U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)
Electronic Logging Devices

Final Rule

Responsible Official

Michael Huntley
Vehicle and Roadside Operations Division
Federal Motor Carrier Safety Administration
202-366-4325
mcpsv@dot.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
DN: c=US, o=U.S. Government, ou=DOT Headquarters, ou=OSTHQ, cn=CLAIRE W BARRETT
Date: 2015.12.16 08:17:08 -05'00'

Claire W. Barrett
DOT Chief Privacy & Information Asset Officer

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 (MAP-21)) is publishing a rule that requires use of electronic logging devices (ELDs)[1] 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.[2] The information associated with the ELD records would include personally identifiable information (PII). This Privacy Impact Assessment (PIA) is necessary to provide information regarding the program, the necessity to collect PII, and the fulfillment of specific privacy requirements in MAP-21. This Privacy Impact Analysis is placed in the public docket for the rulemaking and on the Department's privacy Web site at www.dot.gov/privacy.

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.[3]

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:

[1] The term "electronic logging device" (ELD) is used in Section 32301(b) of MAP-21. See 49 U.S.C. 31137. FMCSA's rulemaking actions, as well as notices announcing certain Motor Carrier Safety Advisory Committee (MCSAC) meetings and public listening sessions, referred to the devices and support systems used to electronically record HOS RODS as "electronic on-board recorders (EOBRs)." In order to be consistent with the MAP-21 language, FMCSA uses the term "electronic logging device (ELD)."

[2] The Agency provides narrow exceptions for those CMV drivers required to keep RODS not more than 8 days in any 30- day period, drivers involved in driveaway-towaway operations if the vehicle driven is part of the shipment, and drivers operating vehicles manufactured before model year 2000. Motor carriers would have the option of continuing to require these drivers to keep paper RODS.

[3]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 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

Overview: Hours of Service Regulation

FMCSA's primary mission is to reduce crashes, injuries, and fatalities involving large trucks and buses. The Agency does this in several ways: we develop and enforce data-driven regulations that balance motor carrier safety with industry efficiency; we use Federal and State safety information systems to focus on high-risk carriers and drivers to enforce safety regulations; we develop and provide educational messages to carriers, CMV drivers, and the public; and we work with stakeholders (e.g., Federal, State, and local enforcement agencies; the motor carrier industry; safety groups; and organized labor) to reduce bus- and truck-related crashes.

FMCSA's HOS regulations are one of the cornerstones of CMV safety. The Federal Motor Carrier Safety Regulations (FMCSRs) require motor carriers to require their drivers to record driving time, other on- duty time, off-duty time, and related information on their HOS on a RODS, and for drivers to do so. Motor carriers – and FMCSA – use these records to document motor carriers' and drivers' HOS compliance.

The HOS regulations are designed to ensure that driving time does not impair the ability of CMV operators to operate the vehicles safely. HOS recording devices that are properly designed, used, and maintained enable motor carriers to track their drivers' on-duty driving hours accurately and automatically, and facilitate the electronic recording of drivers' other duty statuses (on-duty not driving, off-duty, and sleeper berth) to detect and deter HOS regulatory violations.

FMCSA and its predecessor agencies have always required PII in the HOS submission because of the need to identify the CMV driver in HOS records (whether generated in hardcopy or electronic form). The 2012 transportation legislation, MAP-21, explicitly requires the Agency to put in place appropriate measures to preserve the confidentiality of personal data recorded by an ELD that is disclosed in the course of an FMCSRs enforcement proceeding (49 U.S.C. 31137(e)(2)). To protect data of a personal nature unrelated to business operations, the Agency would redact such information included as part of the administrative record before a document would be made available in the public docket.

Use of HOS Data and Information

FMCSA's automatic on-board recording device (AOBRD) regulations (defined at 49 CFR 395.2, performance requirements at 49 CFR 395.15) cover a motor carrier's authority to require use of AOBRDs; information requirements; the duty status and additional information that must be recorded; and the manner of recording change of duty status location. Driving information – distance traveled, time, and speed – is recorded from a source or sources on the vehicle (such as the engine control module, or the transmission tail shaft on older vehicles). Only the driver is permitted to enter other information. Drivers are required to note any failures in the performance of the device and to reconstruct records of their duty on blank RODS forms. For the benefit of both drivers and safety officials, especially law enforcement officers performing roadside inspections who see many types of devices, FMCSA requires that drivers have an instruction sheet describing the operation of the AOBRD in the vehicle.

Performance requirements for AOBRDs are straightforward. The provider must test the design of the device and certify that the testing has taken place, that it demonstrated the device met the requirements of the regulations, and that it performed under the operating conditions the users (drivers, internal auditors, etc.) would encounter. The design must permit duty status to be updated only when the vehicle is at rest, unless the driver is registering the crossing of a State boundary. The AOBRD and support systems must be tamperproof to the maximum extent practicable. The AOBRD must provide a visual or audible warning to the driver if it ceases to function, and any sensor failures and edited data must be identified in the RODS printed from the device. Finally, the AOBRD must be maintained and recalibrated according to the provider's specifications; drivers must be adequately trained in the proper operation of the device; and the motor carrier must maintain a second (backup) copy of electronic HOS files in a separate location.

Although FMCSA and its State partners review the HOS records generated by AOBRDs during roadside inspections, safety audits, and other reviews, FMCSA does not maintain information in electronic form from these devices or their support systems. However, under the ELD rule, when citable HOS violations are found during inspections, the information associated with the ELD records would be collected during inspections, uploaded as an attachment to the inspection report, and maintained by FMCSA.

