U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration

FMCSA

Crash Risks by Commercial Motor Vehicle (CMV) Driver Schedules

(Crash Risks)

Responsible Official

Theresa Hallquist
Email: theresa.hallquist@dot.gov
Phone Number: 202-366-1064

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

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 is authorized to conduct research under 49 U.S.C. 31108 Motor Carrier Research and Technology programs, and under section 31108(a)(3)(A-B), FMCSA may fund research, development, and technology projects related to (A) the causes of Safety Critical event (SCEs), injuries, and fatalities involving commercial motor vehicles and (B) means of reducing the number and severity of SCEs, injuries, and fatalities involving commercial motor vehicles. This information collection supports the DOT Strategic Goal of Safety. This research requires data to be collected for hours of service (HOS) duty logs, crash and incident data, and inspection violations records.

As part of this effort, Pulsar Informatics, Inc. (Pulsar), under contract to FMCSA, will collect the data necessary to address the study objectives and research questions. The information collected will be used to examine the relative risk of crashes and inspection violations based on various factors related to the driver's work schedule and demographics.

This Privacy Impact Assessment (PIA) is being conducted to address the risks associated with Pulsar collecting, processing, and maintaining Personally Identifiable Information (PII) within each set of data collected on behalf of FMCSA.

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]

DOT Privacy Office - Approved - 05/01/2025

[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).

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

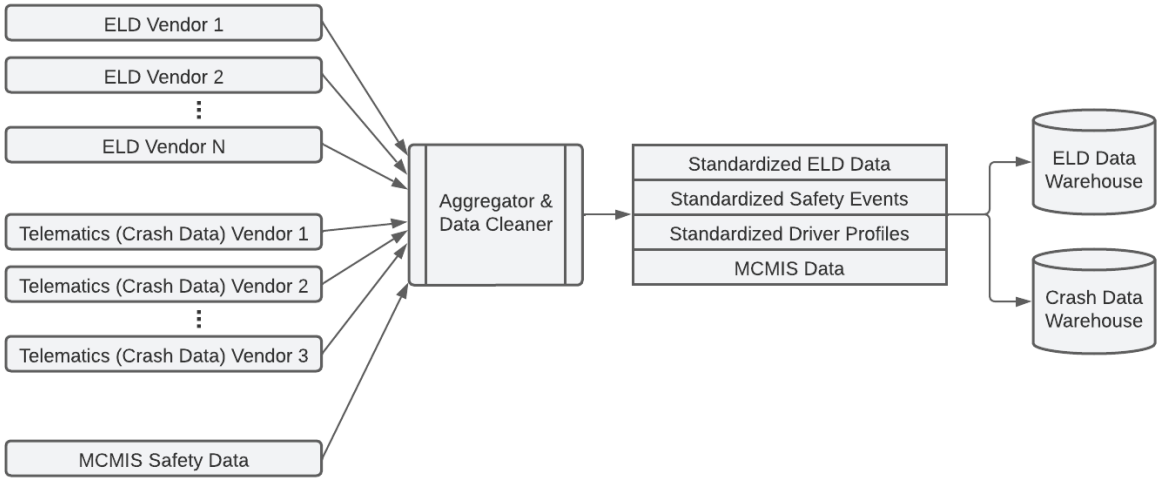
FMCSA is committed to supporting the collection and analysis of Electronic Logging Device (ELD) and crash data from property-carrying and passenger-carrying commercial motor vehicle (CMV) carriers to assess risks posed by alternative schedules as they relate to various aspects of HOS provisions.

Trucking Fatigue Meter is a software product that integrates with ELD and telematics service providers in the CMV industry to provide drivers with real-time alerts relative to conditions associated with elevated fatigue and crash risk. Several functions currently delivered by the Trucking Fatigue Meter are used in the study's data collection system:

- Collection of ELD data through integrations with most ELD service providers
- Collection of crash data through integrations with most Telematics service providers
- Standardization of ELD and crash data
- Analysis of crash risk relative to HOS patterns

Additional data is collected (driver demographic data, telematics / crash data, and ELD data not available via Trucking Fatigue Meter integration) directly from participating carriers via a secure file transfer system. Finally, crash and inspection data are retrieved from Motor Carrier Management Information System (MCMIS). These data sets are aggregated, standardized, and stored in a secure data warehouse:

DOT Privacy Office - Approved - 05/04/2026



Data collection from participating carriers will take place over a period of four years.

