U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration

FMCSA

Query Central

QC

Responsible Official

Tonya Bannister
Email: Tonya.Bannister@dot.gov
Phone Number: 202-366-4096

Reviewing Official

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is an Operating Administration (OA) within the U.S. Department of Transportation (DOT) with a core mission to reduce commercial motor vehicle-related crashes and fatalities. To further this mission, FMCSA created Query Central (QC), a FMCSA intelligent query web-based system to significantly increase access to motor carrier safety information with the goal to reduce commercial motor vehicle-related crashes and fatalities. Query Central is a secure web application that provides federal and state safety enforcement personnel with a single query engine for commercial motor vehicle (CMV) carriers, vehicles, and driver's safety data and significantly increase access to motor carrier safety information. The legal authority for Query Central is 49 U.S.C. 502, 504, 506, 508, Chapter 139, and 49 CFR 1.73.

This Privacy Impact Assessment (PIA) is necessary to provide information regarding the Query Central system and its use of Personally Identifiable Information (PII) of commercial drivers.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

[1] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

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

Query Central (QC) is a secure web-based system that supports FMCSA's Compliance, Safety and Accountability (CSA) initiative. Query Central is accessed through the FMCSA Portal[2]. Federal and state enforcement personnel use QC to perform commercial motor vehicle (CMV) driver inspections, motor carrier and hazardous material shipper compliance reviews, and border safety audits. The QC system is optimized for use with roadside inspections to assist CMV inspectors to gather necessary information for making inspection decisions. The data is specific to the needs of commercial vehicle safety enforcement personnel and includes automated summaries and alerts which enable the staff to identify and determine potential safety and enforcement issues quickly.

QC allows federal and state enforcement personnel to access safety performance and enforcement action information in real-time from multiple sources using a single input. In most cases, a user can submit a single query parameter such as a USDOT number, and data is returned from multiple systems rather than submitting the same data element to several systems.

Other than user information (passwords and preferences) and Automated Commercial Environment (ACE) data, QC does not maintain a database of its own, but instead pulls data from a variety of authoritative sources in real-time. QC retrieves motor carrier, CMV, and CMV driver information from FMCSA's Motor Carrier Management Information System (MCMIS), Safety and Fitness Electronic Records (SAFER), Licensing and Insurance (L&I) System, and Performance and Registration Information Systems Management (PRISM) along with the Commercial Driver's License Information System (CDLIS) operated by the American Association of Motor Vehicle Administrators (AAMVA) and the Mexican Licencia Federal Information System (eLicencias). QC also provides automated notifications and data summaries to allow enforcement personnel to quickly identify and analyze potential safety and enforcement issues. Although QC retrieves information from many sources, only information retrieved from CDLIS and SAFER contain PII. PII from CDLIS is used by federal and state safety enforcement personnel to properly identify CMV drivers during roadside inspections. The PII from SAFER is the roadside inspection data that is uploaded to SAFER.

QC interacts with the U.S. Customs and Border Protection's (CBP) Automated Commercial Environment and International Trade Data System (ACE/ITDS) system owned and operated by the Department of Homeland Security (DHS). ACE is a commercial trade processing system developed by CBP to facilitate legitimate trade and strengthen border security. ITDS provides a secure interface for

[2] The FMCSA Portal (https://portal.fmcsa.dot.gov/login) is a web-based system that supports most FMCSA information technology capabilities. The FMCSA Portal provides FMCSA, State enforcement personnel, and the motor carrier industry with resources needed to improve the safety of U.S. roadways. The FMCSA Portal provides a single-entry point to multiple FMCSA information systems for internal and external users in compliance with the E-Government Act of 2002.

disseminating electronic international trade and transportation data among federal government agencies. The QC-ACE/ITDS Interface enables FMCSA inspectors to quickly screen motor carriers, CMVs, and CMV drivers at congested border crossings to verify the carrier's operating status as part of a pre-clearance check for the CBP border crossing. Critical motor carrier, CMV, and CMV driver information is stored in a database maintained by QC-ACE/ITDS Interface to facilitate screenings. The CBP has a Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) in place to address the sharing and protection of CMV information and use of the information.

Personally Identifiable Information (PII) and Query Central

An example of the use of the system is when an end user uses QC to inquire about the status of a motor carrier's operating authority. QC queries FMCSA's Licensing and Insurance (L&I) information system to retrieve the results. Similarly, the data is used to analyze and respond to inquiries about CDLs that originate in State-owned and administered databases.

The QC system performs the same function with respect to queries from the ACE system. The ACE system includes manifest information with specific details regarding the trip, conveyance, equipment, driver, and shipments related to a commercial land border crossing. A truck manifest is made up of four parts: the driver, conveyance, equipment, and shipments. This information is collected from the e-Manifest submitted by the carriers to CBP. Subsequently, the data elements pertinent to FMCSA are verified using QC, which will interface with FMCSA's Motor Carrier Management Information System (MCMIS), Safety and Fitness Electronic Records (SAFER), Licensing and Insurance (L&I) System, and Performance and Registration Information Systems Management (PRISM) along with the Commercial Driver's License Information System (CDLIS) operated by the American Association of Motor Vehicle Administrators (AAMVA) and the Mexican Licencia Federal Information System (eLicencias).