The Appendix to this PIA contains a brief regulatory history of HOS recording devices covering the period from the 1980s through 2011. A copy of the Supplemental Notice of Proposed Rulemaking (SNPRM), 79 FR 17656 (March 28, 2014) is available in the public docket.

ELD Rule: Overview

Section 32301(b) of the Commercial Motor Vehicle Safety Enhancement Act, enacted as part of MAP-21 (Pub. L. 112-141, 126 Stat. 405, 786-788 (July 6, 2012)), mandated that the Secretary adopt regulations requiring that CMVs involved in interstate commerce, operated by drivers who are required to keep RODS, be equipped with ELDs.[4] The statute sets out provisions that the regulations must address including device performance and

[4] The term "AOBRD" defines the HOS recording device that was the subject of the 1988 rule. See 49 CFR 395.2 (definition of "automatic on-board recording device") and 395.15. The term "EOBR" was used to describe the

design standards and certification requirements. In adopting regulations, the Agency must consider how the need for supporting documents might be reduced, to the extent data is captured on an ELD, without diminishing HOS enforcement. The statute also addresses privacy protection and use of data. In addition, like the Truck and Bus Safety and Regulatory Reform Act, the amendments in MAP-21, section 32301(b), require the regulations to "ensur[e] that an electronic logging device is not used to harass a vehicle operator." Finally, MAP-21 amended the Motor Carrier Act of 1984 to add new 49 U.S.C. 31136(a)(5), requiring that FMCSA regulations adopted under specified statutes address coercion of drivers.

The ELD rule will improve CMV safety and reduce the overall paperwork burden for both motor carriers and drivers by increasing the use of ELDs within the motor carrier industry, which will in turn improve compliance with the applicable HOS rules. Specifically, the ELD rule: (1) prescribes new technical specifications for ELDs that address statutory requirements contained in MAP-21; (2) mandates ELDs for drivers currently using RODS; (3) clarifies supporting document requirements so that motor carriers and drivers can comply efficiently with HOS regulations, and so that motor carriers can make the best use of ELDs and related support systems as their primary means of recording HOS information and ensuring HOS compliance; and (4) prescribes both procedural and technical provisions aimed at ensuring that ELDs are not used to harass vehicle operators.

Motor carriers are required to install and use ELDs compliant with the rule's requirements no later than 2 years after the publication date of the rule. However, motor carriers using on-board HOS recording technologies meeting or exceeding the AOBRD requirements under 49 CFR 395.15 and voluntarily installed in CMVs before the compliance date of the ELD rule may continue to use those technologies until a date 4 years after the publication date of the rule. The Agency estimates that 3,365,000 CMV drivers will be subject to rule's requirements, representing approximately 60% of the 5.6 million CMV drivers that operate in the U.S.—will be subject to the rule's requirements. Many of these drivers work for motor carriers that have voluntarily adopted the use of ELD-type devices.

ELD Functions

FMCSA proposes performance-based technical specifications to accommodate evolving technology and standards, allow for inexpensive adoption of the technical specifications, and afford ELD providers maximum flexibility to offer compliant products that are innovative and meet the needs of drivers and motor carriers. However, FMCSA does prescribe specific standard data formats and outputs that ELD providers would need to use to transfer, initialize, or upload data between systems or to authorized safety officials.

The rule defines and describes the ELD as a recording-only technology with the ability to transfer data to authorized safety officials. The rule does not require the ELD itself to analyze or review driver's RODS data for any purpose, including compliance. Nor does it require the device to provide 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-

HOS recording device and related technology in the 2007-2010 rulemaking actions that led to an April 2010 final rule, now vacated. The term "ELD," also describing HOS recording devices and technologies, appears in the MAP-21 legislation and was used in the SNPRM and final rule, consistent with the term used in the statute.

driving time). However, the rule does not prohibit ELD providers or carriers from offering or using an ELD that provides this type of signal.

Access to the ELD by a driver (and other users, including dispatchers and supervisors) requires a unique authenticated account with unique login identification. This provides critical information for the audit trail for ELD records, discussed in more detail later in this document. The unique identification would include 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 will 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.

Tracking of Vehicle Location

Many motor carriers use Fleet Management Systems (FMS),[5] which often include HOS recording and reporting functions, as well as additional recording capabilities and real-time communication features. Motor carriers use this technology to know where their CMVs are at all times and how much time their drivers may continue to operate in compliance with the HOS regulations. However, some drivers view the FMS as a way for motor carriers to harass drivers or to intrude upon their privacy.

Location recording is a critical component of HOS enforcement. It is needed to review driving time and to enable enforcement officials to correlate information on documents related to non-driving duty statuses. Drivers have always had to record certain location information on paper RODS. Although electronic recording is more accurate, the acquisition of location information for CMV operators is not a novel requirement.

The rule requires automatic recording of location information, using conventional geographic positioning standards (latitude-longitude coordinates). In addition, some of the tamper- resistance measures (physical and software) would use location information in computations to check the consistency of recorded information.

