



U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

Federal Motor Carrier Safety Administration

Case Docketing and Management System (CDMS)

Responsible Official

Mary J Lee

Email: FMCSA.Adjudication@dot.gov

Reviewing Official

Karyn Gorman

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). Its Adjudications Division (MC-CCA) within the Office of the Chief Counsel (MC-CC) operates the Case Docketing and Management System (CDMS). CDMS serves four primary functions: (1) enabling motor carriers and their representatives to submit petitions and pleadings to contest agency enforcement actions; (2) allowing MC-CCA to manage the processing, workflow, tracking, and reporting of contested cases; (3) allowing the Enforcement Division (MC-CCE) to manage cases and submit defense pleadings; and (4) providing the public with access to view docketed petitions and pleadings.

While the system does not directly collect personally identifiable information (PII), it handles documents submitted by regulated entities that may contain PII, and this Privacy Impact Assessment (PIA) details how CDMS collects, processes, and stores such data. This PIA is being updated since the previous publication dated January 06, 2022, to incorporate new login changes, enabling Login.gov access for public users (Motor carriers, Brokers, freight forwarders, intermodal equipment providers, hazardous materials safety permit holders, cargo tank manufacturing and repair facilities (collectively referred to as motor carriers), drivers, and other individuals such as legal representatives), and MyAccess login for all internal users.

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.¹

Introduction & System Overview

The MC-CCA of FMCSA, Office of the MC-CC, is responsible for conducting administrative adjudications of disputed civil matters arising out of the Agency's enforcement actions. MC-CCA adjudicates violations under several key statutes, including:

- The Motor Carrier Safety Act of 1984 (Pub. L. 98-554, 98 Stat. 2832), codified at 49 U.S.C. Chapter 311, Subchapter III
- The Commercial Motor Vehicle Safety Act of 1986 (Pub. L. 99-570, 100 Stat. 3), codified at 49 U.S.C. Chapter 313
- The Hazardous Materials Transportation Uniform Safety Act of 1990 (Pub. L. 101-615, 104 Stat. 3244), codified at 49 U.S.C. Chapter 51
- The ICC Termination Act of 1995 (Pub. L. 104-88, 109 Stat. 803), codified at 49 U.S.C. Chapters 135–149
- The Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU) (Pub. L. 109-159, 119 Stat. 1144)
- The Moving Ahead for Progress in the 21st Century Act (MAP-21) (Pub. L. 112-141, 126 Stat. 405)
- The Fixing America's Surface Transportation Act (FAST Act) (Pub. L. 114-94, 129 Stat. 1312)

CDMS is used to process approximately 200-300 new cases the Agency receives for processing each year.

When the Agency brings a civil enforcement action against a motor carrier or other regulated entity or individual, the respondent can contest the action before the designated 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).



decisionmaker. These civil enforcement proceedings include:

- Operations out-of-service and record consolidation proceedings
- Operating authority registration appeals
- Operating authority revocation or suspension appeals
- Driver disqualification proceedings
- Imminent hazard proceedings
- Safety permit and safety rating appeals
- Civil penalty proceedings

Public users, including motor carriers, brokers, freight forwarders, intermodal equipment providers, hazardous materials safety permit holders, cargo tank manufacturing and repair facilities (collectively referred to as motor carriers), drivers, or other individuals such as legal representatives access CDMS at <https://csa.fmcsa.dot.gov/CDMS/Account/Login> using Login.gov credentials to initiate or respond to proceedings by submitting pleadings and evidentiary documents. Authorized FMCSA personnel users within MC-CCA and the Enforcement Division (MC-CCE) of MC-CC can access CDMS using their FMCSA Portal account or MyAccess.²

Once a proceeding has been initiated and all pleadings and evidence have been uploaded, MC-CCA uses CDMS to manage the case and the Agency decisionmaker will issue a decision (Final Order). The Final Order, along with the pleadings and evidence, are available for viewing on the public-facing side of CDMS in the “docket.”

1. *Obtaining an Account*

A motor carrier or individual can obtain a login.gov account via www.login.gov.

With a login.gov account, a motor carrier or their authorized representative may register for a CDMS account using an electronic registration process. Each account may be associated with one or more USDOT number(s). As part of registration, the system will collect the following information from the motor carrier:

- Username
- Password
- Last, First, and Middle Name
- Business Email address

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.



- Business Telephone number
- Business Address
- USDOT Number
- User-chosen personal security questions and responses (such as Mother's Maiden Name, Maternal Grandmothers Name, or the city where the user was born)

With a login.gov account, a driver or other individual such as a legal representative can register for access to CDMS by providing the following information:

- Username
- Password
- Last, First, and Middle Name
- Email address
- Telephone number
- Address
- User-chosen personal security questions and responses (such as Mother's Maiden Name, Maternal Grandmothers Name, or the city where the user was born)

Once a user has established an account, they are able to login to CDMS and initiate and respond to proceedings.

