U.S. Department of Transportation
Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)
Safety and Fitness Electronic Records (SAFER)

Responsible Official

Raymond Henley
SAFER System Owner
202-493-0346
Raymond.henley@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: 2018.10.16 19:28:12 -04'00'

Executive Summary

The U.S. Department of Transportation (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 implemented the Safety and Fitness Electronic Records (SAFER) system to help manage commercial vehicle and shipper safety data and and provide reliable access to this data to federal and state safety agencies. The SAFER public website allows users to access a wide range of census, inspection, and crash reports for the motor carrier industry as well as motor carrier snapshots and in-depth company safety profiles. This Privacy Impact Assessment (PIA) update is necessary to address risks associated with migrating the SAFER system to the FMCSA Cloud Environment.

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

Safety and Fitness Electronic Records (SAFER) is an information sharing system that provides an interface for state partners, motor carriers, industry groups and FMCSA to share safety information.

Functionality provided by SAFER falls under the following categories:

- **Data Upload** – SAFER provides functionality to allow state safety agencies to send data to FMCSA. This data is processed by SAFER and then stored in FMCSA's authoritative data repositories such as Motor Carrier Management Information System(MCMIS) and Licensing and Insurance (L&I).
- **Data Access** – SAFER provides state safety agencies with the ability to access consolidated data collected by FMCSA as well as other state safety agencies. SAFER provides several mechanisms to access data such as webservices, file transfer protocol (FTP), and a browser web interface.
- **Public Data Access** – SAFER provides the public with a subset of the data collected by FMCSA and state partners. The data is provided via SAFER's public website.
- **Internal Data Access** – SAFER provides FMCSA enforcement and policy users with consolidated access to FMCSA data stored in various authoritative systems such as MCMIS and L&I. Additionally, several FMCSA enforcement applications and authorized third party applications use SAFER as a data interface to avoid the need to access the authoritative data sources directly. These applications include:
    - **Aspen**— Aspen is an FMCSA sponsored tool used by federal and state enforcement officials in the field to conduct roadside inspections of CMVs and CMV drivers.
    - **Commercial Vehicle Information Exchange Window (CVIEW)**— CVIEW collects motor carrier, commercial motor vehicle (CMV), and CMV driver information from state CMV credentialing and tax systems. CVIEW transmits CMV credential information to SAFER for inclusion in interstate motor carrier, CMV, and CMV driver snapshots and reports.
    - **Inspection Selection System (ISS)**— ISS uses motor carrier snapshots containing critical safety performance indicators to determine which CMVs to target for roadside inspections. In addition to a local database, ISS may also receive updated motor carrier snapshots on individual motor carriers from SAFER.
    - **Safety Enforcement Tracking and Investigation (Sentri)**— Sentri retrieves past inspection reports from SAFER for review by federal and state enforcement officials in the field.
    - **Traffic and Criminal Software (TraCS)** — TraCS is a mobile computer technology that enables state enforcement officials to electronically issue tickets and write accident reports. TraCS forwards safety violation and accident reports issued by state enforcement officials to SAFER for processing.
- **Carrier Transations** – SAFER provides functionality to allow carriers to perform certain transactions such as pay fines, request their company safety profile, apply for additional types of operation authorites, update their carrier registration information, and update their licensing and insurance information. SAFER also allows carriers to compare their safety performance against national safety statistics such as Out of Service Percentage Rates, Crash Rates, and Inspection Rates.

Information in SAFER is organized according to the following categories:

- **Carrier Census Information**—Includes general information maintained on motor carriers and their operations (USDOT Number, company name and location, types of CMVs, number of CMV drivers, commodities transported, etc.) as well as safety fitness ratings, prioritization scores, and other summary information
- **Compliance Review Information**—Includes on-site compliance reviews of motor carrier operations, safety performance, and adherence to federal and state regulations
- **Inspection Information**—Includes roadside inspection records on CMVs and CMV drivers as well as safety violations related to CMVs, CMV drivers, and hazardous materials
- **Crash Information**—Includes information collected and maintained by individual states on reportable motor carrier crashes, such as date, time, and location of crash; weather and road surface conditions; investigating agency; CMV crash data recorder identification; motor carrier identification; CMV driver name and license number; and crash outcome (i.e., number of people injured or killed)
- **Vehicle Credential Information**—includes general information maintained on CMVs (registration, e-screening authorization, transponder transactions, etc.) as well as International Fuel Tax Agreement (IFTA), International Registration Plan (IRP), and IRP Fleet status.