QC processes both PII and non-PII on commercial motor vehicles (CMV) drivers. The system displays the following PII from drivers of commercial vehicles subject to FMCSA regulations (authoritative data sources for the following PII are CDLIS and SAFER):

- Driver Name
- Driver Address
- Driver License Number and License State of Issue
- Driver Date of Birth
- Driver SSN.

The information fields transmitted from ACE to QC are as follows:

Conveyance

- License plate on the vehicle and trailer
- State of issuance
- County of issuance
- VIN (Vehicle Identification Number)

Driver

- Name of the driver of the conveyance (truck)
- Date of birth of the driver
- Commercial Driver's License (CDL)/driver's license number
- CDL/driver's license state/province of issuance for the driver
- CDL country of issuance for the driver and
- Hazmat endorsement for the driver.

Motor Carrier

- DOT number

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[3], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[4].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

QC does not collect PII directly from individuals. QC only displays data from other FMCSA systems (PRISM, SAFER, MCMIS, L&I) along with the Commercial Driver's License Information System (CDLIS) operated by the American Association of Motor Vehicle Administrators (AAMVA) and the Mexican Licencia Federal Information System (eLicencias). QC does not retain data. It is not the authoritative source for the PII data. The QC website has a link to DOT Privacy Policy that contains all the protection and advisories required by the E-Government Act of 2002. The Privacy Policy describes DOT information practices related to the online collection and the use of PII.

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

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

FMCSA informs the public that their PII is used by QC through this Privacy Impact Assessment (PIA) published on the DOT website. This document identifies the system's purpose, FMCSA's authority to use the PII, and all uses of the PII transmitted through QC. The QC PIA is available at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

As MCMIS, PRISM, SAFER, MCMIS, and L&I are the primary sources of information for information displayed by Query Central, notice is provided to individuals through the corresponding system specific PIAs available on the DOT Privacy Office website. Furthermore, as an authoritative source and a system of records, the Privacy Act System of Records Notice (SORN) for the MCMIS system, DOT/FMCSA 001 - Motor Carrier Management Information System (MCMIS) - 78 FR 59082 - September 25, 2013, provides additional transparency to the public. This SORN is available to the public on the DOT Privacy Office website at http://www.transportation.gov/individuals/privacy/privacy-act-system-records-notices or on the website of the Federal Register at https://www.gpo.gov/fdsys/pkg/FR-2013-09-25/pdf/2013-23131.pdf.

The MCMIS web interface and the L&I website also provides notice to all individuals who enter their own PII into either system. The websites contain a link to the DOT Privacy Policy at the bottom of the webpage, which applies to online information practices only. The online registration form for L&I (https://www.fmcsa.dot.gov/registration/getting-started) identifies the data fields that are required and those that are voluntary. In addition, the DOT Privacy Policy states that "by providing personally identifiable information, you are granting us consent to use this personally identifiable information for the primary purpose for which you are providing it. Additionally, we will ask for you to grant us consent before using your voluntarily provided information for any secondary purposes, other than those required under the law." The hardcopy L&I registration form states that "all responses to this collection of information are mandatory, and will be provided confidentiality to the extent allowed by the Freedom of Information Act (FOIA)." For direct access and or Intranet access to MCMIS, users must read and agree to a warning message that discusses the penalties of unauthorized access before logging in.

Individual Participation and Redress

DOT provides 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 they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

QC does not collect PII directly from individuals. QC only displays data from other systems (PRISM, SAFER, MCMIS, L&I, CDLIS, and eLicencias). Individual do not have access to any data displayed in QC.

For individuals that have records within MCMIS, they can log into the MCMIS website using a PIN number, and update the information that is stored, including any PII data. Motor carriers also currently have the option of filling-out an updated MCS-150 form and mailing to FMCSA-HQ for data entry.

Under the provisions of the Privacy Act and Freedom of Information Act (FOIA), individuals may request searches of the authoritative sources 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

Included in the request must be the following:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records

With respect to CBP's ACE system, there are no opportunities for affected individuals to consent to particular uses of information, unless they choose not to cross the borders into the United States. Additional information regarding an individual's opportunity to consent to particular uses of information may be found at http://www.dhs.gov/sites/default/files/publications/privacy-piaupdate-cbp-ace-july2015.pdf.

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 it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

49 U.S.C. 502, 504, 506, 508, Chapter 139, and 49 CFR 1.73 authorize FMCSA to operate QC to further its mission to dramatically increase access to motor carrier safety information for state and federal law enforcement personnel. QC uses and disseminates PII to help provide federal and state safety enforcement personnel with information on commercial motor vehicle (CMV) carriers, vehicles, and driver's safety data to perform commercial motor vehicle (CMV) and CMV driver inspections, motor carrier and hazardous material shipper compliance reviews, and border safety audits. QC uses PII collected by other FMCAS information systems to screen certain e-Manifest data elements and return response and error messages to ACE and state and federal commercial vehicle enforcement personnel. This process allows FMCSA to better accomplish its mission to reduce crashes, injuries, and fatalities

involving large trucks and buses. It also increases efficiency and security of commercial vehicle inspections at the international borders.