FMCSA does not require real-time tracking of CMVs or the recording of precise location information. Instead, location data must be recorded when the driver changes duty status, when a driver indicates personal use or yard moves, when the CMV engine powers up and shuts down, and at 60-minute intervals when the vehicle is in motion. During on-duty driving periods, FMCSA limits the location accuracy for HOS enforcement to coordinates of two decimal places, providing an accuracy of approximately a 1-mile radius for purposes of HOS enforcement. However, when a CMV is operated for personal use, the position reporting accuracy is

[5] The reference to a FMS is a generic term for systems that provide a comprehensive suite of vehicle monitoring functions. These may include fuel usage, idling time, speed, and vehicle location. They often include an HOS recording function. FMCSA does not require the use of comprehensive FMS.

further reduced to approximately a 10-mile radius. Thus, the Agency does not require that an ELD determine or record a CMV's or driver's exact location. Moreover, the Agency does not require that the ELD record and transmit any CMV location data in real time, either to the motor carrier or to enforcement officials.[6]

Because presentation of only latitude and longitude coordinate information would not provide an adequate description of location for use by drivers or enforcement officials, FMCSA requires ELDs to report geographic location ("geo-location") information. The Agency incorporates by reference American National Standards Institute (ANSI) INCITS 446-2008, which includes the "USGS GNIS, where Feature Class = Populated Place" list. This is the standard list of populated places containing their latitude-longitude coordinates. FMCSA uses this list to provide for standard conversion and reporting of geographic coordinates into recognizable location names. FMCSA includes only those places with 5,000 or more population. For example, instead of referring to a location according to its latitude and longitude coordinates, an ELD will report "10 miles north of Colorado Springs, CO."

The rule does not require the ELD dataset exchanged with authorized safety officials to include "place name." Instead, latitude and longitude coordinates are recorded and transmitted to those officials at roadside, where software would translate the coordinates into a named place and, as necessary, the distance and direction offset from the named place. This reduces the memory requirements for an ELD because the look-up table for geographic locations is considerably smaller. An ELD would still need to be able to present location information in clear and unambiguous terms to the driver and motor carriers to allow them to review and certify records.

Time Intervals for the ELD to record the required dataset. FMCSA requires the ELD to record HOS data that is included in the RODS (date, time, driver name, duty status, etc.), including geographic information as described above, at 60-minute intervals when the vehicle is in motion, at the time of any duty status change the driver inputs, and when a CMV's engine is powered up or shut down. If a motor carrier has allowed drivers to use a CMV for personal conveyance or yard moves, a driver's indication of the start and end of such occurrences will also use codes to indicate special statuses when the CMV is moving but the driver is not in an on-duty-driving status (yard moves are "on-duty-not-driving" and personal conveyance is "off-duty").

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 will use this identifier to mark the record as incomplete and in need of amendment. The carrier will need 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).

[6] Location codes may be obtained from satellite or land-based sources, or a combination of them. The rule requires the monitoring of engine hours and odometer readings in addition to automatic recording of location information. This is necessary; otherwise, interruptions to GPS or other location services could prevent the ELD from detecting CMV movement.

Duty status categories. Because FMCSA will continue to allow use of paper RODS in certain operations and temporarily during ELD malfunctions, it uses the same four duty status categories that are used for paper RODS: driving, on-duty not driving, off duty, and sleeper berth. However, there are situations where it is necessary to annotate or otherwise flag periods where the CMV is moving as a status other than "on-duty driving," including various covered exceptions under 49 CFR 395.1. An ELD must provide the capability for a driver to indicate the beginning and end of two specific categories, namely, personal use of a CMV and yard moves, as allowed by the motor carrier, where the CMV may be in motion but a driver is not necessarily in a "driving" duty status. This will record the necessary information in a consistent manner for the use of drivers, motor carriers, and authorized safety officials.

Personal conveyance. If a CMV is used for personal conveyance, and the driver uses the ELD to electronically indicate the beginning of the event, the ELD would not record that time as on-duty driving. The rule provides for selection of a special driving category when a CMV is being driven, but the time is not recorded as on-duty driving. FMCSA does not define a specific threshold of distance or time traveled for a driver to be able to use the personal use provision. Authorized motor carrier safety personnel and authorized safety officials will use the ELD data to further explore and determine whether the indicated special driving category (i.e. personal conveyance and yard moves) was appropriately used by the driver.

Collection of Personally Identifiable Information (PII)

The following information will be 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.

- 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 would carry 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 for the 24-hour period and total hours, 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-hostler repositioning the CMV)*
- 17-digit vehicle identification number (VIN)*

Additional data is recorded on the ELD, including engine hours, vehicle miles traveled, and motor carrier identification data (motor carrier name and FMCSA-issued USDOT number).

Driver or authenticated user identification data. The rule requires a unique identification of the driver on the ELD. As has been the case with AOBRDs, drivers using ELDs will need to log in so their duty status records can be linked to them. FMCSA also requires that motor carriers actively manage ELD accounts in order to ensure that only properly authenticated individuals have appropriate access rights. For example, a driver would have access rights only to his or her own account, but a supervisor would have access to many drivers' accounts.

FMCSA requires the following information for a driver "user account": the driver's first and last name, as reflected on the driver's license; a unique ELD username selected by the motor carrier; the driver's valid driver's license number; and the State or jurisdiction that issued the driver's license. A driver's license number or Social Security number may not be used as, or as part of, the username for the ELD account. FMCSA will not collect a driver's PIN, password, or other information needed to access the information associated with the ELD records contained on the ELD.

Enforcement Procedures: Transmission of Data. FMCSA has developed several software tools to facilitate the processes of conducting safety inspections at roadside and on-site compliance reviews at motor carriers' business offices. However, all of these tools require manual entry of data.

Safety officials must review two sets of records to determine HOS compliance, as they do today. The first data set is provided via paper RODs, AOBRD records, or other electronic records (such as from an FMS) and includes entries of duty status, dates, times, locations, and distance traveled. The second set of records consists of "supporting documents" that provide additional support to the information available in the first record set. For example, if a driver recorded 2 hours of ODND at a receiver's location, there should be supporting documentation identifying the shipper, the location, the cargo and how it was packaged (individual cartons, pallets of cartons, etc.). However, the ELD rule is the first time FMCSA has required drivers to share supporting documents in their possession with authorized safety officials during roadside inspections.

To facilitate a transition to automated review of HOS records, FMCSA requires that ELDs (as well as their support systems, if used) to produce output records in specified formats. The Agency is developing new software tools, which would allow authorized safety officials to assess electronic ELD files rapidly and accurately at roadside and during on-site reviews to determine whether the driver is in compliance with the HOS regulations. The software would retrieve data recorded by ELDs, analyze it, and identify instances of potential non-compliance. The safety official would use 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 order for a serious violation.[7] The "Security" section of this document describes the use of

[7] FMCSA is not including a detailed discussion of software systems it will develop, such as eRODS, in the PIA because the software development is still in progress and cannot be completed until the Agency has decided on

communications methods for transferring information recorded on the ELD (and support system, if used) to Federal, State, and local safety officials' portable computers so that the ELD information can be reviewed for HOS compliance. If citable HOS violations are found, information specific to those violations would be transmitted to FMCSA.

ELD Specifications To Protect Against Harassment. In accordance with 49 U.S.C. 31137(a)(2), FMCSA prescribes both procedural and technical provisions aimed at protecting CMV operators from harassment involving ELDs or connected technology. The Agency addresses the problems of: (1) drivers being required to exceed HOS limitations (addressed by the harassment complaint process); and (2) inappropriate communications that affect drivers' rest periods (addressed through ELD technical specifications). The Agency addresses the related but distinct issue of driver coercion in another recent rulemaking (80 FR 78292, December 16, 2015).

In prescribing regulations on the use of ELDs, the Agency is required by statute to ensure that ELDs are "not used to harass a vehicle operator" (49 U.S.C. 31137(a)(2)). The Agency prescribes both procedural and technical provisions to protect drivers of CMVs from harassment resulting from information generated by ELDs. As voiced during public listening sessions and addressed in comment submissions, drivers' primary harassment-related complaints focused on pressures from motor carriers to break the HOS rules. Not every type of complaint suggested a technical solution. However, in the rule's technical specifications, the Agency includes several technical requirements aimed, among other things, at protecting the driver from harassment. For example, the Agency recognizes that some motor carriers will use technology or devices that include both an ELD function and communications function. To protect a driver using such a device from unwelcome communications during rest periods, the rule requires that, if a driver indicates sleeper berth status, either the device must allow the driver to mute or turn down the volume on the communication feature or turn off this feature, or the device must do one of these things automatically. (This option is unavailable if a co-driver is operating the vehicle.)

To protect the driver's data, the rule proposes to require that any changes made by a motor carrier would require the driver's approval. Furthermore, the rule proposes to ensure that a driver has a right to access the driver's ELD data during the 6-month period a carrier must keep such records.[8] Access to these records will help a driver protect him or herself against harassment.

In developing the technical performance requirements, the Agency has taken into account drivers' privacy interests. As explained above, FMCSA would not require vehicle location information to be recorded at the level of precision that could identify street addresses. Further, detailed location information would be required to be recorded only at discrete instances, such as when a driver changes duty status or at 60-minute intervals

---

the final technical requirements for ELD output data. A separate privacy analysis and, if appropriate, public PIA will be developed prior to such tools being implemented in an operational environment.

[8] If a driver's records are available through an ELD, the driver need not request them through the carrier. However, if the records were no longer available through the ELD, a motor carrier would need to provide the driver with access to and copies of the driver's records, on request.

when the vehicle is in motion. FMCSA believes these features also would help ensure that driver harassment does not arise from the use of ELDs.

Although the statute provides that regulations relating to ELDs shall "ensur[e] that an electronic logging device is not used to harass a vehicle operator," the Agency notes that it cannot adopt a regulation guaranteeing that every instance and form of harassment, whether real or perceived, is eliminated. Nor does the Agency believe that Congress intended that the Agency interfere with labor/management agreements or disputes not directly related to the required use of ELDs, or duplicate the role Congress has assigned to the U.S. Department of Labor under 49 U.S.C. 31105.

In addition, as explained in the rule's preamble, FMCSA does not require an ELD to provide functionality beyond basic recording of the data elements required for HOS compliance assurance. However, the Agency would not prohibit motor carriers from using communication technologies, an FMS, and other functions beyond mere recording. Many current systems, which have been on the market for years, go beyond the recording abilities in the ELD rule. The Agency does not believe that the anti- harassment provision in section 31137(a)(2) meant that Congress expects FMCSA to ban or impose significant new restrictions on those functions in this rulemaking. However, to address driver complaints on interruptions during sleeper berth periods, FMCSA addresses the use of technology beyond the minimally compliant ELD – but only if that technology included an ELD function.

Explicit Prohibition on Harassment

FMCSA adds a new § 390.36 to prohibit a motor carrier from engaging in harassment of a driver. As defined, "harass or harassment" would mean "an action by a motor carrier towards a driver employed by the motor carrier (including an independent contractor while in the course of operating a [CMV] on behalf of the motor carrier) involving the use of information available through an ELD … or through other technology used in combination with and not separate from the ELD, that the motor carrier knew, or should have known, would result in the driver violating § 392.3 or part 395 [of 49 CFR]."[9] This definition recognizes that pressure imposed by a motor carrier on a driver that results in an HOS violation or in a driver operating when the driver's alertness is impaired through fatigue or illness can result in dire safety consequences.