SAFER does not directly store any carrier safety data. It is an interface that provides safety data that is stored in FMCSA's authoritative data repositories. These repositories are:

- **MCMIS** - is the central repository for motor carrier census, inspection, compliance review, crash, and registration information. MCMIS transmits motor carrier census, inspection, compliance review, crash, and registration information to SAFER via application batch. SAFER uses this information to generate census, inspection, and crash reports. SAFER transmits crash reports submitted by crash investigators in the field to MCMIS for processing.
- **L&I** is the authoritative source for licensing and insurance information for sole proprietors, commercial motor carriers, freight forwarders, and hazardous material shippers. L&I transmits motor carrier licensing and insurance information to SAFER via application batch. SAFER then disseminates this information to federal and state enforcement officials. SAFER also receives CMV credential information from the Commercial Vehicle Information Exchange Window (CVIEW) for inclusion in interstate motor carrier, CMV, and CMV driver snapshots and reports.

Personally Identifiable Information (PII) and SAFER

SAFER processes and transmits PII concerning CMV drivers obtained from CMV inspection reports. The PII associated with CMV drivers includes CMV driver name, driver address (possibly if driver is a sole proprietor), driver license number, and issuing state. If a commercial motor carrier is a sole proprietorship, PII concerning the sole proprietor-driver (owner-operator) may also be processed and transmitted by SAFER. The PII associated with owner-operators may include vehicle identification number (VIN), name and Social Security Number (SSN) if the owner-operator uses his or her SSN as the Employer Identification Number (EIN)[2]. The Agency strongly encourages owner-operators to

[2] Additional information about applying for an Employer Identification Number (EIN) on the Internal Revenue Service website - http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Apply-for-an-Employer-Identification-Number-(EIN)-Online.

obtain an EIN. However, the Agency will continue to permit an owner operator to provide their social security number (SSN) in lieu of the EIN.

SAFER processes and transmits Personally Identifiable Information (PII) concerning CMV vehicle inspection and crash reports. The vehicle inspection and crash reports may contain PII including, driver name, driver contact information (address and phone number), Commercial Driver License number, license plate number, date of birth, VIN, date, time and location of crash.

Move to the FMCSA Cloud Environment

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

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

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.

SAFER does not collect PII directly from individuals. SAFER only stores and disseminates PII that has been collected through other FMCSA systems. FMCSA informs the public that their PII is collected, stored, and used by SAFER through this Privacy Impact Assessment published on the DOT website. This document identifies the collections' purposes, FMCSA's authority to collect, store, and use the PII, and all uses of the PII collected, stored, and transmitted through SAFER.

As MCMIS and L&I are the authoritative sources for information in SAFER. Notice is provided to individuals through the Privacy Act System of Records Notice (SORN) DOT/FMCSA 001 - Motor Carrier Management Information System (MCMIS) - 78 FR 59082 - September 25, 2013. The MCMIS and L&I PIAs published on the DOT Privacy website provides addition notice and information to the public regarding the collection, use, and maintenance of PII by both MCMIS and L&I. The PIAs are published on the DOT Privacy Office website 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 provides the capability for individuals whose records may be available via the SAFER system to correct or challenge the information. The SAFER website provides a link to the DataQs system (https://dataqs.fmcsa.dot.gov/login.asp) along with instructions to contact FMCSA if corrections to SAFER records are required. DataQs allows a filer to challenge data maintained by FMCSA on, among other things, USDOT Number registration, operating authority registration, and insurance matters. Through this system, any registration-related data concerns are automatically forwarded to the appropriate FMCSA office for resolution. If the information is corrected as a result of the challenge, the change will be made in MCMIS. SAFER will receive the changed information through the monthly snapshot from MCMIS.

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

Under the provisions of the Privacy Act , individuals may request searches of SAFER or any other FMCSA information system, including MCMIS and L&I, 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

Motor Carriers may request records through FOIA. In addition a motor carrier can log into the MCMIS website using their PIN, and update the information that is stored for the company. Motor carriers may also complete an updated MCS-150 form (https://www.fmcsa.dot.gov/registration/form-mcs-150-and-instructions-motor-carrier-identification-report) and mail it to FMCSA-Headquarters for data entry.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which its collects, uses, maintains, or disseminates PII.

The primary purpose of SAFER is to provide motor carrier, vehicle, and driver safety information to federal and state agencies to improve the safety of interstate and intrastate commercial motor carriers, commercial motor vehicles (CMV), and CMV drivers. This information allows roadside inspectors to select CMVs and CMV drivers for inspection

based on the number of previous inspections as well as on carrier, vehicle, and driver safety and credential histories. In addition, SAFER provides motor carrier safety information and related services to industry groups, insurance companies, and the general public via the Internet. Access is provided free of charge via SAFER to the Company Snapshot, a concise electronic record of a company's identification, size, commodity information, and safety record, including the safety rating (if any), a roadside out-of-service inspection summary, and crash information.