The account holder to the ACE system submits personal information about the carrier's driver, the carrier and the carrier's vehicles when creating an account in ACE, or when submitting a manifest on a transactional basis (each time the truck crosses the border). In turn, ACE transmits a message to QC requesting validation of certain data elements (i.e., driver information, vehicle information and DOT number).

QC generates a message stating that the information provided to ACE via the e-Manifest is valid or invalid. This is similar to a red light, green light type of notice.

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.

FMCSA only uses data that is relevant and necessary for the purpose of QC. QC displays data from other systems (PRISM, SAFER, MCMIS, L&I, etc.).

As a result, the other FMCSA systems (PRISM, SAFER, MCMIS, and L&I) retain and dispose of information in accordance with the approved records retention schedule as required by the U.S. National Archives and Records Administration (NARA). MCMIS records are retained and destroyed in accordance with applicable NARA retention schedule N1-557-05-07 Item #5.[5] The PRISM and SAFER systems retain and dispose of information in accordance with the applicable NARA retention schedule N1-557-05-07 Item #6.[6] The L&I system retains and disposes of information in accordance with the applicable NARA retention schedule N1-557-01-001. [7] MCMIS records are retained and destroyed in accordance with applicable NARA retention schedule N1-557-05-07 Item #5. Please see the CBP ACE PIA for the NARA retention schedule (http://www.dhs.gov/sites/default/files/publications/privacy-piaupdate-cbp-ace-july2015.pdf).

Records accessed by 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.

FMCSA collects, uses, and retains only that ACE data that are relevant and necessary for the purpose of QC. QC retains and disposes of information in accordance with the approved records retention schedule

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

[6] *Ibid*.

[7] See https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0557/n1-557-01-001_sf115.pdf.

as required by the U.S. National Archives and Records Administration (NARA). Records in QC may be retrieved by; individuals' name, driver's license number, date of birth, company name, trade name, and geographical location. QC records are retained and destroyed in accordance with applicable NARA retention schedule. 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 help provide federal and state safety enforcement personnel with information on commercial motor vehicle (CMV) carriers, vehicles, and driver's safety data to perform commercial motor vehicle (CMV) and CMV driver inspections, motor carrier and hazardous material shipper compliance reviews, and border safety audits. QC is not the authoritative source for any data, PII data is displayed from other FMCSA systems. It is used by federal and state enforcement personnel.

The following groups have access to QC:

- FMCSA and State Enforcement Users - Authorized FMCSA users have full access to all the data to review and monitor the applications. A User ID and password is required to access the system.
- System Administrators and Developers - Federal contractors (System administrators and developers) have full access to the QC Online to perform their assigned roles and responsibilities (development and maintenance of the system).

The QC website 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.

For more information about the limits of use for information in the MCMIS and L&I systems, please refer to the MCMIS and L&I PIAs published on the DOT Privacy Office website at https://www.transportation.gov/privacy.

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 FMCSA systems is relevant to the purposes for which it is specified by the Agency, and to the extent necessary for those purposes; it is accurate, complete, and up-to-date.

Sources of information, such as other FMCSA systems, CDLIS, State police departments or other officials, are responsible for inputting correct information.

QC does not collect PII directly from individuals. QC and ACE/ITDP only displays data from other FMCSA systems (PRISM, SAFER, MCMIS, and L&I) along with the Commercial Driver's License Information System (CDLIS) operated by the American Association of Motor Vehicle Administrators (AAMVA) AAMVA and the Mexican Licencia Federal Information System (eLicencias). QC does not retain data. It is not the authoritative source for the PII data. For more information, please see the other FMCSA systems' PIAs (PRISM, SAFER, MCMIS, and L&I) published on the DOT Privacy Office website at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments for more detailed information with respect to Data Quality and Integrity within those systems.

Security

DOT shall implement administrative, technical, and physical measures to 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 QC 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 QC 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 QC system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the QC system is logged and monitored.

Logical access controls restrict users of the QC. 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 QC 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 QC 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 to gain access to QC. 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 retrieved by QC.

The QC 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 QC 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 act in situations properly and securely where they may use PII while performing their duties. No access will be allowed to the QC 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 QC.

A security authorization is performed every year to ensure that QC meets FMCSA and federal security requirements. QC also undergoes an additional security authorization whenever a major change occurs to the system. QC 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. QC is approved through the Security Authorization Process under the National Institute of Standards and Technology.

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. 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 QC. Audit provisions are also included to ensure that QC 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.

FMCSA follows the Fair Information Practice Principles as best practices for the protection of information associated with the QC 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 QC consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Tonya Bannister
System Owner
(202) 366-4096
FMCSA Office of Information Technology

Prepared by: Pam Gosier-Cox (FMCSA Privacy Officer)

Approval and Signature

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer