



**U.S. Department of Transportation**

## **Privacy Impact Assessment**

**Federal Motor Carrier Safety Administration**

**FMCSA**

### **National Consumer Complaint Database**

#### **Responsible Official**

Thomas Liberatore

Email: [Thomas.Liberatore@dot.gov](mailto:Thomas.Liberatore@dot.gov)

Phone Number: 202-366-3030

#### **Reviewing Official**

Karyn Gorman

Chief Privacy Officer

Office of the Chief Information Officer

[privacy@dot.gov](mailto:privacy@dot.gov)





## Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is an operating administration within the U.S. Department of Transportation (DOT) with the mission to reduce commercial motor vehicle-related crashes and fatalities. To further this mission, FMCSA established the National Consumer Complaint Database (NCCDB) to receive and manage filer<sup>1</sup> complaints of alleged violations of commercial motor vehicle regulations. The NCCDB allows FMCSA to identify problematic motor carriers to take necessary enforcement actions and promote compliance with FMCSA regulations.

FMCSA previously published a Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002 to address the privacy risks associated with NCCDB and its collection and use of Personally Identifiable Information (PII). FMCSA is updating the PIA to reflect changes to the system that include an update to the system of records notice (SORN), and expanded system functionality such as new complaint categories and a public company complaint search feature.

## 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.<sup>2</sup>*

*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:*

---

<sup>1</sup> "Filer" is the term used to refer to NCCDB users who submit complaints.

<sup>2</sup>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).



- *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 PLA, 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**

Since 2016, the National Consumer Complaint Database has been the central repository for motor carrier complaints received by FMCSA; however, responding to filer complaints has a long-standing Agency regulatory history. Congress first mandated the Safety Violation Hotline Service in Section 4017 of the “Transportation Equity Act of the 21st Century,” Public Law 105–178, 112 Stat. 107 (June 9, 1998) to establish, maintain, and promote the use of a nationwide toll-free telephone system to be used by drivers of commercial motor vehicles and others to report potential violations of the Federal Motor Carrier Safety Regulations.

The Motor Carrier Safety Improvement Act of 1999, Public Law 106–159, 113 Stat. 1748 (December 9, 1999), created the FMCSA and expanded the Safety Violation Hotline Service to include a 24-hour operation and accept filer complaints on violations of the commercial regulations previously administered by the Interstate Commerce Commission (i.e., household goods and hostage load<sup>3</sup> complaints).

The Safe, Accountable, Flexible, and Efficient Transportation Equity Act: A Legacy for Users, (SAFETEA–LU), Public Law 109–59, 119 Stat. 1144 (August 10, 2005) required FMCSA to create a system to record and log aggregate complaint information regarding violations of the Federal Motor Carrier Safety Regulations.

Complaints are also accepted through the NCCDB in connection with other statutory mandates including the protection of drivers against harassment and coercion under sections 32301(b) and 32911, respectively, of the Moving Ahead for Progress in the 21st Century Act, Public Law 112–141, 126 Stat. 405 (July 6, 2012).

---

<sup>3</sup> A hostage load occurs when a consumer/shipper agrees to a price or service terms with a motor carrier, but the carrier later raises the price significantly without justification and refuses to deliver the shipment. A formal definition of “hostage load” can be found on page 527 of [Title 49 U.S Code 14915\(c\)](#).



The NCCDB data provides FMCSA with statistical information regarding commercial motor carriers, in particular the household goods moving industry. The NCCDB data is used to alert filers of those motor carriers with a history of complaints related to transporting household goods and helps FMCSA provide guidance to the public on how to avoid being victimized by non-compliant moving companies. The data also allows FMCSA to identify problematic motor carriers and brokers for enforcement actions and promote compliance. Motor carriers and brokers can use The NCCDB data to assist with complaint reconciliation.

FMCSA is modernizing the NCCDB system and expanding the program to enhance FMCSA's ability to centralize the collection, monitoring, and response to filer complaints about Agency programs, establish reasonable procedures to provide timely responses to filers regarding their complaints, and share complaint information with the public as well as Federal and State agencies, as necessary and applicable. The modernization introduces twelve complaints categories across multiple FMCSA programs, automated Salesforce workflows for case assignments and routing, migration of legacy data into the modernized platform, enhanced metrics collection through Salesforce and Google Analytics to improve website performance, and a public complaint search feature that allows users to view the number of complaints associated with a company without disclosing filer PII or sensitive business information.

