U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)
FMCSA Service Center Applications

Responsible Official

Richard Scott
System Owner
(202) 385-2787
Richard.Scott@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: 2018.09.16 13:09:05 -04'00'

Executive Summary

The U.S. Department of Transportation's (DOT) Federal Motor Carrier Safety Administration 's(FMCSA) core mission is to reduce commercial motor vehicle-related crashes and fatalities. To further this mission, FMCSA created the FMCSA Service Center applications to help FMCSA manage commercial vehicle safety data and shipper safety data. The FMCSA Service Center applications support regional FMCSA Service Centers Division Offices, Field Offices and Southern Border Offices along with numerous roadside inspection sites across the country. FMCSA personnel such as attorneys, Safety Investigators, federal, state and local enforcement personnel, as well as the authorized MCSAP state lead agencies have access to the information collected through the FMCSA Service Center applications.

This Privacy Impact Assessment (PIA) is necessary to provide information regarding the FMCSA Service Center applications and the collection and use of Personally Identifiable Information (PII).

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 FMCSA Service Center Applications is a general term for multiple minor applications that support FMCSA's Compliance, Safety and Accountability (CSA) initiative along with service centers, field offices, border offices, and inspection sites across the United States. By optimizing FMCSA's business processes and improving IT functionality, the FMCSA Service Center applications provide FMCSA and State enforcement personnel and the motor carrier industry with resources needed to improve the safety of U.S. roadways. In addition, the FMCSA Service Center applications allow field users to easily upload information to other FMCSA IT systems.

FMCSA operates four FMCSA Service Centers: Eastern Service Center (ESC), Western Service Center (WSC), Midwestern Service Center (MWSC), and Southern Service Center (SSC) with the primary function of processing and storing FMCSA enforcement cases and reports. In addition, FMCSA operates numerous Field Offices and Southern Border Offices across the US. These sites focus on enforcement and safety compliance activities on motor carriers, drivers, and the vehicles they operate. Furthermore, there are many state and local government operated motor carrier inspection sites focusing on enforcement and safety compliance.

The FMCSA Service Center Applications do not store information, but allows users to upload information to FMCSA IT systems. Specific information flows are detailed below for each application. FMCSA has analyzed the privacy risks associated with each of these IT systems and all have individual PIAs available to the public on the DOT Privacy Office website (https://www.transportation.gov/individuals/privacy/privacy-impact-assessments).

To ensure that individuals at all of these sites across the country can effectively complete their missions, FMCSA operates multiple IT applications. The FMCSA Service Center Applications include the following applications, which are self-contained and exist as icons on desktop or laptop computers at service centers, field offices, border offices, and inspection sites across the United States.

ASPEN

Allows federal and state safety personnel to collect CMV and CMV driver information from roadside safety inspections and other FMCSA applications. Records and reports in this system include inspection information related to the driver which may include name, date of birth, driver's CDL number, and violation information (section, violation description, out of service (OOS), and citation information).

ASPEN is used to collect all the commercial driver/vehicle roadside inspection details. It uses several other applications that pull data from remote access - ISS, CDLIS Access, and QC. It also includes communication features to electronically transfer inspection details to Safety and Fitness Electronic Records (SAFER) and/or SAFETYNET. ASPEN collects the inspection details and prints these details in an associated report for the driver and carrier. In addition, ASPEN addresses the FMCSA's critical need for timely upload of inspection outcome/reports/details/whatever to SAFETYNET and the Motor Carrier Management Information System (MCMIS), Once the data is it is included in the SafeStat prioritization algorithm, which ranks CMV carriers for safety and prioritizes resource allocation for on-site compliance reviews. This information is also exported to CDLIS Access and CaseRite.

CaseRite

Assists federal prosecutors in creating legal cases for Federal Motor Carrier Safety Regulations (FMCSR) and FHMR violations. CaseRite collects driver PII including name, social security number, vehicle identification, mailing address and telephone numbers. The purpose of this application is to gather violation data that has been collected from roadside inspections and compliance review investigations. CaseRite integrates with other FMCSA Service Center applications (CAPRI, ASPEN, and UFA) by importing carrier and violation data to ensure efficiency and data integrity. This information is then collated and used to produce legal case documents for prosecution and subsequently uploaded into the Enforcement Management Information System (EMIS).