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 only uses and retains data that are relevant and necessary for the purpose of SAFER. SAFER receives a monthly snapshot from MCMIS and L&I which includes PII determined to be necessary for SAFER system functions. SAFER 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).

SAFER retains and disposes of information in accordance with NARA retention schedule, NARA Job No. N1-557-05-7 Item #6[3], Safety And Fitness Electronic Records (SAFER) System. The length of retention time for SAFER documents depends on whether the information falls under inputs, master data files, documentation, or outputs. For any information entering SAFER, the data is destroyed or deleted, regardless of media, after information is converted or copied to the SAFER master data files, backed up, and verified. For master data files and any documentation, the information is destroyed or deleted when the data is superseded or becomes obsolete. For SAFER outputs (reports) the information is destroyed or deleted when the data is no longer needed for reference.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

Information provided by SAFER is used Federal and State enforcement officials to select drivers and vehicles for inspection. The enforcement officials determine which drivers and vehicles to inspect based on safety and credential histories and the number of previous inspections. SAFER information is also used by FMCSA personnel to increase intrastate and interstate commercial vehicle safety operations and by insurance companies to improve safety performance. Access to non-public and public information in SAFER is determined by the user's role and responsibilities.

The following groups have access to SAFER for their distinct user roles:

- **Federal and State Enforcement Officials**- Users access SAFER via web-based roadside applications in order to submit inspection and crash investigation reports to MCMIS for processing and to retrieve motor carrier snapshots, updated registration information, compiled safety fitness ratings, and previous inspection reports. Users can also access the SAFER website via the FMCSA Portal.

[3] https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0557/n1-557-05-007_sf115.pdf

- **State Transportation Departments** - Users access SAFER via the Commercial Vehicle Information Exchange Window (CVIEW), SAFETYNET, ASPEN and other third-party state applications. State transportation departments access SAFER in order to transmit CMV credential information for inclusion in interstate motor carrier, CMV, and CMV driver snapshots and reports and to retrieve motor carrier snapshots, updated registration information, and compiled safety fitness ratings.
- **Third-Party Contractors** - State transportation departments may use third-party contractors to develop and maintain CVIEW-equivalent IT systems. State transportion departments may also use third-party contractors to perform data related functions such as data verification/validation, data entry and data analysis. These contractors are able to access data provided by SAFER on their client's behalf.
- **General Public** - Users, including industry groups, insurance companies, and motor carriers, access SAFER via the SAFER website to obtain safety rating and other safety information, inspection and crash data, and general motor carrier information. Users can also subscribe to receive electronic copies of motor carrier data stored on SAFER.

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 SAFER 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 SAFER system itself does not provide internal data quality and completeness checks, as the system only stores PII that has been collected through other FMCSA systems. MCMIS and L&I are the authoritative sources for information stored in SAFER.

MCMIS

FMCSA leverages manual and automated data verification process to ensure that accurate information is entered in MCMIS. FMCSA requires motor carriers to submit a Motor Carrier Identification Report (MCS-150) in order to obtain a USDOT Number. This number is used for accesss MCMIS. To ensure that all necessary information is provided to receive a USDOT Numbner, MCMIS uses internal validation functionality to ensure that all required data fields have been completed on the MCS-150.

FMCSA also allows the MCS-150 to be submitted in paper form. In order to ensure that the data entered into the sytem is accurate, 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; 1) review application for completeness, 2) data accuracy verification, 3) data entry into MCMIS, 4) verification and approval.

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

Individuals who 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.

L&I

The L&I Customer Support Team reviews and approves all forms submitted by commercial motor carriers, freight forwarders, and property brokers before the information is entered into L&I. Forms are checked for completeness and verified for accuracy. Verification may include requesting legal documents directly from motor carriers or from their agents or representatives. Registered electronic filers may file certificates and cancellations, view their last transmissions, and print their confirmation, acceptance, and reject reports.

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

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

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

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 SAFER 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 SAFER.

A security authorization is performed every year to ensure that SAFER meets FMCSA and federal security requirements. SAFER also undergoes an additional security authorization whenever a major change occurs to the system. SAFER is assessed in accordance with the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, and the DOT Certification and Accreditation Guidance. The SAFER 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 SAFER was last authorized on January 2017.

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 SAFER 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 will conduct regular periodic security and privacy compliance reviews of the SAFER consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Audit provisions are also included to ensure that SAFER 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 SAFER.

Responsible Official

Raymond Henley
SAFER System Owner
Federal Motor Carrier Safety Administration
202-493-0346
Raymond.henley@dot.gov

Approval

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