U.S. Department of Transportation

Privacy Impact Assessment (PIA)

Federal Motor Carrier Safety Administration (FMCSA)

Performance and Registration Information Systems Management (PRISM)

Responsible Official

Camille M. White
PRISM Program Manager
202.493.0442
Camille.White@dot.gov

Reviewing Official

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

CLAIRE W BARRETT Digitally signed by CLAIRE W BARRETT
Date: 2019.08.15 14:49:15 -04'00'

Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is an agency within the U.S. Department of Transportation (DOT) with a core mission to reduce commercial motor vehicle (CMV) crashes, injuries and fatalities. PRISM is a key component to FMCSA's mission and improves highway safety by partnering with States to create a safety mechanism to identify and imobolize motor carriers that are prohibited from operation by FMCSA due to a Federal Out-of-Service (OOS) order. PRISM enforces a safety standard to incentivize motor carriers that are prohibited from operating by FMCSA to correct their safety deficiencies to continue operating, or face State registration and law enforcement sanctions.

State CMV registration agencies, mainly the International Registration Plan (IRP) upload registration data to the Safety and Fitness Electronic Records (SAFER) database daily. This data allows FMCSA to link the motor carrier's safety fitness to their vehicle registration, bringing safety down to the vehicle level. FMCSA disseminates this combined Federal and State safety data known as the "PRISM Target file" back to the States to support their daily PRISM enforcement activities and improve highway safety of interstate motor carriers.

The PRISM data provides States with information about every motor carrier that has a USDOT Number, such as the the Tax Identification Number, which is essential to the State registration agencies in order to validate the motor carrier prior to registration.

This PIA is being conducted because some of the data facilitated through PRISM contains information on individuals who own CMV related businesses, some of which are sole-propieters for whom the TIN is the individual's Social Security Number (SSN). This PIA also addresses changes to the environment's security risk associated with the migration to the FMCSA Cloud.

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.

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]

[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).

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.

Introduction & System Overview

The Performance and Registration Information Systems Management (PRISM) program was developed to meet the challenge of reducing the number of commercial vehicle crashes of a rapidly expanding interstate carrier population. It has increased the efficiency and effectiveness of Federal and State safety efforts through a more accurate process for targeting the highest-risk carriers, which allows for a more efficient allocation of scarce resources for compliance reviews and roadside inspections. The PRISM program requires that motor carriers improve their identified safety deficiencies or face progressively more stringent sanctions up to the ultimate sanction of a Federal Out-of-Service order and concurrent State registration suspensions. The PRISM program has proven to be an effective means of motivating motor carriers to improve their compliance and performance deficiencies.

PRISM originated as a pilot project mandated by Congress in the Intermodal Surface Transportation Efficiency Act of 1991. The Federal Motor Carrier Safety Administration (FMCSA) and the State of Iowa developed the pilot project. In addition to Iowa, the States of Colorado, Indiana, Minnesota, and Oregon also participated in the pilot, which ended in 1997. The pilot demonstrated that State commercial vehicle registration sanctions could be a powerful enforcement tool in Federal and State motor carrier safety improvement efforts. Congress authorized funding through the Transportation Equity Act for the 21st Century (TEA-21), P.L. 105-178 (1998) to expand PRISM nationally. The Safe, Accountable, Flexible, and Efficient Transportation Equity Act: A Legacy of Users (SAFETEA-LU), P.L. 109-59 (2005) established statutory requirements for States to participate in PRISM and added a PRISM grant program to assist states in modernizing their motor carrier registration systems to comply with the requirements of PRISM. Section 5101 of the FAST Act made participation in PRISM a requirement of the Motor Carrier Safety Assistance Program (MCSAP). MCSAP grant recipients must meet the full participation requirements of PRISM no later than October 1, 2020.

There are two major sets of data collected and used by FMCSA that are shared with states who participate in the PRISM program.

1. **Census data** contains information on every USDOT Number established. When applying for a USDOT Number, every motor carrier must fill out the Motor Carrier Identification Report (Application for USDOT

Number) MCS-150 form and submit the form to FMCSA. The MCS-150 form requires data such as the motor carrier's name, address, phone number, tax identification number, and total number of vehicles/drivers, etc. The carrier data is first entered into the Motor Carrier Management Information System (MCMIS). Each night, any new/updated data from MCMIS is sent via a snapshot to the SAFER-PRISM database. The PRISM program and SAFER (Safety and Fitness Electronic Records) program share the same database. The PRISM Census data is generated daily based on the MCMIS snapshots, and then provided to the PRISM State agencies.

The primary use of the PRISM Census data is for the State vehicle registration offices to validate the USDOT Number prior to registration. The USDOT Number and FEIN provided by the motor carrier is compared to the USDOT Number and FEIN in the PRISM data to ensure that the State is working with the correct carrier, and that the carrier did not just use some random USDOT Number/FEIN combination.

