U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

FMCSA Customer Relationship Management (CRM)

Responsible Official

David Turnbull
Email: David.turnbull@dot.gov
Phone Number: 202-366-6490

Reviewing Official

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

Executive Summary

The Department of Transportation's (DOT) Federal Motor Carrier Safety Administration's (FMCSA) core mission is to reduce commercial motor vehicle-related crashes and fatalities. FMCSA's Office of Registration (MC-RS) houses the Agency's motor carrier and related entity registration, licensing, insurance, vetting functions, along with various customer service/contact center efforts. FMCSA receives, processes, stores, analyzes, researches, and disseminates safety, licensing, and registration data for interstate and intrastate motor carriers of property including hazardous materials, motor carriers of passengers, and other motor carrier-related entities in the United States (U.S.), Canada, Mexico, and other non-U.S. based carriers. To do this, FMCSA acquired Salesforce Customer Relationship Management (CRM) and Amazon Telephony, a commercial off-the-shelf, FedRAMP accredited cloud-based system CRM tool provided by the DOT Office of the Secretary (OST) to support the activities of its Contact Center program.

This Privacy Impact Assessment (PIA) is necessary to provide information regarding the use of the CRM within the FMCSA customer service program and evaluates the privacy risks and mitigations associated with the collection, use, and maintenance of Personally Identifiable Information (PII) collected from members of the public and the commercial motor vehicle industry. FMCSA is updating the PIA to reflect: (1) the system's name change from Customer Information Registration System (CIRIS) to FMCSA Customer Relationship Management (CRM); (2) an update to the records disposition schedule; (3) an update to the System of Records Notice (SORN); (4) the transition from a contractor managed system to an FMCSA managed system; and (5) expanded system functionality.

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.*

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

FMCSA receives, processes, stores, analyzes, researches, and disseminates safety, licensing, and registration data for interstate and intrastate motor carriers of property including hazardous materials, motor carriers of passengers, and other motor carrier-related entities in the U.S., Canada, Mexico, and other non-U.S. based carriers. In July of 2025, FMCSA established a contact center technology modernization effort to replace the contractor provided and managed multi-channel CRM with an OST provided, and FMCSA managed registration data integrated multi-channel CRM. The new FMCSA CRM includes multi-channel contact center solution that utilizes the FedRAMP accredited cloud-based, Salesforce CRM and Amazon Telephony tool. The major FMCSA CRM functions supported include FMCSA customer service, user management, user verification via government issued identification (ID) review, tracking, call recording, data entry, data dissemination, workflow management, contact center service level agreement (SLA) monitoring, knowledge management, and report building.

The primary purposes of this solution are to address the following agency needs:

- Tracking of data dissemination requests by FMCSA authorized personnel on behalf of the agency.

[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).

- Creation of a central repository for customer interactions to better facilitate registration, licensing, vetting and enforcement efforts.
- Creation of a unique Customer Contact Record for each customer. The record is available to all FMCSA authorized users. The record includes all inquiry responses facilitating consistency across engagements and limiting opportunities for "answer shopping[2]". Answer shopping can cause inconsistent responses and increase time to answer, which is why this activity should be limited within the contact center.
- Improvement of records management and customer verification as customer submissions are now a part of a record that links inquiries with agency actions and correspondence.
- Expansion of customer engagement platforms to include email, web-to-case form submissions, chat, and co-browsing in addition to phone and mail.
- Call and screen recording for quality and training purposes.
- User, workflow, and knowledge management with skills based, subject matter expertise, and authority of resulting transaction alignment.
- SLA monitoring within the contact center of FMCSA authorized personnel for customer satisfaction, adherence, reporting, and workforce forecasting and alignment to work volumes.

CRM Workflow: The FMCSA CRM is used to capture all interactions with customers and FMCSA authorized personnel regardless of the platform used by the customer to initiate their inquiry. All customer service engagements result in the creation of or an update to a Customer Contact Record. All inquiries are assigned a unique case number which are then assigned to FMCSA authorized personnel based on skill, Subject Matter Expert (SME), or authority to research, resolve, and provide responses. The cases are assigned in the order in which they are received. The system captures the time and date of the case, along with the caller's contact information (name, company, phone, email, address, DOT#). The name of the assigned FMCSA authorized personnel and any information they include regarding the inquiry, its resolution, and the engagement is also added to the case as the FMCSA authorized personnel works to resolve the customer's issue.

The FMCSA CRM is integrated with the phone system. When a customer calls, the CRM automatically checks the customer database to determine if the phone number is already known to FMCSA CRM and associated with a customer file. If the customer already has a FMCSA CRM engagement on file, a new case is created and populated with the customer profile. If the customer is not previously known to FMCSA CRM, the CRM creates a new master customer service record and generate a new case populated with the phone number. A similar process is initiated when a customer emails or initiates an inquiry using one of the

[2] "Answer shopping" is when someone asks the same question to multiple agents until they get their desired response, rather than the most accurate.

web-to-case forms hosted on the FMCSA web site (www.fmcsa.dot.gov), except the CRM uses the customer email address to search the customer database.

