomplish the above by providing information to Federal, State, and local government agencies as well as to the public about motor carrier safety behavior and safe operations. For example, MCMIS data are used by: (1) State agencies for targeting motor carrier safety enforcement and for developing safety programs; (2) safety organizations to evaluate safety trends, promote safety programs, and evaluate the effectiveness of existing and proposed safety guidelines, enforcement standards, and rules, (3) insurance companies for evaluating potential clients; and (4) the general public to choose safe companies for household moving and bus transportation.

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 MCMIS 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 MCMIS system provides internal data edit checks on all data submitted to MCMIS. FMCSA data entry contractors have a verification process to ensure that accurate information is entered in MCMIS. MCMIS requires motor carriers to submit through the Unified Registration System (URS) a Motor Carrier Identification Report (MCSA-1) to obtain a USDOT Number and uses internal validation functionality to ensure that all required data fields have been completed on the MCSA-1.

FMCSA data entry contractors have a 4-step verification process to ensure that accurate information is entered in MCMIS regardless of whether the forms are received via fax or mail. When an application is received, the first step is to review the application to ensure that all required data elements are present. The next step is to verify that the data is correct. Step three is to enter the information into MCMIS. The last step is the verification and final approval of the data entered into MCMIS matches the data on the form.

Individuals who provide PII through FMCSA forms to request MCMIS reports provide that PII directly and are responsible for its accuracy. FMCSA staff reviewing and approving submitted forms check for completeness on required fields, and verify requirements when there is a question of whether a requestor has the right to a PII-containing report.

Individuals who must submit PII in order to obtain direct access to MCMIS submit this information directly to FMCSA. These individuals may contact their approving supervisor for any corrections to submitted information.

At any time, a user may request, through email, to telephone, to request that privacy practices be reviewed. This contact information is provided in the Privacy Policy, posted visible on the Web site.

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

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

The MCMIS 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 MCMIS 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 MCMIS 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 MCMIS.

A security authorization is performed every year to ensure that MCMIS meets FMCSA and federal security requirements. MCMIS also undergoes an additional security authorization whenever a major change occurs to the system. MCMIS 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 MCMIS 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 MCMIS 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 MCMIS 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 MCMIS 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 MCMIS 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 MCMIS.

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