[9] 49 CFR 392.3, Ill or fatigued operator. No driver shall operate a commercial motor vehicle, and a motor carrier shall not require or permit a driver to operate a commercial motor vehicle, while the driver's ability or alertness is so impaired, or so likely to become impaired, through fatigue, illness, or any other cause, as to make it unsafe for him/her to begin or continue to operate the commercial motor vehicle. However, in a case of grave emergency where the hazard to occupants of the commercial motor vehicle or other users of the highway would be increased by compliance with this section, the driver may continue to operate the commercial motor vehicle to the nearest place at which that hazard is removed.

Under the rule, a driver who believes that a motor carrier required him or her to violate§ 392.3 or part 395 in a manner described in the definition could file a complaint alleging harassment with FMCSA in accordance with procedures prescribed in the rule.[10]

Although FMCSA's definition of harassment does not require adverse action by the carrier against the driver, it does require an actual violation of § 392.3 or part 395 of the FMCSRs. MAP-21 eliminated the reference to productivity in 49 U.S.C. 31137; however, the Agency would not penalize motor carrier actions aimed at productivity, provided that the action did not constitute harassment as defined in the rule.

Complaint Procedures

The ELD rule adds a new process for drivers to use to file a complaint of harassment. Among other things, the driver must describe in the complaint the action by the motor carrier that the driver deems harassment, including how the ELD or related technology was used to contribute to the carrier's action. The complaint would also need to identify how the motor carrier's action resulted in a violation of 49 CFR 392.3 or part 395.

The rule give drivers control over their own ELD records and ensures driver access to the information in such records. Furthermore, drivers will be able to annotate their records reflecting concerns such as driver fatigue. These records would provide drivers with better information to substantiate any complaint.

Enhanced Penalties To Deter Harassment

A motor carrier that engages in harassment is subject to civil penalties under part 386 of 49 CFR. Because harassment would be considered in cases of alleged HOS violations, the penalty for harassment supplements the underlying HOS violations of 49 CFR 392.3 and part 395. An underlying violation would have to be found for a penalty for harassment to be assessed.

If after investigation of a harassment complaint, an FMCSA Division Administrator determines that a violation has occurred, the FMCSA Division Administrator may issue the motor carrier a Notice of Violation alleging that a violation has occurred and requiring the carrier take corrective action, or a Notice of Claim to levy a civil penalty against the carrier, or other authorized action. In addition to the rule's procedural protections, the rule's technical specifications for the ELD are specifically designed to provide drivers additional protection. By recording the time spent behind the wheel of a CMV accurately, all parties involved can easily be made aware of the actual time for a driver to make a certain trip. FMCSA believes this increased transparency will lead to reduced pressure on drivers to falsify their RODS. ELDs provide a more reliable and simpler tool for recording drivers' HOS than paper RODS. FMCSA believes the use of ELDs would lead, not only to better compliance with HOS regulations, but also to a clearer understanding of driver schedules.

[10] Drivers currently can file an informal complaint on any violation of the FMCSRs with FMCSA's National Consumer Complaint Database help desk. This option would not change.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template based on the fair information pratice 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 FIPPsd 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[11]*, 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*[12].

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.

This PIA fully describes the nature and type of PII to be collected and used pursuant to the Motor Carrier Act of 1935 (Pub. L. 74-255, 49 Stat. 543, August 9, 1935, codified at 49 U.S.C. 31502(b)), as well as the 1984 Motor Carrier Act, the 1988 Truck and Bus Safety and Regulatory Reform Act, and MAP-21.

The ELD rule makes ELDs mandatory for most drivers currently required to use paper RODS. Although the specific processes FMCSA would use to gather information from ELDs would be different from those used to gather information from paper RODS, the necessity of gathering the information, the need to review it, and the need to determine the necessity of taking enforcement actions would not fundamentally change.

The rule is designed to allow drivers to maintain a level of control over their RODS. A driver will know, based on the type of operation being conducted, if the driver needs an ELD to prepare and maintain RODS. The ELD will be readily visible to the driver, because the driver must interact with it to log in, to enter duty status information (on-duty-not driving, off-duty, sleeper berth) as well as remarks related to duty status information. A driver is required to certify his or her RODS on the ELD at the end of each duty day. Additionally, the driver is required to submit RODS to the motor on a regular basis. During a roadside inspection, an authorized safety official may request the driver's RODS recorded on and available via the ELD, and the driver will need to affirmatively act to give the authorized safety official access to his or her RODS. In an inspection or audit conducted at a motor carrier's place of business, the motor carrier will only be able to provide those RODS that have been submitted and certified by a driver (this is the same way that information from drivers' paper RODS is handled).

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

In order to better address privacy and harassment, FMCSA held public listening sessions, and tasked the Motor Carrier Safety Advisory Committee (MCSAC) to develop a report on the topic of harassment. This report, MCSAC Task 12-01: Measures to Ensure Electronic On-Board Recorders (EOBRs) Are Not Used to Harass Commercial Motor Vehicle (CMV) Drivers, is available at http://mcsac.fmcsa.dot.gov/Reports.htm.

FMCSA maintains several information systems to perform its motor carrier safety oversight activities. The Motor Carrier Management Information System (MCMIS) contains motor carrier demographic and other "census" information, as well as inspection results. ELD data collected as part of an inspection or enforcement activity may be stored in MCMIS, which is a system of records subject to the Privacy Act. The amended MCMIS system of records notice was published in the Federal Register on September 25, 2013 (DOT/FMCSA 001—Motor Carrier Management Information System, FR 2013-23131). The MCMIS SORN will be updated to reflect the ELD rule. In addition, the MCMIS PIA is published on the DOT Web site at http://www.dot.gov/individuals/privacy/pia-motor-carrier- management-information-system.