Compliance Analysis and Performance Review Information (CAPRI)

Provides federal and state safety personnel with information needed to conduct compliance reviews, safety audits, specialized cargo tank facility reviews, hazardous material shipper reviews, and security contact reviews. CAPRI cs including names, dates of birth, driver license numbers, and social security numbers for identifying drivers. It electronically transfers data through the CAPRI Web Service to MCMIS and to SAFETYNET.

ISS (Inspection Selection System)

Screens CMVs to determine if an inspection should be conducted. The ISS is the primary tool used on the roadside to screen motor carriers vehicles and determine the usefulness of conducting an inspection. ISS imports data from SAFER and returns the following: carrier identification data, an overall inspection value from 1 to 100, and additional safety performance indicators. ISS exports the safety evaluation data to ASPEN and improves data integrity by auto-populating carrier identification fields in the ASPEN inspection software.

UFA (Uniform Fine Assessment)

UFA performs the calculation of a uniform and reasonable fine amount based on the nature of the violation and the various criteria set forth in the Federal Motor Carrier Safety Regulations (FMCSRs). UFA is used to provide a uniform fine assessment to compliance reviews generated in CAPRI and brought to court through a case generated in CaseRite.

Investigators use UFA to help identify the reviews that should be carried on to the court system. Investigators install these three inter-related applications, UFA, CAPRI, and CaseRite, on their laptop or desktop computers. Federal Safety Specialists nationwide and some State Safety Specialists use UFA when performing on-site reviews at the carrier's primary place of business.

UFA does not have any network connection components. It uses export and import functionality to transfer data to CAPRI and CaseRite. UFA makes available the following information for CaseRite: Valid Case Number, Selected Violations, UFA Fine Amount, and Data elements needed to reproduce the UFA Report.

Safety Enforcement Tracking and Investigation (Sentri)

SENTRI is a single application that combines the functionality from all of FMCSA's legacy applications (ASPEN, CAPRI, CaseRite, CDLIS Access, ISS, and UFA), giving Enforcement personnel in the field, faster and seamless access to the safety information that they need in order to intervene more quickly and effectively.

The client-server SENTRI provides:

- A single environment for Field users to conduct inquiries, inspections, investigations, interventions, and create and review reports. That is, users will be able to login to SENTRI with a single username and password and have access to all of the functionality currently implemented in multiple legacy systems.
- Connectivity that will allow users to work online or offline. When online, users will have real-time access to carrier, vehicle, and driver information.
- Improved data quality, with a central standardized database and consistent edit checks. Users will be able to work offline and later synchronize with the database once connected.

SENTRI works closely with the FMCSA Portal and interacts with systems available through the portal. When Field users connect to the FMCSA network, information that they have entered into SENTRI will be uploaded to and synchronized with the central system database. SENTRI provides the functionality required by federal, state, and local enforcement field staff to monitor and enforce Motor Carrier Safety Regulations. SENTRI is primarily used by Safety Auditors to conduct safety audits. SENTRI is also used by Safety Investigators.

After an audit is complete, users can upload the data collected from the audit, along with any comments and recommendations to the back-end systems. Later releases of SENTRI will incorporate inspections,

interventions, enforcement cases, enforcement follow-up, and reporting functionality. Users will be able to download and install subsequent releases of SENTRI when connected to the FMCSA network.

Guard (formerly MCREGIS)

Guard provides up-to-date motor carrier regulatory information and guidance to enforcement staff. Guard is used by FMCSA's safety investigators and state partner-agencies throughout the United States to access and search safety information and regulations. All of the information contained within Guard is public information that can be obtained from other sources. Guard was design to provide a convenient repository for safety investigators and state partner-agencies. All actions performed by users of the Guard are permitted without identification and authentication. Users have access to Code of Regulation data to assist them in carrying out their duties only in accordance with FMCSA mission/business objectives.

Personally Identifiable Information (PII) and FMCSA Service Centers

The desktop applications making up the FMCSA Service Center Applications allow for users to perform safety compliance and enforcement activities on motor carriers, CMVs, and CMV drivers. The information collected during safety compliance and enforcement activities is used to conduct trend analyses to ensure that enforcement actions are implemented consistently and appeals are processed efficiently. This information is also used to verify information related to medical waivers and vehicle registrations.