FMCSA CRM Quality Assurance: The FMCSA quality assurance program allows FMCSA to provide oversight of the FMCSA CRM program, ensure the consistency and conformity with FMCSA regulations of responses, and continuously improve its customer service. At the conclusion of each engagement, the FMCSA provides the customer an opportunity to provide feedback on the process and the information provided. Customer satisfaction surveys are sent via email to all customers who provide their email address.

Once access is established, the FMCSA CRM also captures call-center performance metrics such as number of abandoned and answered calls, by whom, call duration, etc., for FMCSA analysis.

The FMCSA CRM records and stores customer calls and screenshots. Stored calls are reviewed on an ad-hoc basis by FMCSA management and contractor supervisors for quality assurance. Additionally, as part of the quality assurance program, FMCSA staff and contractor supervisors may listen to "live" calls to provide more immediate support or feedback to FMCSA authorized personnel.

The FMCSA CRM software solution provided by OST also allows customers access to online self-service options where they have access to a FAQ knowledge base that provides the top five answers by topic and allows the user to rate the effectiveness of the resolution (so the feature can be continuously improved). The FMCSA CRM also includes a web-to-case form configured to suggest FAQs before allowing the end-user to initiate a web chat or email, further reducing the need to directly engage with Customer Service Agents (CSAs).

Note: Co-browsing technologies allows customers to permit FMCSA customer service authorized personnel temporary remote access to only the customer web-browser to help the customer with their system issue or understanding.

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

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

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.

FMCSA authorized personnel notify all callers that phone calls are recorded for quality assurance and that telephone numbers may be used to contact the customer about their customer service experience.

Records in the system will be protected in accordance with DOT/FMCSA 001 - Motor Carrier Management Information System (MCMIS) system of records notice (SORN), which is being updated to include CIRIS records. The updated SORN will be available to the public on the DOT Privacy website, www.transporation.gov/privacy.

FMCSA informs the public that their PII is stored and managed in the FMCSA CRM through this PIA, published on the DOT website, www.transporation.gov/privacy. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the PII, along with all uses of the PII stored and transmitted through the FMCSA CRM system.

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.

The FMCSA CRM support allows individuals to directly engage with a FMCSA authorized personnel to amend their file.

Individuals seeking access or to amend their FMCSA CRM records may file a Freedom of Information Act (FOIA) request by sending a written request directly to:

Federal Motor Carrier Safety Administration
Attn: FOIA Team MC-MMI

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

1200 New Jersey Avenue SE
Washington, DC 20590

If an individual wishes to access or amend records that the FMCSA maintains that are protected under the Privacy Act concerning him or her, the individual may submit the request to:

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

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

- An explanation of why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DOT component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulation.

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.

FMCSA receives, processes, stores, analyzes, researches, and disseminates safety, licensing and registration data for interstate and intrastate motor carriers of property including

hazardous materials, motor carriers of passengers, and other motor carrier-related entities in the U.S, Canada, Mexico, and other non-U.S. based carriers. Information is collected directly via phone call, web-to-case form, email, and mail. For the form to be processed, customers need to provide valid, government-issued identification by email, mail, or the web-to-case form so that FMCSA authorized personnel can validate the authorizing official's identity on the form and in the system of record prior to processing. The government issued identification (ID) images retention are as follows: 1) retained during the application review (such as standard reviews, vetting and fraud) even when the escalation of incidents to different teams is permitted; 2) must be deleted just prior to the incident being solved; 3) longer-term storage for open, active investigation is prohibited; 4) if a program office needs to retain outside of these parameters, they must find an authorized FMCSA system to do so. Under no circumstances can FMCSA retain government IDs in the CRM past the time in which it's needed to decide on the received application (e.g., accept, return, reject). Permission to accept, then destroy the government issued ID can be found in 49 U.S.C. 13301, which is delegated to FMCSA in 49 CFR 1.87(a).

FMCSA information collection Office of Management and Budget (OMB) 2126-0013, 49 U.S.C. s. 31136(a) "minimum safety standards" and 49 U.S.C. s. 31502 "motor carrier requirements" allows for the collection of a social security number. Collection of the SSN is not mandated. Sole proprietor owner/operators of a business who do not have an existing employer or tax identification number may provide a social security number in lieu of an employer/tax identification number.