The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency into FMCSA's ELD rulemaking.

Individual Participation and Redress

DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

The ELD rule requires most CMV drivers who operate CMVs in interstate commerce and who are required to keep RODS to record their HOS information to use an ELD. Motor carriers are to actively manage ELD user accounts and ensure that properly authenticated individuals have ELDs with appropriately assigned rights to access, and 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 6 months that the carrier must retain it. While the motor carrier may suggest changes to the RODS, in order to protect the driver and the integrity of the record, the driver must re-certify the record after making any edits.

FMCSA continues to ensure that individuals have the right to (a) obtain confirmation of whether FMCSA has PII relating to them; (b) access the PII related to them in a reasonable time, cost, and manner and in a form that is readily intelligible to them; (c) an explanation if a request made under (a) and (b) is denied and be able to challenge such denial; and (d) challenge PII relating to them and, if the challenge is successful, have the data erased, rectified, completed, or amended.

FMCSA has 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/login.asp. 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.

The DataQs PIA published on XX DATE 2015, and is available on the DOT Privacy Web site at http://www.dot.gov/privacy.

Statutory Authority and 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 its collects, uses, maintains, or disseminates PII.

The authority for the ELD rulemaking 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 rule.

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 rules.

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. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The only PII FMCSA requires ELDs to collect is that which is necessary to determine interstate CMV driver and motor carrier compliance with HOS regulations (date, time, location, sequences of duty status; driver and vehicle identification; time, date, identity of persons making original data entries and annotations to data; quality-control flags on availability of location information). Although FMCSA considered using the driver's name and a partial driver's license number instead of the full number, this would not lower the security requirements the Agency must establish for handling of the data. In addition, use of a partial driver's license number would not be practical because States use different methods to assign drivers' license numbers. Therefore, the Agency determined that including the entire driver's license number and driver's license issuing State would be necessary to ensure a unique identification of each driver and to attain a sufficient level of tamper resistance for the ELDs by preventing the potential creation of multiple aliases for a single driver within a motor carrier.

FMCSA requires automatic recording of CMV location information only to a limited accuracy (within an approximate 1-mile radius while driver is on-duty driving and approximate 10-mile radius during personal use) and to reference a nearby city, town, or village, or the compass direction and distance from the nearest city, town, or village. The ELD SNPRM requires recording of the CMV's location at each change of duty status and once every 60 minutes while a CMV is in motion and the driver is in an on-duty-driving status, to allow authorized safety officials to determine the driver's HOS compliance.

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

The collection of the information associated with the ELD records by FMCSA would enable the comparison of records obtained at roadside with records received during compliance reviews and other investigations. This effort would enhance the Agency's ability to identify any tampering with data or falsification of records.

FMCSA will retain the information associated with the ELD records only if citable HOS violations are found during an inspection. In accordance with the FMCSA's Electronic Document Management System record schedule Job Number N1-557-05-7, the information associated with the ELD records containing PII and transmitted to FMCSA would be destroyed or deleted when no longer needed for enforcement proceedings. Motor carriers must retain records for 6 months from date of receipt.

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 FMCSA minimizes its data collection to that necessary to meet the authorized business purpose and mission of the Agency. In order to perform HOS compliance-assurance and enforcement functions, the information collected in support of the implementation of the ELD rule 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 rules. The data that ELDs would 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 contained in paper RODS.

In support of its safety mission, FMCSA has been 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)). For further discussion on the effect of the MAP-21 provision, see the preamble of the ELD rule.

FMCSA does not place a limit on the motor carrier's use of the ELD records, provided that the records are maintained so as 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 requires PII in ELD data to clearly and uniquely identify the records of individual CMV drivers. This is consistent with the existing requirement for FMCSRs, which applies, regardless of the type of HOS records (RODS or timecards) a motor carrier uses and whether the records are prepared and maintained in hardcopy or electronic form. The rule requires use of specific processes and technology standards to ensure that PII collected, used, and maintained is relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, that it is accurate, complete, and current. 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.

Review, Correction, and Certification of the Information Associated with the ELD Records

The ELD rule requires drivers to review their records of duty status daily and certify their correctness prior to submission to the motor carriers. ELDs support a standard visual presentation format for the data so a driver could easily perform that review. 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. There is one exception: drivers may not reduce the amount of automatically recorded driving time.

Although the ELD allows a driver to edit records, the device will retain both the original and the amended records. Once the driver's edits are complete, the driver will certify or re-certify his or her daily records. As an example, consider a case where a driver parks the CMV with its engine running and goes off to have lunch; assume that the driver forgets to properly set the ELD's status to "off-duty" prior to going off duty. In this situation, the ELD would automatically switch the driver's status to "on duty not driving" after the CMV had been stationary for 6 minutes. The driver would later have the ability to change the duty status for time recorded as "on-duty not driving" to "off-duty," if that was the true and correct status for that driver. If a driver knowingly falsifies records, then the driver could be liable for civil penalties pursuant to 49 U.S.C. 521.

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 have to 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. An example of such a motor carrier edit request would be to revise a duty status designation from "off duty" to "on-duty not driving" such as in the case of coding training time for drivers. In this example the carrier would likely note, "Driver logged training time incorrectly as off duty." This edit and annotation would then be sent back to the driver for approval. A proposed edit would reflect its authorship; the ELD would require driver's approval or rejection of proposed motor carrier edits; and, the ELD would retain records of original, requested, approved, and rejected edits.