FMCSA Service Center applications in general process and store the PII data fields summarized below from commercial motor vehicle (CMV) drivers and motor carrier representatives. The PII is collected using individual desktop applications (PII collected by each application is described in the section above). The general PII fields collected through the FMCSA Service Center applications include:

- Name (First, Last, Middle)
- Home address
- Home Phone number and/or Cell Phone Number
- Sex, Eye color, Height and Weight
- Commercial Class and Status
- Conviction History
- Violation Information
- Fine Information
- Inspection Value and Safety Information
- Social Security Number (SSN)
- Date of Birth Driver's license number
- Mother's Maiden Name
- Medical Information.

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.

CMV drivers and motor carrier representatives are required under 49 U.S.C. § 31106 to provide information as part of the inspection and crash data collection process and the FMCSA Service Center Applications do not provide additional notice or options for consent. Since PII collected from CMV drivers and motor carrier representatives by FMCSA Service Center Applications is used to fulfill FMCSA statutory and regulatory mandates, these individuals cannot specify how their PII will be used or shared. Therefore, FMCSA does not directly provide notice and consent.

FMCSA informs the public that their PII is stored and used by FMCSA Service Center applications through this Privacy Impact Assessment published on the DOT website. The FMCSA Service Center Applications PIA is available at https://tranpsortation.gov/privacy. While information is collected and entered into the Service Center desktop applications, FMCSA's Motor Carrier Information System (MCMIS), Enforcement Management Information System (EMIS), SAFETYNET, and Safety and Fitness Electronic Records (SAFER)are the authoritative sources for the information collected. Privacy Impact Assessments have been published for these three systems and are publically available on the DOT Privacy Office website.

- MCMIS: Motor Carrier Management Information System (MCMIS) - March 20, 2017
- EMIS: Enforcement Management Information System (EMIS) - March 20, 2017
- SAFER: Safety and Fitness Electronic Records (SAFER) - June 15, 2009
- SAFETYNET: SAFETYNET - December 5, 2003

In addition, MCMIS, EMIS, and SAFETYNET have been identified as Privacy Act systems of record. System of Records Notices (SORNs) have been published for these three systems and are available on the DOT Privacy Office website.

- MCMIS: DOT/FMCSA 001 – Motor Carrier Management Information System, 78 FR 59082, September 25, 2013
- EMIS: DOT/FMCSA –002 –Motor Carrier Safety Proposed Civil and Criminal Enforcement Cases, 65 FR 83124, December 29, 2000
- SAFETYNET: DOT/FMCSA 006 - SAFETYNET - 71 FR 68884 - November 28, 2006

These documents identify the information collection's purpose, FMCSA's authority to collect, store, and use the PII, and all uses of the PII collected, stored, and transmitted through the applicable systems.

Individuals are also informed of the existence of the desktop applications on the FMCSA website (https://www.fmcsa.dot.gov/mission/information-systems/information-systems) which provides an overview of all IT systems used by the agency.

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.

CMV drivers and motor carrier representatives are required under 49 U.S.C. § 31106 to provide information as part of the inspection and crash data collection process. Individuals providing data and PII do so directly to FMCSA personnel or through FMCSA forms.

FMCSA provides redress for individuals whose records may be maintained in the FMCSA Service Center applications through its DataQs system.

The DataQs system (https://dataqs.fmcsa.dot.gov/login.asp) is an electronic means for filing concerns about federal and state data released to the public by FMCSA. Individuals can use DataQs to challenge information included in their records. Motor carriers, state agencies, and FMCSA offices can use DataQs to challenge information concerning crashes, inspections, compliance reviews, safety audits, enforcement actions, vehicle registrations, operating authorities, insurance policies, and consumer complaints stored in any FMCSA system. 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 the appropriate system.

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 appropriate applications 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

When seeking records about yourself from any FMCSA 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.

Statutory Authority and 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.