2. **"Target Data"**: includes data on those vehicles that are associated with motor carriers that are either under a Federal Out-of-Service order, or have a history of bad safety data and may include the Vehicle Identificatio Number (VIN) or the licesne plat number. PRISM State registration offices upload their vehicle information to the PRISM-SAFER database on a nightly basis. Any applicable vehicles are then added to the PRISM Target data, and provided to the PRISM State agencies.

   The primary use of the PRISM Target data is for the State vehicles registration offices and roadside law enforcement agencies to check the vehicle to see if it has a valid registration, or should even be operating in general. The Targeted vehicle data set does not contain any PII related information.

Personally Identifiable Information (PII) and PRISM

PRISM does not collect PII directly from individuals. PRISM only stores and disseminates PII that has already been collected through the Motor Carrier Management Information System (MCMIS). MCMIS is the authoritative source for carrier information stored in PRISM.

PRISM processes, stores, and transmits business information and Personally Identifiable Information (PII) in the form of the Federal Employer Identification Number (FEIN) of the motor carrier. The business information and PII associated with the carrier may include the carrier name and Social Security Number (SSN), if the carrier is a sole proprietor who uses his or her SSN as the Employer Identification Number (EIN).

PRISM processes and stores the following business information and PII from commercial motor carriers:

- Name
- Physical Address
- Mailing Address
- Carphone Number
- Entity Type
- Operation Type (such as Interstate vs. Intrastate)
- Tax Identification Number (which can be the Social Security Number (SSN) in some cases if the sole proprietor of the motor carrier opted to use their SSN instead of the tax identification number)

PRISM receives a monthly snapshot from the MCMIS which includes SSNs and/or Employer Identification Numbers (EINs). The SSNs and EINs are collected when the motor carrier or individual registered for a USDOT Number or Operating Authority. It is verified during the safety audit or compliance review process. The SSN is collected on sole proprietors who do not have an EIN number. FMCSA encourages sole proprietors to obtain the EIN and to provide it

when applying for their USDOT number registration. The collection of the SSN will be solely used for identification purposes.

MCMIS is the authoritative source of PII in PRISM. MCMIS system obtains 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. State officials and FMCSA field offices forward safety information to MCMIS soon after it has been compiled and processed locally. Motor carrier information is obtained by company officers that have completed the Motor Carrier Identification Report. Company officers must sign to the accuracy of the information reported.

Impact of the Move to the FMCSA Cloud Environment

The portal-based FMCSA Cloud Environment platform provides for service-oriented architecture (SOA) access to FMCSA safety information data and FMCSA supporting IT processing and FMCSA data sharing processes.

As an infrastructure-as-a-service (IaaS) platform, the FMCSA Cloud Environment integrates disparate FMCSA application components into a common IT design and execution framework that is aligned to FMCSA business processes and objectives. The NATSS SOA framework and cloud technology environment establishes a process baseline that enhances existing FMCSA operational efficiency and future development agility while increasing FMCSA IT security and risk compliance through proven governance processes inherited from the FedRAMP compliant AWS Cloud.

In the transition to the FMCSA Cloud Environment, no fundamental changes were made to the PRISM system. The transition into the FMCSA Cloud Environment followed a lift-and-shift migration approach that replicated the existing system and infrastructure hosting environment directly onto the IaaS platform provided by AWS Cloud. In following this technical migration approach, FMCSA enterprise systems, including PRISM, were not redesigned or modified to accommodate the physical transition to the new AWS Cloud IaaS platform or environment.

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.

PRISM does not collect PII directly from individuals. PRISM only stores and disseminates PII that has been collected through MCMIS. The PRISM PIA provides notice to the public regarding the PRISM program and its use of PII. The PIA is published on the DOT Privacy website and is available at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

As MCMIS is an authoritative source for information stored in PRISM, 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.

The MCMIS PIA published on the DOT Privacy website provides addition notice and information to the public regarding the collection, use, and maintenance of PII by MCMIS (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 PRISM system through its Motor Carrier Information Management system (MCMIS) and DataQs system.

PRISM does not collect PII directly from individuals. PRISM receives a snapshot of data, some of which is PII, from the MCMIS database on a nightly basis. The uploaded data is not altered in any way once it enters the system. MCMIS is the authoritative source of PII in PRISM. The MCMIS system obtains information, including PII, from commercial motor carriers when they apply for, or update, their USDOT Number information using the MCS-150 form and/or the MCMIS website. At any time, a motor carrier can log into the MCMIS website using their PIN number, and update the information that is stored, including any PII data. Motor carriers also currently have the option of filling-out an updated MCS-150 form and mailing to FMCSA-HQ for data entry.

In addition, PRISM includes a link to the DataQs system. DataQs (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. 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. 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, the change will be made in MCMIS. PRISM will receive the change through the data refresh.