In summary, FMCSA believes that there are good reasons for both the motor carrier and the driver to be able to view HOS records and, under certain circumstances, to correct them. FMCSA also believes that the process will both provide an effective way to mark errors for correction, and to perform the correction in a way that enhances the transparency of the process between the driver and the motor carrier, and provides an audit trail for use by enforcement personnel.

Technology Standards Improving Data Quality and Integrity

The quality and integrity of the HOS data will be enhanced in two ways: (1) by the standards for ELD inputs, and (2) by the methods for an ELD to self-monitor and identify its own compliance malfunctions and data inconsistencies. There is no specific calibration requirement for ELDs because an ELD must have the capability to identify instances when it can no longer meet fundamental technical requirements. Motor carriers are responsible for proper installation and maintenance of the technology in accordance with the provider specifications to avoid system malfunctions.

An ELD automatically captures driving time without the need for a driver's input, even in cases when a driver has not logged into the system. An ELD also automatically captures location information associated with the ELD records (at least once every 60 minutes while the CMV is in motion and at each change of duty status). Additionally, an ELD is able to determine whether a location measurement is valid (sufficiently precise, based upon the availability of satellites or communication towers) for ELD recording purposes and only use valid measurements. This will improve the accuracy of driving time reporting. The ELD still requires a driver to provide manual inputs to the system, such as indicating the instance of each duty status change, as currently required under 49 CFR 395.8 and 395.15. Because the ELD would automatically capture the time and location of the CMV at each change of duty status, however, the accuracy and integrity of the records would be significantly improved.

The rule prescribes detailed data recording and data transfer protocols that will secure the ELD data in transit (from an ELD to an inspection official's portable computer, for example) and at rest (for example, while maintained within one of FMCSA's enforcement software systems). Among other things, "data recording" processes include "data integrity check" elements that enable quick identification of missing or manually altered records. Data transfer protocols each require security measures.

FMCSA believes that the performance standards in the appendix to subpart B of part 395 can be met in a number of different ways, whether the ELD application was a component of another system (such as a Fleet Management System) or if it were offered as a stand-alone technology. The rule requires ELD providers to certify their systems. However, FMCSA is developing a standard set of compliance test procedures that providers may use in their certification processes. FMCSA anticipates that industry standards for testing and certification of ELDs may emerge and evolve , standards may use or build upon the compliance test procedures FMCSA establishes. ELD providers are not required to follow FMCSA's compliance test procedures to certify compliance of their product. Their ELDs, however, would need to meet or exceed the performance requirements in the appendix to subpart B of part 395.

FMCSA stresses that it does not have statutory authority over system providers and does not propose any manufacturing oversight, blanket testing, or certification criteria. Allowing ELD providers flexibility to meet or exceed the performance requirements of these criteria is consistent with other DOT regulations and would be as effective as existing DOT regulations. That said, FMCSA may subject registered ELDs to FMCSA's compliance test procedures to independently verify their compliance.

The rule requires certified ELDs to be registered with FMCSA, and requires motor carriers to use only those ELDs listed on FMCSA's Web site. Through the registration process, FMCSA will maintain a list of certified

ELDs and inform motor carriers of all available options through a single resource. The rule also outlines a process under which an ELD model not meeting the rule's technical specifications can be removed from the list.

As outlined in this section, the rule establishes performance standards for ELDs including data quality and tamper-resistance measures. Implementation of this rule will improve the accuracy of interstate CMV drivers' HOS records. Interstate CMV drivers and their employing motor carriers continue to be responsible for the accuracy of the information not automatically identified by ELDs, as they would be if they were using handwritten RODS.

Because compliance with the HOS regulations is mandatory, the primary "benefit" to motor carriers and their drivers is their ability to legally operate CMVs in interstate commerce. Motor carriers also benefit from paperwork reductions and increased ability to more systematically assess and better comply with HOS regulations.

The redress process described in the Individual Participation and Redress section is a mechanism to maintain and improve accuracy of information.

Security

DOT shall implement administrative, technical, and physical measures 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 in transmission to, and when stored or processed on the ELD device.

According to best business practices, FMCSA requires data transferred to authorized safety officials to be secured, encrypted, or, in the case of a display or print-out, physically protected, reducing the likelihood of the unauthorized capture of ELD data. In order to physically protect the information that could be displayed, the official will need to protect his/her portable computer, not leave it lying about, and possibly use a screen shield. This requirement addresses the protection of personal data consistent with requirements of MAP-21, 49 U.S.C. 31137(e)(2).

MAP-21 requires that FMCSA "include such measures as [FMCSA] determines are necessary to protect the privacy of each individual whose personal data is contained in an [ELD]." The rule requires ELDs to implement user authentication and access control mechanisms, which limit access to data, including PII stored on the ELD, to only users with approved authorization. For a CMV driver subject to the regulations to log into an ELD, the driver needs to enter information (such as a user ID and password) into the ELD that uniquely identifies the driver. Alternatively, the CMV driver may use other means (such as a smart card or a biometric reader) that uniquely identifies the driver to the ELD.

FMCSA protects the ELD PII that is: (1) in transit to an FMCSA IT system and (2) stored on an FMCSA System that is not accessible to the public in accordance with applicable rules and policies, including all applicable FMCSA automated systems security and access policies. FMCSA has developed secure processes

for the transmission of the information associated with the ELD records, records control and repository, and the ability to retrieve and search records. The rule prescribes ELD data transfer protocols that include detailed security measures governed by industry and NIST standards. These apply to the transmission of roadside inspection data from an ELD (or an ELD support system) to the FMCSA and State IT systems.