FMCSA assessed its operations and determined the minimum PII required to be collected and used to process filer complaints in the NCCDB for analyzing, investigating, and monitoring complaints. Using this information, FMCSA will target motor carriers and brokers with high levels of complaints for enforcement actions. The information is shared with companies, government agencies, and Congressional offices to promote compliance with Federal Motor Carrier Safety and Commercial Regulations (FMCSRs). Other statistical information is used to improve the filer's experience and develop guidance and direction for the public identifying the most common problems and the means to avoid them.

Filers can submit a complaint through the NCCDB website, by calling the FMCSA toll-free number, or by mail. When submitting a complaint online, filers are prompted to provide the PII necessary for their specific complaint based on the type(s).

In addition to name and contact information and some selectable options associated with a complaint type, the NCCDB prompts the filer to provide a narrative description of their issue and the proposed resolution in free-form text boxes. The NCCDB instructs the filer not to provide PII in their narrative description; however, a filer may provide PII in their narrative while providing details that they believe are relevant to their complaint. The NCCDB also provides an option for the filer to upload documentation to support their complaint. The documentation that a filer chooses to upload may contain PII such as their name, contact information, and other such legally sufficient evidence.



Filers can alternatively choose to submit complaints or make an inquiry by calling the FMCSA's toll-free number or submitting information to the FMCSA's mailing address. Mail submissions are scanned and manually entered in the NCCDB by a customer service agent. For complaints, the agent enters in the NCCDB the same PII over the phone or through scanned mail as filers would provide online. The agent creates an account or matches a filer to an existing account using name and contact information, when possible. This PII, along with complaint details and supporting documentation, is used to create and process the complaint.

The FMCSA may also receive a filer complaint through a third-party referral such as from a Congressional office or other agencies (e.g., the Office of the Inspector General, State law enforcement). In some instances, an FMCSA customer service agent enters the filer's name and contact information into the NCCDB to create a complaint for the filer or match to an existing complaint. This PII, along with complaint details and supporting documentation, is used to create and process the complaint.

In addition to submitting complaints, filers can choose to share their experiences to the public. Filers have the option to provide limited PII, such as name and contact information, but are not required to do so. Filers can also grant the FMCSA permission to share their experiences with the public and with external stakeholders. Submission of these customer narratives does not require that the filer create an account.

### **Personally Identifiable Information (PII) and NCCDB**

For each complaint category, the NCCDB collects the following PII for filer complaint creation. The system supports twelve (12) categories across multiple FMCSA program areas:

- (1) Moving Company - Respondent names, tracking number, addresses, phone numbers, and e-mail addresses.
- (2) Bus Company - Respondent's name, tracking number, phone numbers, email addresses, and addresses.
- (3) Truck company - Respondent names, tracking number, addresses, phone numbers, and e-mail address.
- (4) Electronic Logging Device (ELD) Provider - Driver's name, address, tracking number, phone numbers, email addresses and motor carrier names.
- (5) Drug and Alcohol Service Agents - Respondent's name, addresses, tracking number, phone numbers, email addresses.
- (6) Entry Level Driver Training/Training Provider - Respondent's name, addresses, tracking number, phone numbers, email addresses.
- (7) Property Broker - Respondent's name, addresses, tracking number, phone numbers, email addresses.



(8) Hazardous Material Transportation - Respondent's name, addresses, tracking number, phone numbers, email addresses.

(9) Intermodal Equipment Provider - Respondent's name, addresses, tracking number, phone numbers, email addresses.

(10) Motorist Safety - Respondent's name, addresses, tracking number, phone numbers, email addresses.

(11) Occupational Safety and Health Administration - Respondent's name, addresses, tracking number, phone numbers, email addresses.

(12) Registration-Related Fraud and Identity Theft - Respondent's name, addresses, tracking number, phone numbers, email addresses.