Prior to data collection, carriers sign an Informed Consent Form (ICF) that is approved by an Institutional Review Board (IRB). All data will be collected electronically. Data from MCMIS (i.e., crash data and inspection violations) will be collected monthly via a link to a secure, password-protected website used by DOT. Each link is delivered to the research team by email from the Data Analysis and Reports Team (DART) in the FMCSA Analysis Division. HOS and incident and crash data will be collected continuously and automatically through an integration with carriers' telematics system provider (TSP) using Pulsar's Trucking Fatigue Meter technology. Driver demographic data will be collected from electronic reports that carriers export from their existing fleet management software, human resources management system, driver management platform, or other appropriate system on a quarterly basis. Carriers will upload these reports via a secured file transfer platform (e.g., Box.com). There will be no burden on individual drivers. The research team aims to recruit approximately 60 carriers.

Data Collected

1. Driver identification information, including last name, first name, driver license number, license state, date of birth
2. Driver demographic data including age, sex, and years of experience
3. Driving data including HOS duty logs, SCE data, and inspection violation data

Data Deidentification

Pulsar, under contract with FMCSA, is required to develop a publicly available deidentified data set to be housed in the FMCSA Data Repository. All PII shall be removed, and other methods of protecting privacy shall be utilized as needed. On a regular 6-month interval, data will be deidentified for use in data analysis and reporting, and driver-identifiable data older than six months will be deleted.

DOT Privacy Office - Approved - 05/2

Data Analysis and Reporting

At the end of the collection period, the data will be used to perform analysis to answer research questions related to crash risk under various conditions and time frames. A final report will be drafted, peer reviewed, and presented to FMCSA in a final briefing. No PII will be part of the report. All data collected will be reported in an aggregated format in which participants cannot be identified. The final report will be saved to FMCSA's Office of Research Publications shared drive.

Contract End Closeout

All study data is maintained or destroyed in accordance with the approved Record Disposition Schedule (RDS). After the study ends, administrative data is destroyed at a predetermined date annually. A dataset that has been processed and reduced to remove PII following Office of Management and Budget (OMB) guidance will be provided to FMCSA for inclusion in FMCSA's Data Repository for use in future analyses.

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[2], 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[3].

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.

As this study requires the collection of data about human subjects, approval from WCG Clinical Solutions IRB is required before data collection begins. This study will be reviewed

DOT Privacy Office - Approved - 05/04/2026

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

by this IRB prior to the start of data collection. The IRB will also approve an ICF that carriers will sign prior to participating. The ICF will outline the carrier's role in the study, describe how their data (including PII) will be used, and describe how deidentified data will be housed in the FMCSA Data Repository.

Pulsar, under contract with FMCSA, is required to develop a publicly available deidentified data set to be housed in the FMCSA Data Repository. All PII will be removed, and other methods of protecting privacy will be utilized as needed.

This PIA identifies the information collection's purpose and Pulsar's authority, under FMCSA, to collect, store, and use the PII for the purposes of the contracted study. This PIA will be available to the public on the DOT Privacy website, www.transportation.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.

The data collected for this project is provided by the participating carriers. In data subject rights terms, the carriers are data controllers, and by participating in the project they are asserting that they have informed the individual drivers represented in the data of the PII disclosure to Pulsar for use in this study. Pulsar will fully support the carriers in affording drivers the ability to access their PII that has been collected for this project and to have it corrected, amended, or deleted, as appropriate.

Once the data has been de-identified, there will be no way for individual drivers to identify their data to ask for removal. All data made available in the FMCSA Data Repository will be deidentified. Any concerns by individual drivers may be expressed by sending an email to privacy@pulsarinformatics.com.

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.

DOT Privacy Office - Approved - 05/04/2026

FMCSA conducted a study that evaluated the impact of time-on-task, in terms of driving hours and working hours on SCE and the benefits of breaks from driving (Blanco, M., et. al., 2011)[4]. The study included 99 drivers who drove a total of 700,000 miles, during which naturalistic driving video and data were collected. FMCSA needs additional data to answer important questions related to driver schedules and how these factors impact overall driver performance and fatigue. This project will collect additional information to improve decision making regarding various aspects of the hours-of-service (HOS) provisions, how HOS provisions are being used, and the impact of driver schedules on crash risk. The preamble of FMCSA's 2011 Final HOS Rule stated: "FMCSA is committed to an analysis of the relative crash risk by driving hour, the impact of the changes in the HOS provisions, and examine difference in crash risk after restarts that include two nights and those that do not."

FMCSA and Pulsar are unaware of other research conducted, currently or in the past, that could be used to fulfill the research goals of the Crash Risks by CMV Driver Schedules project.

