U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration

FMCSA

Electronic Logging Device (ELD) System

Responsible Official

Bill Mahorney
Email: Bill.Mahorney@dot.gov
Phone Number: 202-493-3001

Reviewing Official

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

December 20, 2021

Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) under authority of the Motor Carrier Act of 1935, the Motor Carrier Safety Act of 1984, the Truck and Bus Safety and Regulatory Reform Act of 1988, the Hazardous Materials Transportation Authorization Act of 1994, and the Commercial Motor Vehicle Safety Enhancement Act of 2012 (part of Moving Ahead for Progress in the 21st Century Act (MAP-21)) published a rule that requires use of electronic logging devices (ELDs) for recording hours-of-service (HOS) information. Under this rule, commercial motor vehicles (CMVs) operated in interstate commerce, by drivers required to maintain records of duty status (RODS), must be equipped with ELDs.

The agency developed the ELD system to facilitate the transfer of HOS data to authorized safety officials for their review during roadside inspections, investigations, and safety audits. The ELD system facilitates retrieval of data recorded by ELDs and provided in the ELD output file, analysis of the ELD data, and identification of instances of potential non-compliance. The safety official uses the results of this initial assessment to determine if citable HOS violations exist, and to take appropriate action. Examples of these actions include providing a warning of a minor violation, issuing a citation for a more significant violation, or placing a driver out-of-service for a serious violation.

The agency requires that ELDs meet certain technical specifications that are set forth in its HOS regulations. FMCSA may use ELD data to investigate registered ELDs and determine whether devices are compliant with the HOS regulations. Devices that are found not to be compliant with FMCSA's technical requirements may be removed from FMCSA's list of registered ELDs.

Although the primary purpose of the ELD system is to support FMCSA enforcement of the HOS regulations, FMCSA may also use ELD data to inform research efforts related to safety regulations, including driving hours, as such research may ultimately improve compliance with HOS requirements. As such, FMCSA may access ELD data collected by safety officials to inform analysis activities. In such situations, FMCSA thoroughly de-identifies the data before releasing it to the public, in the interest of protecting carrier and driver identities.

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

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 requires motor carriers to install electronic logging devices (ELDs) on commercial motor vehicles (CMVs) that are involved in interstate commerce and operated by drivers who are required to keep records of duty status (RODS). The ELDs must be capable of generating a standard data file in a specified format and transferring that file to FMCSA's ELD system so an authorized safety official can review a driver's hours of service (HOS). The agency developed the ELD system to facilitate the transfer of HOS data and the review of HOS data by authorized safety officials. The ELD system is also used to manage and

[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).

monitor ELD vendor's compliance with ELD device registration requirements and conformance to ELD technical specifications.

The ELD system consists of the following components:

- Electronic Record of Duty Status (eRODS) HOS review tool
- ELD website and database
- ELD provider web service
- Enforcement ELD web service

Electronic Record of Duty Status (eRODS). eRODS is a software application installed on a safety official's computer or accessed via the ELD website and is used to retrieve and display the information on an ELD output file. eRODS allows enforcement users to analyze a driver's HOS data and perform a roadside inspection, investigation, or safety audit.

An ELD device is required to support one of two options for providing an ELD file to FMCSA:

Option 1 is telematics which consists of web services transfer or email transfer. For the web service transfer, the ELD uploads the data file directly to FMCSA servers via a secure web service call. For an email transfer, the ELD sends the data file via secure, encrypted email to FMCSA servers.

Option 2 is local transfer which consists of Bluetooth connection or USB transfer. The Bluetooth connection allows the ELD to use the safety official's internet connection to connect to the ELD provider web service to transfer to FMCSA servers. The USB transfer is made using the safety officials self-encrypting USB device to transfer data from the ELD to the safety official's device. This is the only method that does not require internet connectivity.

ELD website and database. The ELD website and database is the centerpiece for all stakeholders. The website includes a section for each stakeholder. ELD vendors use the website to register their organization with FMCSA and to self-certify and maintain the registration of each ELD. ELD vendors also have access to tools necessary to build and test their interfaces with FMCSA. Motor carriers can access the ELD site to obtain information on the ELD Rule and other communications that educate them on the ELD process. They can also review the list of self-certified ELD devices. Enforcement users can access ELD policy and training information related to ELDs as well as access web eRODS for reviewing motor carrier HOS compliance.

The FMCSA vetting team reviews ELD vendor submissions prior to placing the ELD on the list of self-certified ELDs. The ELD database contains all the ELD vendor and device registration information. It also stores the ELD files submitted to FMCSA via ELD provider web service.

The ELD technical team also reviews ELD file submissions from specific ELD devices as part of ELD device technical compliance investigations as described below under process of reviewing ELD data.

ELD provider web service. The ELD provider web service provides the means for a registered, self-certified ELD device to transfer, via web service or blue-tooth transfer options, an ELD file to FMCSA. During the self-certification process for an ELD device, the ELD vendor provides FMCSA with their public certificate and receives FMCSA's public certificate and additional information on building the connection between their ELD and FMCSA's ELD provider web service. Once the connection is established, the ELD can submit output files of a driver's HOS data to FMCSA via this service.

Enforcement ELD Web Service. The enforcement ELD web service is used to transfer the ELD file to the safety official's eRODS HOS review tool. The eRODS desktop and web-based system has a connection to this service. To complete the connection, an enforcement officer enters their portal credentials and after proper validation, can access the ELD files submitted to the safety official via this service. Files that are submitted via ELD provider web service, Bluetooth connection, or email can be accessed by enforcement via a connection to this service.

Process of Reviewing ELD Data

Safety officials must review data from ELDs for compliance with 49 CFR Part 395 during a roadside inspection, an off-site or onsite investigation, or safety audit of a motor carrier.

The first step for safety officials is to obtain the ELD data from the driver during an inspection or from the motor carrier for an investigation or safety audit. The safety official selects the transfer method used during this transfer based on the option(s) supported by the ELD device. As noted earlier, if the ELD device supports the telematics transfer option, the safety official can request transfer via the ELD vendor web service or via an encrypted email transfer to FMCSA servers. If the ELD device supports the local transfer option, the safety official can request transfer to FMCSA servers via Bluetooth transfer option or via a self-encrypting USB device transfer to the safety official.

The safety official will use eRODS to perform the HOS compliance review. As part of this, eRODS will:

1. Connect to the enforcement ELD web service to retrieve and load the provided ELD file (for web service, email, or Bluetooth transfer options).
2. Load ELD file from the safety official's USB device (for USB transfer option).
3. Ensure an ELD is registered with the agency and is on the self-certified list of ELD devices.*
4. Analyze the data file sent from the ELD.*
5. Flag potential HOS violations for the safety official to review.*

Note that items with an * are also performed by the ELD provider web service.

The eRODS software displays ELD data in a format that is similar to paper-based RODs with each day's data presented with an ELD file header, a daily header, and a graphical presentation of duty status changes. In addition, an events list contains details for each recorded event. eRODS also provides visual indicators and a listing of potential areas of non-compliance with HOS regulations. Based on a review of the HOS data and other supporting documentation, the safety official determines whether violations should be cited, or other enforcement actions should be taken.

Twenty-four hours after initial transfer, a safety official will be unable to retrieve an ELD file provided by a driver for a roadside inspection. ELD files that are submitted as part of a motor carrier's safety audit or investigation are available for retrieval and review by safety officials within eRODS until the safety audit or investigation is completed. When these timeframes are met, the submitted ELD file will be deleted from FMCSA's ELD database unless retained for an ELD device investigation as described below.

Since data is not stored within eRODS, if it is determined that the HOS data needs to be retained by the safety official to support any follow up actions, the safety official must save the ELD file to their local system. The ELD file can then, if necessary, be uploaded into the motor carrier's record within the electronic document management system (EDMS).

In addition, if FMCSA initiates an investigation into the technical compliance of an ELD, ELD files submitted by motor carriers using the device under investigation will be retained within FMCSA's ELD database. These files will be available to FMCSA's ELD technical team to support the investigation of the device. Files used for an investigation into the technical compliance of an ELD will be deleted 6 years after the investigation is closed, consistent with FMCSA's document retention practices for motor carrier investigations. Safety officials do not have access to these ELD files.

ELD Functions

The ELD functions as a recording-only technology with the ability to transfer data to authorized safety officials. The ELD does not analyze or review driver's RODS data for any purpose, including compliance. The ELD is not prohibited from providing a specific type of advisory or warning signal to the driver of potential HOS non-compliance (for example, nearing the limit on daily on-duty-driving time).

Access to the ELD by a driver (and other users, including dispatchers and supervisors) requires a unique authenticated account with unique login identification. The unique identification includes the entire driver's license number and driver's license issuing State. This is necessary to prevent a motor carrier (or a driver) from creating multiple aliases for an individual driver.

Drivers have the opportunity to review all information generated by ELDs and to make additional annotations ("annotations" are entries that would augment, but not overwrite, other recorded data) as needed to clarify information related to their duty status. These annotations would generally cover the same types of information that would be included in the "Remarks" section of a paper RODS. After drivers complete this review, they electronically sign, and by that action, certify the accuracy of their duty status information before it is transmitted to the motor carrier. If a driver knowingly falsifies this certification of accuracy, then the driver could be liable for civil penalties pursuant to 49 U.S.C. 521.

As noted earlier, each driver or other user of the ELD needs an authenticated account with a unique login identification assigned by the motor carrier. At the time the vehicle begins moving, the ELD records the driver account logged into the ELD. If no driver is logged in, then the ELD would record a standard identifier. The motor carrier uses this identifier to mark the record as incomplete and in need of amendment. The carrier then needs to add the name of the driver (if the driver neglected to log in), or to otherwise identify who was operating the CMV (for example, an engine service technician taking the CMV on a test run).

Personally Identifiable Information (PII) and ELD

FMCSA requires that ELDs (as well as their support systems, if used) be capable of generating a standard data file in specified format and transfer it to an authorized safety official upon request. The following information is recorded within the ELD dataset and transferred to authorized safety officials when requested. Data elements marked with an asterisk "*" may be PII when linked to ELD username or driver/ co-driver name or license number. FMCSA de-identifies any ELD data that contains PII in any public-use database that results from a special study.

- ELD username
- Driver's first name, last name
- Co-driver first name, last name (if there is a co-driver)
- Co-driver ELD username (if there is a co-driver)
- Driver's license number
- State of license issuance*
- Duty status*
- Date and time of each change of duty status*
- Location of CMV when the CMV's engine is turned on and turned off, at each change of duty status, and at intervals of no more than 60 minutes when the CMV is in motion.*
- Starting time for each 24-hour period (e.g., 12 midnight, 12 noon). This is a requirement for paper RODS and carriers over to ELDs. The reason is that many elements of the HOS regulations are based on activities within 24-hour periods.*

- Hours in each duty status to 1-minute accuracy.*
- Special driving mode status (e.g., personal conveyance, yard move).*
- Log of user activity ("user" is generally the driver, but could be a technician test-driving the CMV or a yard-hotelier repositioning the CMV)*
- 17-digit vehicle identification number (VIN)*

Additional data is recorded and provided within the ELD output file, including engine hours, vehicle miles traveled, and motor carrier identification data (motor carrier name and FMCSA-issued US DOT number).

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[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.

FMCSA clearly discloses its policies and practices concerning all PII collected, maintained, used, and disseminated pursuant to the implementation of all FMCSA rules. FMCSA provides notice to individuals several different ways. These include the publication of the Supplemental Notice of Proposed Rulemaking (SNPRM) and Electronic Logging Devices and Hours of Service Supporting Documents Final Rule; the privacy policy on the FMCSA website (www.fmcsa.dot.gov); and the System of Record Notice (SORN) that will be published in the Federal Register and on the DOT Privacy Program website. The SORN will

[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

provide notice as to the conditions of disclosure and FMCSA's routine uses for the information collected in the system. The SORN will also require that any dissemination of information maintained within the system be compatible with the purpose for which the information was originally collected. In addition, FMCSA issued an Electronic Logging Devices Rule Brochure and an ELD Fact Sheet to the industry on the agency website.

The publication of this PIA further demonstration FMCSA's commitment to providing appropriate transparency into the ELD system. 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.

FMCSA ensures that individuals have the right to (a) obtain confirmation of whether or not FMCSA has PII relating to him or her; (b) access the PII related to him or her within a reasonable time, cost, and manner and in a form that is readily intelligible to the individual; (c) obtain an explanation if a request made under (a) and (b) is denied and challenge such denial; and (d) challenge PII relating to him or her and, if the challenge is successful, have the data erased, rectified, completed, or amended.

CMV drivers who operate CMVs in interstate commerce and who are required to keep RODS to record their HOS information are required to use an ELD. Motor carriers manage their CMV drivers' ELD user accounts and ensure that individuals are properly authenticated and assigned rights to access, read, and annotate the information associated with the ELD records.

When a driver certifies and signs a paper RODS, he or she is stating that its contents are true and correct, and the driver then submits it to the motor carrier as a part of the motor carrier's records. Similarly, when a driver logs into an ELD and certifies his or her electronic RODS, he or she is following the same process. The driver has control over his or her ELD RODS. The driver has the right to review or edit the data before submitting it, and he or she has the right to annotate the data. The driver also has the right to access the data for the six months that the carrier must retain it. While the motor carrier may suggest changes to the RODS, to protect the driver and the integrity of the record, the driver must re-certify the record after making any edits.

FMCSA adopted effective and timely procedures to permit each driver to examine the PII that is on file with FMCSA concerning him or her and to obtain a copy of such information upon a written request under the Privacy Act.

Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOT by complying with DOT Privacy Act regulations found in 49 CFR Part 10. Privacy Act requests for access to an individual's records must be in writing (either handwritten or typed), and may be mailed, faxed, or emailed and must include a completed Privacy Waiver form.

DOT regulations require that the request include a description of the records sought, the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Additional information and guidance regarding DOT's Freedom of Information Act / Privacy Act (FOIA/PA) program may be found on the DOT Web site (www.dot.gov/foia).

Federal Motor Carrier Safety Administration
Attn: FOIA Team MC-MMI
1200 New Jersey Avenue SE Washington, DC 20590
Fax: (202) 385-2335
Attn: FOIA Team E-mail: foia@fmcsa.dot.gov

FMCSA has a redress process to challenge inspection data. The process, called DataQs, is accessible at https://dataqs.fmcsa.dot.gov. DataQs provides an electronic method for motor carriers and drivers to file concerns about information maintained in FMCSA systems (principally, roadside inspection results included in MCMIS). The DataQs system automatically forwards data concerns to the appropriate Federal or State office for processing and resolution. Any challenges to data provided by State agencies are resolved by the appropriate State agency. The system also allows filers to monitor the status of each filing.

Under the DataQs process, FMCSA cannot "correct the information associated with the ELD records" that are stored in the motor carrier's information systems. If an interstate CMV driver is incorrectly identified in an enforcement action, the DataQs system provides an avenue for a driver or motor carrier to request FMCSA to correct enforcement information that it may store in its own information systems.

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.

The authority for the ELD system is derived from: The Motor Carrier Act of 1935 (Pub. L. 74-255, 49 Stat. 543, August 9, 1935), as amended, (the 1935 Act), The Motor Carrier Safety Act of 1984 (Pub. L. 98-554, Title II, 98 Stat. 2832, October 30, 1984), as amended, (the 1984 Act), Section 9104 of the Truck and Bus Safety and Regulatory Reform Act (Pub. L. 100-690, 102 Stat. 4181, 4529, November 18, 1988), Section 113 of the Hazardous Materials Transportation Authorization Act of 1994, (Pub. L. 103-311, 108 Stat. 1673, 16776-1677, August 26, 1994), (HMTAA), Section 32301(b) of the Commercial Motor Vehicle Safety Enhancement Act, enacted as part of the Moving Ahead for Progress in the 21st Century Act (Pub. L. 112-141, 126 Stat. 405, (July 6, 2012)) (MAP-21). The authorities are described in detail in the preamble of the regulations.

FMCSA limits its use of PII related to purposes pertaining to enforcement of HOS regulations. The collection of PII is necessary because it allows Federal and State law enforcement agencies to match an interstate CMV driver's name with his or her HOS record. In order to perform HOS compliance-assurance and enforcement functions, authorized safety officials must use personal information to verify the time, date, and location for duty status changes of interstate CMV drivers to ensure that motor carriers and interstate drivers comply with applicable HOS regulations. FMCSA does not retain HOS data beyond use for roadside inspection, investigation, safety audit, follow-up enforcement actions, or research projects relating to highway safety and HOS compliance.

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 proposes to maintain information associated with the ELD records only if citable HOS violations are found during an inspection, investigation, safety audit or, if the ELD records are needed to investigate the compliance of a device with FMCSA's technical specifications, or if the ELD records were obtained as part of an approved special study. In the latter instance, FMCSA de-identifies the ELD records prior to sharing in any resulting public-facing dataset. Motor carriers must retain records for six months from date of receipt. In accordance with FMCSA's MCMIS record schedule Job Number N1-557-05-007, item 5a for MCMIS inputs, where the data will be deleted after the information is converted or copied to the MCMIS master data files, backed up, and verified.

FMCSA retains ELD records for comparison of records obtained at roadside with records received during compliance reviews, safety audits, and other investigations. This effort enhances the Agency's ability to identify any tampering with data or falsification of records.

FMCSA does not require ELDs to collect data on vehicle speed, braking action, steering function, or other vehicle performance parameters.

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 collects and uses data only to the extent necessary to meet its authorized business purpose and mission of the Agency. Disclosure of PII is limited to the purposes and uses specified in on the FMCSA website.

In order to perform HOS compliance-assurance and enforcement functions, the information collected on the ELD allows authorized safety officials to use personal information to positively identify the driver's name with his or her HOS records (date, time, duty status, location of changes in duty status). This is necessary to ensure that motor carriers operating in interstate commerce, and the motor carriers' drivers, comply with applicable HOS regulations. The data that ELDs collect electronically is analogous to the data collected manually via paper RODS, and it serves the same purpose. Other information collection requirements concerning the HOS record of duty status would not change, nor would information be contained in paper RODS.

In support of its safety mission, FMCSA is delegated broad authority to prescribe recordkeeping and reporting requirements (49 U.S.C. 31133(a)(8); 49 CFR 1.87(f)). However, in MAP-21, Congress restricted the way ELD data might be used. Specifically, the statute provides that the Agency "may utilize information contained in an electronic logging device only to enforce motor carrier safety and related regulations, including record-of-duty status regulations" (49 U.S.C. 31137(e)(1)). Furthermore, appropriate measures must be instituted "to ensure any information collected by electronic logging devices is used by enforcement personnel only for the purpose of determining compliance with hours of service requirements" (49 U.S.C. 31137(e)(3)). As explained in the accompanying conference committee report, Congress intended that such data "be used only to enforce federal regulations" (H. Rep. No. 112-557, at 607 (2012)).

Accordingly, FMCSA may retain ELD record to support research relating to HOS compliance and highway safety. FMCSA would retain the data until the completion of the research study. Collection of PII for research projects would be necessary to link to relevant data from other FMCSA systems. Once the relevant data were linked and analysis complete, FMCSA would de-identify the research dataset.

FMCSA does not place a limit on the motor carrier's use of the ELD records, provided that the records are maintained to protect drivers' privacy in a manner consistent with sound business practices.

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).

FMCSA ensures that the collection, use, and maintenance of PII for maintaining the ELD system is relevant to the purposes for which the data is to be used and, to the extent necessary for those purposes, it is accurate, complete, and up-to-date. Among these processes are the structured management of records authorship, reviews by drivers and motor carriers, automatic capturing of certain ELD inputs, and self-monitoring of system health by ELDs.

The ELD drivers review their records of duty status daily and certify their correctness prior to submission to the motor carriers and FMCSA. If a driver notices that information is missing or contains errors, the driver would use the ELD functions to make the necessary corrections or enter missing information.

After a driver submits his or her certified daily records to the motor carrier, the motor carrier reviews those records. If the carrier identifies additional errors, the carrier may request the driver to make additional edits. However, motor carriers or dispatchers that propose a change a drivers' HOS records following submission to the carrier are to have the driver re-certify the accuracy of the record. All edits must be annotated to document the reason for the change. This procedure is intended to protect the integrity of the ELD records and to prevent related instances of potential driver harassment.

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 incorporates standards and practices required for Federal information systems under the Federal Information System Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and NIST Special Publication (SP) 800-53 Rev. 4, and Recommended Security Controls for Federal Information Systems and Organizations, dated April 2013. 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 ELD system was deployed. These safeguards are designed to achieve the following objectives:

- Ensures 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 ELD system 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 ELD system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. All records that are stored in the ELD system will be protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the ELD system is logged and monitored.

The ELD system maintains an auditing function that tracks all user activities in relation to data, including access and modification. Through technical controls including firewalls, intrusion detection, encryption, access control lists, and other security methods, FMCSA prevents unauthorized access to data stored in the ELD system. These controls meet federally mandated information assurance and privacy requirements.

All FMCSA personnel and FMCSA contractors completes security and privacy awareness training and role-based training offered by DOT/FMCSA. This allows individuals with varying roles to understand and retain knowledge of how to properly and securely act in situations where they may use PII while performing their duties. No access is allowed to the ELD system prior to receiving the necessary clearances and security and privacy training as required by DOT/FMCSA.

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 ELD system. In addition to

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

Responsible Official

Bill Mahorney
Division Chief, Enforcement Division

Prepared by: Pam Gosier-Cox (Privacy Officer)

Approval and Signature

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