Filer name and contact information collected through account creation is automatically included for each complaint associated with the account.

The NCCDB collects the following PII for company and government user account creation:

- User's first and last name
- Business email address
- Phone number
- User's job title, department, and manager.

The NCCDB collects the following information during complaint submission process:

- Filer mailing address
- Complaint type and related answers to system questions to narrow down the allegation of the complaint
- Name of the entity in which the complaint is against
- Description of event(s) resulting in the complaint; and
- Description of desired resolution.

The filer may choose to provide additional PII as part of their complaint submission, including but not limited to:

- Account identifiers for companies to identify filers in their records to facilitate their responses (e.g., where applicable, account information, credit card information, receipts, or transaction details);
- Pertinent emails, letters, notes, text messages, voicemails, phone logs, personnel files, contracts, work products, and meeting minutes which may contain demographic and biographic information about the filer;
- Legally sufficient documents (e.g., notice, order, contract) or other such competent evidence that, if accepted as true, would establish a violation occurred;
- Information about entity employees, events and witnesses that occurred where the entity did not comply with program requirements; and





- Correspondence between the filer and the entity supporting the complaint or correspondence sent to the entity that was unanswered or not reported correctly.

The PII is provided directly by filers through the NCCDB web form, by phone when the filer calls the NCCDB, or by mail; or received from companies or those making referrals on behalf of the filer, including from Congress or other agencies. Through the NCCDB, FMCSA receives and routes complaints to companies or refers them to other FMCSA offices, as appropriate.

### **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<sup>4</sup>, 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<sup>5</sup>.*

### **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.*

The FMCSA does not secretly collect or store PII. The FMCSA clearly discloses its policies and practices concerning the PII collected and held associated with the implementation of this system. The FMCSA provides notice to individuals through a layered approach including the FMCSA website at [www.fmcsa.dot.gov](http://www.fmcsa.dot.gov) and the NCCDB website.

This document identifies the information collection's purpose, FMCSA's authority to store and use the PII, and all uses of the PII stored and transmitted through the NCCDB. Records in the NCCDB are retrieved by the individual's name and other personal identifiers and are subject to the provisions of the Privacy Act. FMCSA maintains these records in accordance with the Department's published System of Records Notice (SORN), [DOT/FMCSA 004](#),

<sup>4</sup> <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

<sup>5</sup> [http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft\\_800-53-privacy-appendix-J.pdf](http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf)



[FMCSA Complaint Center Records – 90 FR 47496, October 1, 2025](#). The SORN provides notice as to the conditions of disclosure and FMCSA's routine uses for the information collected in the system.

The SORN also requires that any dissemination of information maintained within the system be compatible with the purpose for which the information was originally collected. In addition, FMCSA issues press releases, posts information on the NCCDB website (<https://nccdb.fmcsa.dot.gov/>), sends emails via a listserv, provides periodic updates at industry outreach events, and posts information related to the NCCDB on various social media outlets. The publication of this PIA further demonstrates FMCSA's commitment to providing appropriate transparency into the NCCDB. This PIA is available to the public on the DOT website at <http://www.dot.gov/privacy>.

### 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.*

Filers voluntarily enter their information, including PII, into the NCCDB when they file a complaint. They can cancel their complaint at any time before submission if they have any concerns regarding how the information will be used or stored by the FMCSA Complaint Center. All information provided by the user is directly accessible and modifiable by the user, so errors in the information may be corrected at any time.

Filers filing complaints are given the opportunity to either accept or decline opting in with respect to their name being forwarded to the respondent along with details of the complaint. This opportunity presents itself under the following consent mechanisms:

1. Filers who call the NCCDB hotline to file a complaint are asked if they authorize their names to be forwarded to the respondent in a notification letter from FMCSA.
2. Filers who use the NCCDB website are provided the option to authorize FMCSA to use their names in a notification letter sent to the respondent.
3. Filers who file complaints via mail receive phone calls from Hotline representatives. The Filers are asked if they authorize their names to be released to the carrier in a letter from FMCSA.