Customers may also request assistance regarding the medical certification process as part of the FMCSA medical program forms located at https://www.fmcsa.dot.gov/medical/driver-medical-requirements/medical-applications-and-forms. Information on these forms includes medical information required to obtain and maintain a commercial driver's license. Customers may also provide information concerning their drug and alcohol violations (including positive drug or alcohol test results and test refusals) when requesting assistance in registering under the FMCSA Drug and Alcohol Clearinghouse program. In addition to the information collected on the forms, the customer may relay company/personnel information and/or sensitive medical information over the phone or email to explain their inquiry and process their request. The contact center phone system records customer calls and retains a copy of the recording. DOT employees and contractors use their Personal Identity Verification (PIV) cards to access FMCSA CRM. FMCSA CRM collects audit records of its users.

This information is collected and stored to create a centralized repository of carrier records and communications to better serve carriers seeking status updates on various registration related transactions, ensure the agency provides consistent guidance as FMCSA authorized personnel can now easily see the notes and transaction details for each caller, and provide

detailed, up-to-date records for FMCSA's vetting and enforcement users. Additionally, the data is made available to CMV companies that use the information for educational, legal, or safety analysis purposes. Authority to collect is granted under 49 U.S.C. 5121(a), 49 CFR 1.87(d)(1), and 49 CFR part 107, subpart F.

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 collects, uses and retains only that data that are relevant and necessary for the purpose of the FMCSA CRM. Records in the FMCSA CRM may be retrieved by individuals' name, address, email address, and telephone number.

The FMCSA CRM retains and disposes of information in accordance with the applicable NARA retention schedule DAA-0557-2015-0006. The records are considered temporary and are destroyed 20 years after the end of the event product lifecycle and then until no longer needed for conducting business.

The system access records are retained and disposed of in accordance with NARA Information Systems Security Records 3.2 General Records Schedule Item 30: System Access Records. DAA-GRS-2013-0006-0003. The records are considered temporary and destroyed when business use ceases.

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.

FMCSA CRM support may request information from the individual to further assist with questions and issues, including authentication used to:

- Confirm information that is already in our system; and
- Authenticate in writing or online for request for data changes.

The specific data elements collected are dependent on the nature of the call. Information collected may include the person's name, email address, telephone number, and photo of driver's license. In addition, all inbound calls to the FMCSA CRM support are recorded for quality monitoring and customer satisfaction assurance purposes. The recorded content may contain PII (based upon the nature of the conversation).

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 CRM support ensures accuracy by collecting information directly from the individual. Callers are required to authenticate themselves before service can be granted. To complete authentication, FMCSA authorized personnel may either use the reference number provided from FMCSA correspondence, the confirmation number provided when the individual submitted a web-to-case form, or if neither apply, the FMCSA authorized personnel can create a new case record.

If the correspondence number, confirmation number or basic demographic data (such as company name, address, or phone number) is provided and the system finds a match, the FMCSA authorized personnel ask questions and requests a driver's license image to validate the caller's identity and assist with the inquiry, preventing unauthorized disclosure or updating of information. These questions include asking additional questions that are likely only known to the individual, such as name, DOT or Motor Carrier (MC) number, email address, or the principal address for the business. Each inquiry creates a case record which also allows the agency to relate cases and merge records to maintain a more up-to-date and accurate archive by reducing duplicate records and linking multiple inquiries.

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. 5 Recommended Security Controls for Federal Information Systems and Organizations, dated September 2020. 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 CRM are safeguarded in accordance with applicable rules and policies, including all applicable DOT and FMCSA 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 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. The CRM employs role-based access controls and privileges based on whether the user is an FMCSA employee or FMCSA CRM support contractor. Such authorized users may read, add, and modify as commensurate with their role.

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 is allowed to the FMCSA CRM prior to receiving the necessary clearances as required by DOT/FMCSA.

All FMCSA CRM users 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 the FMCSA CRM.

The public does not have access to the FMCSA CRM. The FMCSA CRM is approved through the Security Assessment and Authorization process under the National Institute of Standards and Technology (NIST). After a review of the security and privacy controls, the CRM was issued an Authority to Operate on June 30, 2015, and undergoes an annual security assessment to ensure compliance with federal security requirements. The FMCSA CRM also undergoes an additional security authorization whenever a major change occurs to the system. All access to the FMCSA CRM system is logged and monitored.

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 Practice Principles as best practices for the protection of information associated with the FMCSA CRM 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 Acceptable Rules of Behavior. The FMCSA Security Officer and FMCSA Privacy Officer conducts regular periodic security and privacy compliance reviews of the CRM 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 the FMCSA CRM system is used appropriately by authorized users and monitored for unauthorized usage. All FMCSA information systems are governed by the FMCSA Rules of Behavior (ROB) for IT Systems. The FMCSA ROB for IT Systems must be read, understood, and signed by each user prior to being authorized to access FMCSA information systems, including the CRM. FMCSA contractors involved in data analysis and research are also required to sign the FMCSA Non-Disclosure Agreement prior to being authorized to support the FMCSA CRM System.

Responsible Official

David Turnbull
System Owner
Customer Service Deputy Chief, MC-RSC

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2025.12.03 09:28:02 -05'00'