2. Initiating and Responding to a Proceeding

Proceedings are initiated by either the motor carrier or MC-CCE, depending on the proceeding type:

Proceeding Initiated by Motor Carrier: The Motor Carrier can log into CDMS, select the type of proceeding it would like to initiate in order to contest an Agency action, indicate whether it will be represented by an attorney or other authorized representative, and upload and submit a pleading and evidence to support its pleading. MC-CCA sees the submitted pleading as a "New Submission" on the backend of the system. MC-CCA processes the New Submission by reviewing and verifying the submission. Once verified as a valid submission, MC-CCA generates a docket number. Once a docket number is generated, MC-CCE (the division representing the Agency in the proceeding) may respond to the motor carrier's pleading (or by Order of the Agency decisionmaker) by submitting its own pleadings and evidence. The motor carrier may also upload and submit additional pleadings.

Proceeding Initiated by MC-CCE: The Agency attorney uploads and submits a pleading in support of the Agency action. The system automatically generates a docket number, and the motor carrier can respond to MC-CCE's submission (or by Order of the Agency decisionmaker) with its own submission. MC-CCE may also upload and submit additional pleadings.

3. Managing the Proceeding and Issuing a Final Decision



Once all submissions are complete, the Agency decisionmaker, Hearing Officer, Administrative Law Judge (ALJ), and MC-CCA use CDMS to draft, review, and approve Final Orders, as well as other orders for issuance. This process is not visible to the motor carrier, individual user such as a driver or legal representative, or MC-CCE.

For complete information about orders related to motor carriers and other regulated entities to be made available for enforcement actions, CDMS interfaces with other FMCSA internal systems including:

- Enforcement Management Information System (EMIS)
- Motor Carrier Management Information System (MCMIS)
- Safety Measurement System (SMS)

Data transferred between CDMS and these systems includes carrier names, carrier DOT numbers, enforcement case numbers, and investigation details. CDMS is also used to keep track of proceedings and their statuses, as well as generating reports on data.

4. *Accessing the Public Docket*

CDMS serves as a public repository for agency Orders, pleadings, and evidentiary documents. Once an Order is issued, the MC-CCA uploads the Order to the public Docket, alongside the pleadings and evidence after redacting all PII. Until the public-facing side of the system is available, these orders, pleadings, and evidence remain available to the public at www.regulations.gov.

Personally Identifiable Information and CDMS

Motor carriers and other regulated persons upload documents directly to CDMS that could include the following PII:

- Driver Name
- Date of birth
- Address
- E-mail addresses
- Telephone numbers
- Controlled substances and alcohol testing results
- Medical information
- Social security numbers
- Financial information
- Employer identification number
- Driver's license number
- Vehicle identification 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) v3³, 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 Organizations⁴.

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.

Enforcement proceedings are available for viewing on CDMS's website. FMCSA's Freedom of Information Act (FOIA) Electronic Reading Room also provides a link to CDMS's website.⁵ Documents provided by motor carriers and other regulated entities, as well as FMCSA orders, are available through this link. However, PII contained within these documents is redacted prior to releasing the documents for public viewing.

The agency does not use personal identifiers to retrieve records from CDMS. Instead, the agency retrieves records from CDMS by using case docket numbers. Therefore, CDMS is not a Privacy Act protected system of records; however, FMCSA maintains CDMS in accordance with the Fair Information Practice Principles.

FMCSA informs the public that their PII is collected, stored, and used by CDMS through this Privacy Impact Assessment (PIA) published on the DOT website. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the 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-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf

⁵ The FOIA Electronic Reading Room currently provides a link to regulations.gov, which is where the docket is currently located. <https://www.fmcsa.dot.gov/foia/final-opinions-orders-adjudicated-cases>.



and all uses of the PII collected, stored, and transmitted through CDMS.

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.

Motor carriers and other regulated entities can upload pleadings and other supporting documents, which can be used as evidence to challenge an alleged violation or the proposed consequences resulting from the violation, by logging into CDMS with a username and password. Authorized FMCSA personnel users may also upload documents that were provided by the motor carriers and other regulated entities in the same manner.