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 PRISM to determine if any records have been added that may pertain to them. This is accomplished by sending a written request directly to:

Federal Motor Carrier Safety Administration
Attn: FOIA Team MC-MMI
1200 New Jersey Avenue SE
Washington, DC 20590

Purpose Specification

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

PRISM is not a website, and it cannot be accessed from the internet. PRISM is a data sharing system that allows state agencies to access information concerning commercial motor vehicles registered in other states. PRISM also integrates registration and enforcement processes to identify motor carriers and hold them responsible for the safety of their operations. The International Registration Plan (IRP) within the state commercial vehicle registration process establishes a system of accountability by ensuring that no vehicle is registered without identifying the motor carrier responsible for the safety of that vehicle. The Motor Carrier Safety Improvement Process (MCSIP) systematically tracks and improves the safety performance of motor carriers with poor safety records using a comprehensive system of accurate identification, performance monitoring, and treatment.

PRISM State agencies use the PRISM data to ensure that the motor carrier they are dealing with is not under a Federal Out-of-Service order, and that the motor carrier is valid for Interstate operations prior to registration. The primary use of the PRISM data is for the State vehicle registration offices to validate the USDOT Number prior to registration. The USDOT Number and FEIN provided by the motor carrier is compared to the USDOT Number and FEIN in the PRISM data to ensure that the State is working with the correct carrier, and that the carrier did not just use some random USDOT Number/FEIN combination.

PRISM is authorized pursuant to the Safe, Accountable, Flexible, and Efficient Transportation Equity Act: A Legacy of Users (SAFETEA-LU), P.L. 109-59 (2005) which established statutory requirements for States to participate in PRISM and added a PRISM grant program. The Moving Ahead for Progress in the 21st Century Act (MAP-21), P.L. 112-141 (2012) further authorized PRISM funding for fiscal years 2013-2014.

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 purposes of the PRISM and SAFER programs. The PRISM-SAFER shared database receives a nightly snapshot from MCMIS, which includes PII determined to be necessary for the PRISM system functions.

The SAFER team is responsible for processing the data snapshot updates that are sent from MCMIS to the PRISM-SAFER database. PRISM is only a user of the data, and provider of the data. 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 applicable NARA retention schedule N1-557-05-07 Item #6. 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 the PRISM-SAFER database, 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.

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. The information collected in support of PRISM allows FMCSA to provide credentials to commercial motor carriers. The end users of the PRISM Census data, which contains the PII, are the State vehicle registration agencies that provide credentials to commercial motor carriers. Only PRISM State agencies that have signed-off on the FMCSA rules and behavior have access to the data. For any user with access, a FMCSA Organization Coordinator needs to also sign the account request form prior to the State getting access to the data. Only State agencies that have been approved by FMCSA are allowed to access the data.

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 PRISM 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.

PRISM does not collect PII directly from individuals. PRISM only stores and disseminates PII that has already been collected through the Motor Carrier Management Information System (MCMIS). MCMIS is the authoritative source for carrier information stored in PRISM, and as such MCMIS has the following elements in place:

- 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 a Motor Carrier Identification Report (MCS-150) to obtain a USDOT Number and uses internal validation functionality to ensure that all required data fields have been completed on the MCS-150.

- 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.

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

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

The PRISM 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 PRISM 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 PRISM 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 PRISM.

A security authorization is performed every year to ensure that PRISM meets FMCSA and federal security requirements. PRISM also undergoes an additional security authorization whenever a major change occurs to the system. PRISM 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 PRISM 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 PRISM was last authorized on September 28, 2015.

Security Assurances Inherited from the AWS Cloud

Use of the AWS Cloud, allows FMCSA to re-use and leverage a FedRAMP compliant cloud system environment and approved Federal cloud service provider (CSP). The AWS FedRAMP compliant environment consists of the AWS Cloud network and AWS internal data center facilities, servers, network equipment, and host software systems that are all under reasonable control by AWS. The AWS Cloud environment and service facilities are restricted to US personnel and all AWS Cloud community customers are restricted to US government entities from federal, state or local government organizations.

The AWS environment had been evaluated and tested by FedRAMP-approved independent third-party assessment organizations (3PAOs). The AWS is designed to meet NIST SP 800-53 minimum security and privacy control baselines for information and/or Federal information systems risk up to Moderate impact levels. As confirmed through audit, the AWS addresses recent requirements established by NIST SP 800-171 for Federal agencies to protect the confidentiality of controlled unclassified information in non-federal information systems and organizations. AWS provides FIPS Pub 140-2 compliant services to protect data-at-rest with AES-256 based encryption and validated hardware to secure connections to the AWS.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FMCSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to FMCSA privacy and security policies and regulations. FMCSA follows the Fair Information Principles as best practices for the protection of information associated with the PRISM 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 PRISM 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 PRISM 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 PRISM.

Responsible Official

Camille M. White
PRISM Program Technical Manager
Federal Motor Carrier Safety Administration
202.493.0442
Camille.White@dot.gov

Approval

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