FMCSA Personnel such as Attorneys, Safety Investigators, and Enforcement Personnel have access to the information collected through the FMCSA Service Centers Applications. These personnel determine if motor carriers, CMVs, and CMV drivers are in violation of FMCSA safety regulations. Information collected by FMCSA Service Center applications allows each regional service center to perform the following functions under the direction and supervision of designated FMCSA Field Administrators:

- Ensure that enforcement actions are justifiable and uniformly applied to all motor carriers, CMVs, and CMV drivers
- Respond promptly to appeals submitted by motor carriers and CMV drivers related to enforcement actions ordered by FMCSA division offices
- Evaluate the legitimacy of enforcement actions during the appeals process
- Identify process improvements and implement regulatory and program initiatives
- Provide oversight of the Commercial Driver's License (CDL) Program and various grant programs in FMCSA division offices

FMCSA Service Center Applications process and store PII, including SSN, from commercial motor vehicle drivers and motor carrier representatives. FMCSA Service Center applications are used to perform safety compliance and enforcement activities on motor carriers, CMVs, and CMV drivers. The information collected during safety compliance and enforcement activities is used to conduct trend analyses to ensure that enforcement actions are implemented consistently and appeals are processed efficiently.

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)

The FMCSA minimizes its data collection to that information necessary to meet the authorized business purpose and mission of the Agency. FMCSA collects, uses and retains only that data that is relevant and necessary for the purpose of safety inspections and compliance activities carried out by the FMCSA field personnel. Electronic records are retained on backup media for at least one year pursuant to National Archives and Records Administration (NARA) records schedule NI-557-045-107, "Field Operations." When the records are no longer required for safety compliance and enforcement activities, they are sent to the Electronic Document Management System (EDMS) to be archived in accordance with FMCSA retention procedures (Schedule NI-557-05-07, 'Information Technology & Deputy Chief Information Officer, Item 4). Information uploaded to MCMIS (Schedule NI-557-05-07, 'Information Technology & Deputy Chief Information Officer', Item 5) or EMIS (Schedule NI-557-10-1, 'Office of Information Technology,' Item 1) is retained according to their applicable schedules.

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 FMCSA minimizes its data collection to that necessary to meet the authorized business purpose and mission of the Agency. FMCSA Service Center Applications are used to perform safety compliance and enforcement activities on motor carriers, CMVs, and CMV drivers. The following groups have access to FMCSA Service Center Applications:

- Safety Inspectors/Investigators and Enforcement Personnel - Authorized users have full access to all of the data to review, use, and monitor the applications. A User ID and password is required to access the applications. Each application requires a unique log in.
- System Administrators and Developers - Federal contractors (System administrators and developers) have full access to perform their assigned roles and responsibilities (development and maintenance of the system) for each application.

FMCSA Service Center Applications are interconnected with several FMCSA systems to allow field personnel to access the IT systems and upload information into these systems. The FMCSA Service Center applications can be accessed via the single sign-on (SSO) FMCSA Portal. 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 FMCSA Service Center Applications 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.

Information entered into FMCSA Service Center applications is compared with information in other FMCSA systems (MCMIS, SAFER, QC, ASPEN, CaseRite, ISS, PIQ, UFA, and SAFETYNET) to ensure data accuracy. Information providers, such as state inspectors and other officials, are responsible for the accuracy and completeness of data entered into FMCSA Service Center applications and ultimately uploaded into FMCSA IT systems.

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

Individuals who provide PII directly to personnel or through FMCSA forms provide that PII themselves and are responsible for its accuracy. FMCSA staff reviewing and approving submitted information or forms check for completeness on required fields. Individuals who must submit PII in order to obtain direct access to Service Center applications 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 or telephone, that privacy practices be reviewed. This contact information is provided in the Privacy Policy, posted visiblyon the FMCSA 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.

The FMCSA Service Center applications and the systems in which the information is uploaded 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 FMCSA Service Center applications 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. The FMCSA Service Center applications are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the FMCSA Service Center applications is logged and monitored. 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 FMCSA Service Center applications 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 FMCSA Service Center applications.

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 FMCSA Service Center applications. 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 will conduct regular periodic security and privacy compliance reviews of the FMCSA Service Centers 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 the FMCSA Service Center applications 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 the FMCSA Service Center applications.

Responsible Official

Richard Scott
FMCSA Service Centers System Owner

Approval

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