FMCSA is authorized to conduct this research under 49 U.S.C. 31108[5], Motor Carrier Research and Technology Programs. Under section 31108(a)(3)(A-B), FMCSA may fund research, development, and technology projects related to (A) the causes of SCEs, injuries, and fatalities involving commercial motor vehicles and (B) means of reducing the number and severity of SCEs, injuries, and fatalities involving commercial motor vehicles. This information collection supports the U.S. Department of Transportation (DOT) Strategic Goal of Safety. The study aim is to improve decision making related to the usage of HOS provisions and the impact of CMV driver schedules on crash risk.

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 determined that this collection of information is necessary for study completion. There is currently no existing dataset that can be used for this project. The data collected and retained during this project is limited to the datasets described in the system overview and retained only for the duration of the contract performance period.

DOT Privacy Office - Approved - 05/04/2026

[4] https://rosap.ntl.bts.gov/view/dot/131

[5] House of Representatives, Congress. (2024, January 3). 49 U.S.C. 31108 – Motor carrier research and technology program. [Government]. U.S. Government Publishing Office. https://www.govinfo.gov/app/details/USCODE-2023-title49/USCODE-2023-title49-subtitleVI-partB-chap311-subchapI-sec31108

To produce the publicly available data set, individual driver identifiable information is deidentified according to OMB guidance, effectively removing PII fields and assigning an anonymized driver ID.

Individual driver data falls under the research record retention requirements found in the Department of Health and Human Services (HHS) regulations for Protection of Human Research Subjects at 45 CFR 46. The HHS protection of human subjects regulations require institutions to retain records of IRB activities and certain other records frequently held by investigators for at least three years after completion of the research (45 CFR 46.115(b)).

For all files, any paper documents will be destroyed after the information has been converted into an electronic medium, backed up, and verified. For correspondence files, electronic files will be deleted 5 years after cutoff. Electronic files related to publications and completed research products will be kept up to 3 years in office after cutoff then transferred to NARA in accordance with 36 CFR 1228.270 (if the disposition is permanent) or deleted when no longer needed (if the disposition is temporary). Reference files that are electronic will be deleted when no longer needed.

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 IRB process requires the researcher to provide a detailed protocol explaining the purpose of the study, how the data is collected and stored and who may have access to the data in the future. This study only collects the data necessary to answer the research questions that have been approved by WCG Clinical Solutions IRB.

External researchers can request access to identifiable data by submitting a request on the website to the Data Repository. For access to be approved, the requester must show proof of IRB approval and sign a Data Use License (DUL) with Virginia Tech Transportation Institute (VTTI) describing their need for identifiable data. The request must be approved by FMCSA. Identifiable data may only be viewed in the secure data enclave located at VTTI. Researchers cannot remove PII from the secure data enclave. All personal items are examined before the researcher can leave the secure data enclave to ensure no PII is removed.

DOT Privacy Office - Approved - 05/07/2026

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).

Driving data (HOS logs) are collected directly from carrier ELD systems, where possible. Crash / SCE data and vehicle inspection reports are collected directly from MCMIS.

Driver identification and demographic data, as well as HOS data when an ELD integration is not available) are provided directly by participating carriers.

HOS data is aggregated in Trucking Fatigue Meter, which standardizes the data from various sources and enables Pulsar's researchers to identify data quality issues.

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 secured using appropriate safeguards to prevent loss, unauthorized access, destruction, misuse, alteration, or disclosure. These protections follow federally mandated standards for information systems as outlined in the Federal Information Security Management Act (FISMA). Specific requirements are established in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006), and in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (September 2020). FMCSA maintains a robust information security program that includes managerial, operational, and technical measures to protect PII. The program is designed to:

- Safeguard the confidentiality, integrity, and security of PII;
- Defend against reasonably foreseeable risks or hazards that could compromise PII; and
- Prevent unauthorized access to or use of PII.

Records managed by Pulsar are protected under all applicable regulations, DOT system security policies, and access control requirements. controls are implemented to reduce the likelihood of compromise. Access to infrastructure housing these records is restricted to authorized personnel who require it to perform official duties and possess the necessary

DOT Privacy Office - Approved 05/04/2026

clearances and permissions. Additionally, the records are protected from unauthorized access by a combination of administrative, physical, and technical safeguards. All access to the 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.

Regular testing of information systems security is performed by Pulsar operations personnel. These tests include the use of assessment and scoring tools provided by the Center for Internet Security. FMCSA personnel and FMCSA contractors are required to attend security and privacy awareness training and role-based training offered by DOT/FMCSA. This training allows individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly and securely act in situations where they may use PII while performing their duties.

FMCSA follows the Fair Information Principles as best practices for the protection of information associated with the Data Repository. 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.

Responsible Official

Theresa Hallquist
System Owner
Research Analyst, FMCSA

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2026.05.04 11:22:29 -04'00'

DOT Privacy Office - Approved - 05/04/2026