If authorization is not granted by the filer, FMCSA does not send a notification letter to the respondent and the carrier will not know that a complaint was filed against it by a





particular filer. If authority is granted (opted in), FMCSA forwards a notification letter to the respondent. If the filer has declined opting in, his/her identifying information is withheld.

At any time, a filer or respondent may contact the appropriate FMCSA Program Office listed in the acknowledgement letter regarding a complaint.

Filers wishing to know if their records appear in the NCCDB to access the information about them in the system or to contest the content of the information about them in the NCCDB should send a written request to the System Manager. The request must include the requestor's name, mailing address, telephone number and/or email address, a description and the location of the records request, the complaint tracking number, and verification of identity. FMCSA's requirement for identity verification for NCCDB includes the following:

- Complaint ID/ complaint tracking number
- Name, address, and telephone number
- Date of complaint
- Origin and destination of the complaint (if appropriate)
- Respondent's name and DOT number (if appropriate)
- Description of the complaint

Under the provisions of the Privacy Act and FOIA, individuals may make requests regarding information in the NCCDB system to determine if any records have been added or modified 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

The request must include the following information:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought.

## 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 NCCDB is the Agency's management system used to collect, respond to, and refer complaints. The major goal of the FMCSA Compliant Center is to meet the requirements set forth in legislation SAFETEA-LU 4214(a)(1). It contributes to safer motor carrier operations on our nation's highways by identifying carriers for investigations and improved filer protection by ensuring moving companies use fair business practices. The NCCDB gathers information from drivers of commercial motor vehicles, filers, and industry professionals and others who report potential violations of Federal motor carrier safety and commercial regulations through the NCCDB.

The NCCDB collects filer PII in various ways: 1) when a filer directly submits a complaint through the web portal; 2) when a filer calls the FMCSA's toll-free number or mails information to the FMCSA; 3) when a filer complaint is referred to the FMCSA on behalf of a filer by a third party such as a Congressional office or government agency; or 4) when filers choose to submit an inquiry about their previous experiences and interactions with the NCCDB.

The NCCDB collects filer complaints that express dissatisfaction with, or communicate suspicion of wrongful conduct by, an identifiable entity related to a filer's personal experience in one of the following Agency program categories:

- (1) Moving Company
- (2) Bus Company
- (3) Truck company
- (4) ELD Provider
- (5) Drug and Alcohol Service Agents
- (6) Entry Level Driver Training/Training Provider
- (7) Property Broker
- (8) Hazardous Material Transportation
- (9) Intermodal Equipment Provider
- (10) Motorist Safety
- (11) Occupational Safety and Health Administration
- (12) Registration-Related Fraud and Identity Theft



## 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 data that are relevant and necessary for the purpose of the NCCDB. The NCCDB 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).

NCCDB records are retained and disposed of in accordance with applicable NARA retention schedule NI-557-05-13, Item 1. Complaint records including telephone messages, electronic mail or forms, telefaxed messages, letters, are retained temporarily and destroyed or deleted 36 months after the information has been converted into an electronic medium, backed up, and verified. Master data files of the NCCDB are temporary records and deleted 6 years after the end of the calendar year in which a case is closed or when no longer needed for reference whichever is sooner.

## 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 uses the NCCDB complaint information, including PII collected, to meet the following objectives:

- Receive filer complaints and route them for response by the entity that is the subject of the complaint, or to another authorized user for further investigation
- Respond to filer inquiries by providing necessary information or resources
- Conduct research and analysis to understand trends in the filer experience. This data can also be helpful in establishing the presence of a harmful practices in the marketplace or violations of the FMCSRs. Such information may be analyzed to prepare and publish reports and to facilitate supervisory, enforcement, and FMCSA monitoring activities
- Improve customer service and operations (e.g., data associated with a phone interaction may be used to evaluate the performance of customer service agents)
- Share complaint data with other authorized federal, state, and local partners to aid in their practices in accordance with the appropriate complaint type
- Provide statutorily mandated reports to Congress, as necessary, and



- Meet FMCSA's objective of ensuring that customer service experiences are fair, transparent, and effective.