Although these supporting documents may contain PII belonging to the employees of motor carriers or other regulated entities, no PII is made publicly available on CDMS. Instead, if a motor carrier or other regulated entity would like the Agency to rely on PII that is contained in the document as evidence, it is the motor carrier's or other regulated entity's responsibility to upload two copies of the document, including an original unredacted copy and a redacted copy. While the unredacted copy is used as evidence, only the redacted copy is made publicly available on CDMS. If the motor carrier or regulated entity does not upload a redacted copy, or if the redacted still contains elements of PII, an authorized FMCSA personnel user redacts all PII before making the document available to the public.

As part of the document upload process, users are given a warning message about uploading sensitive data that is substantively similar to the following:

Do any of the documents you upload contain PII or other sensitive data? If so, you must upload both a redacted version of the documents as well as the originals. Examples of PII or other sensitive data that must be redacted include:

- drivers' license information
- dates of birth,
- personal addresses,
- personal phone numbers,
- personal email addresses,
- social security numbers,
- employer identification numbers, and
- financial information.



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 collection of PII is incidental to the purpose of the system, and therefore, the system does not use or disseminate that information. PII only exists on the documents provided by motor carriers and other regulated entities, and such information is redacted before these documents are posted to the system for the public display. PII may be submitted by the motor carrier as evidence or documentation related to a filed petition.

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.

The system only collects PII during the registration process (First and Last Name, Address, Telephone Number, Email of Driver or Business or Legal Representative) and indirectly collects PII when it is contained in a document uploaded by a motor carrier or other regulated entity for evidentiary purposes. These documents are submitted to support a petition for adjudication. For example, a sole proprietor carrier might submit a business document that contains his or her Social Security Number (SSN) (in lieu of an Employer Identification Number (EIN)) as evidence that it did not violate a regulation. Although the SSN is maintained in the system as evidence used to support the carrier's case, it is redacted prior to the evidence being made available to the public.

CDMS records are retained in accordance with items 11 and 13 of NARA-approved record control schedule N1-557-05-2.

Non-Public Field Attorney Administrative Endorsement Files (Item 11):

- Electronic copies of documents (excluding driver qualification-related documents) Delete 6 years after cutoff.
- Electronic driver qualification-related documents: Delete 15 years after cutoff.

Public Docket Adjudication Files (Item 13): Destroy 20 years after cutoff or when no longer needed, whichever is later. File copies shall be electronic and stored in the document management system. Delete paper documents after information has been converted, backed up and verified.



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 does not use PII in any manner that is incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

FMCSA does not use PII in a manner that is not specified in this PIA. Any PII contained within CDMS is not to be shared with any other governmental or private entity.

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).

Information uploaded to CDMS is used for adjudicatory proceedings and therefore must remain unmodified. Any PII submitted is redacted prior to making this information publicly available.

If an individual believes that inaccurate information pertaining to them is being maintained within CDMS, that individual may submit a written request for amendment directly to:

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

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, Security and Privacy Controls for Federal Information Systems and Organizations. FMCSA has a comprehensive information security program that contains management, operational,



and technical safeguards that are appropriate for the protection of PII.

Records in the CDMS 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 system is limited to those individuals on a need-to-know basis for the performance of their official duties, and who have appropriate clearances and permissions. All records in the CDMS are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to CDMS is logged and monitored.⁶

Logical access controls restrict users of CDMS. 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 access, which are necessary to accomplish assigned tasks in accordance with compelling operational needs and business functions of the CDMS.

Any changes to user roles require 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 CDMS must submit some personal information (e.g., First and Last Name, Address, Telephone Number, and Email of Driver or Business or Legal Representative) to FMCSA as part of the registration process. Such authorized users may add and/or delete data commensurate with their requirements.

CDMS is assessed in accordance with the Office of Management and Budget (OMB) Circular A-130 Appendix I, Responsibilities for Protecting and Managing Federal Information Resources. CDMS is approved through the Security Authorization Process under the National Institute of Standards and Technology (NIST).

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 will follow the Fair Information Principles as best practices for the protection of information associated with the CDMS. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees will be given clear guidance in their duties as they relate to collecting,

⁶ See Privacy Act of 1974; System of Records, 67 Fed. Reg. 30757 (May 7, 2002).



using, processing, and securing data. Guidance will be provided in the form of mandatory annual security and privacy awareness training.

The FMCSA Security Officer and FMCSA Privacy Officer will conduct regular periodic security and privacy compliance reviews of the CDMS 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 CDMS 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 CDMS. FMCSA contractors involved in data analysis and research are also required to sign the FMCSA Non-Disclosure Agreement prior to being authorized to access CDMS.

Responsible Official

Mary J Lee
Attorney, Adjudications Division

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN
MARIE
GORMAN

Digitally signed
by KARYN MARIE
GORMAN
Date: 2026.09.28
15:52:49 -04'00'