The FMCSA collects name, email address, and phone number to create authenticated user accounts and address when the filer submits a complaint. FMCSA may use this information to communicate or manage the complaint process, depending on the user's role. FMCSA also uses filer name and contact information to verify a filer if they contact the FMCSA to receive updates on their complaint and to provide automated status updates to filers about the progress of their complaint, or to send an alert if any additional action is needed by the filer.

There is a risk that filers may submit more PII than necessary when submitting a complaint. For example, an individual could unnecessarily provide their personal information, health information, or other types of PII in their complaint description. To mitigate this risk, the NCCDB cautions the submitter not to include PII in their complaint narrative since it will be collected separately in dedicated fields later in the complaint form. FMCSA designed the NCCDB to streamline the collection of PII to only include the information needed to help companies identify filers in their own records. Similarly, the same approach promoting minimization is applied to other data fields where possible, such as only collecting PII where necessary to help companies respond to complaints and aid FMCSA in its investigative efforts.

FMCSA ensures that the information collected through the system is only used for authorized purposes such as analyzing, investigating, and monitoring complaints. FMCSA also ensures that information is only shared with FMCSA staff, companies, government agencies, and Congressional offices with approved data access related to their valid need-to-know.

### **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).*

There is a risk of inaccurate information being submitted to the NCCDB. Filers and third parties submit information by web, by postal mail, or over the telephone. If over the telephone, there is a possibility that the representative did not accurately record the filer's submission. This is mitigated by the training the NCCDB customer service staff has received regarding use of the NCCDB, the fields that guide what information needs to be entered into the NCCDB, and the review of the information with the caller before closing out the entry.



There is also a risk that the filer provides incorrect information through the web or by mail or telephone. The FMCSA mitigates this risk by ensuring the filer affirms the following statement: “the information given is true to the best of [their] knowledge.” When providing information through the web, NCCDB has built-in processes and controls to mitigate issues with accuracy and completeness prior to and following filer submission of information. For example, filers must validate their email address before starting to submit a complaint online. Online forms include field-level data validation rules to ensure completion at the time of submission. Finally, the filer is prompted to review the information provided on the online complaint form for accuracy before submission.

Regardless of the channel of submission, if FMCSA determines a complaint is incomplete, FMCSA contacts the filer to request that they provide additional information. Additionally, the filer can contact FMCSA through the NCCDB to correct or amend records about themselves or can access submissions online through the NCCDB to make corrections. The FMCSA also provides filers a means through the Privacy Act to amend or correct a person’s records at their request, or a request made on their behalf. Information about Privacy Act requests is available in the SORN DOT/FMCSA 004, and through use of a Freedom of Information Act request.

Finally, there is a limited risk that FMCSA staff may manually route a complaint to an incorrect company or other authorized user. However, this risk is mitigated through NCCDB functionality to automatically remove entity access to complaint information through administrative response functions. FMCSA also instructs the entity to delete downloaded complaint information if a complaint is incorrectly routed to them.

## 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, and Recommended Security Controls for Federal Information Systems and Organizations, dated September 2020.



The FMCSA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. All required authorizations (e.g., to operate, analysis) were established before the NCCDB was deployed. 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 NCCDB are safeguarded in accordance with applicable rules and policies, including all applicable DOT and FMCSA automated systems security and access policies. Strict controls are imposed on all DOT/FMCSA systems to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in the NCCDB 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 that are stored in the NCCDB are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. 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 NCCDB prior to receiving the necessary clearances as required by DOT/FMCSA.

All access to the NCCDB 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 FMCSA employees and contractors 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 PII associated with the implementation of the NCCDB. In addition to these practices, additional policies and procedures are consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees is given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training as well as the DOT/FMCSA Rules of Behavior. The FMCSA





Information System Security Officer and FMCSA Privacy Officer conducts periodic security and privacy compliance reviews of the NCCDB consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b (3), Securing Agency Information Systems.

### **Responsible Official**

Thomas Liberatore  
Business Owner  
Director, Office of Enforcement and Compliance, FMCSA

### **Approval and Signature**

Karyn Gorman  
Chief Privacy Officer  
Office of the Chief Information Officer

DOT Privacy Office - Approved - 12/18/2025