It is worth noting, however, that by encrypting transmission of the information associated with the ELD records, FMCSA is making it considerably more difficult to capture information from a transmission and tie it to a specific individual. The transmission of data from the law enforcement official's portable computer to MCMIS takes place later (usually that same day), and the information is encrypted for transmission in accordance with NIST FIPS 140-2 standard. In the event of a citable HOS violation, the information associated with the electronic ELD record is uploaded to MCMIS as an attachment to the inspection report, and the paper record is scanned into FMCSA's EDMS.

Access to EDMS, which stores the information associated with the ELD records, is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate authorizations and permissions. EDMS and MCMIS are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the electronic system is logged and monitored. Access is automatically restricted by systems and policies with oversight conducted by the FMCSA Information Systems Security Manager and the MCMIS and EDMS System Owners.

Authorized DOT employees and contractors have password-protected access to the system to perform their official duties, including system administration, monitoring, security functions, as well as viewing and verifying the information. Access to the data is limited to authorized representatives of FMCSA or authorized Federal, State, or local enforcement agency representatives.

Government Personnel and contractors are required to attend security awareness and privacy training offered by DOT/FMCSA and role-based training. This 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 business information in the course of performing their duties. Access will be automatically restricted by systems and policies, with oversight conducted by the IT Security Officer and management level government personnel. No access will be allowed prior to receiving the necessary clearances and training as required by DOT/FMCSA.

The EDMS Authorization to Operation was granted on September 4, 2014 for a period of 3 years under the National Institute of Standards and Technology. The MCMIS Authorization to Operate was granted on September 4, 2014 for a period of 3 years under the National Institute of Standards and Technology.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FMCSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to FMCSA privacy and security policies and regulations. FMCSA will follow the Fair Information Practice

Principles as best practices for the protection of information associated with the ELD records held in MCMIS and EDMS in the event of a citable HOS violation. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees will be given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance will be provided in the form of mandatory annual Security and privacy awareness training as well as Acceptable Rules of Behavior. The FMCSA Security Officer and FMCSA Privacy Officer will conduct regular periodic security and privacy reviews of EDMS and MCMIS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Motor carriers will be responsible for specifying, procuring, and implementing ELD systems to comply with the regulations. Motor carriers need to do due-diligence when they select ELD suppliers. They will also need to provide training to drivers, dispatchers, supervisors, and other staff who need to access these systems. When they plan for implementing ELD systems, motor carriers will need to work with their ELD suppliers to provide the appropriate read, write, and edit rights to system users.

The motor carriers are required to obtain ELDs provided by providers that certify that their devices meet the standards of 49 CFR part 395, as listed on an FMCSA Web site. ELD providers must provide the instructions on how to use the ELD that must remain with the ELD inside the CMV. Motor carriers will be responsible for driver compliance with HOS regulations.

While many motor carriers are likely to have data privacy and security policies in place, others may need to develop them. They would also need to develop and implement procedures relating to protection, retention, and destruction of records.

FMCSA would not audit data from ELDs on a routine basis. Rather, the Agency would review carriers' compliance with FMCSR requirements for ELD systems as a part of compliance reviews.

Responsible Official

Michael Huntley
Vehicle and Roadside Operations Division
Federal Motor Carrier Safety Administration
202-366-4325 mcpsd@dot.gov

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer

APPENDIX: The Regulatory History of HOS Recording Devices

FMCSA and its predecessor agencies have had the authority to review drivers' and motor carriers' documents since the first HOS regulations were published in 1937. In the mid-1980s, motor carriers began to look to automated methods of recording drivers' duty status records as a way to save drivers' time and to improve the efficiency of the compliance-assurance procedures. In April 1985, the Federal Highway Administration (FHWA, the predecessor agency of FMCSA within the Department of Transportation) first allowed motor carriers to use AOBRDs under a pilot program. The FHWA issued the AOBRD Final Rule in September 1988. That rule established the first technical requirements for HOS recording devices.

An AOBRD is defined in the Federal Motor Carrier Safety Regulations as an "electric, electronic, electromechanical, or mechanical device capable of recording driver's duty status information accurately and automatically. The device must be integrally synchronized with specific operations of the commercial motor vehicle in which it is installed. At a minimum, the device must record engine use, road speed, miles driven, the date, and time of day."

The FMCSA conducted rulemaking to update the technical requirements for HOS recording devices, publishing an Advanced Notice of Proposed Rulemaking (ANPRM) on September 1, 2004 (69 FR 53386) and a Notice of Proposed Rule Making (NPRM) on January 18, 2007 (72 FR 2340). The Electronic On- Board Recorder (EOBR) final rule, (75 FR 17208, April 5, 2010), included a new performance-oriented technology standard and offered incentives to promote voluntary use of EOBRs. However, use of EOBRs would have been mandatory only for motor carriers found to be in serious non-compliance with HOS regulations.

An electronic on-board recording device (EOBR) was defined as "an electronic device that is capable of recording a driver's hours of service and duty status accurately and automatically and that meets the requirements of § 395.16. The device must be integrally synchronized with specific operations of the commercial motor vehicle in which it is installed. The EOBR must record, at minimum, the information listed in § 395.16(b)." The April 2010 rule required an EOBR to record the following information:

(1) Name of driver and any co-driver(s), and corresponding driver identification information (such as a user ID and password).
(2) Duty status.
(3) Date and time.
(4) Location of CMV.
(5) Distance traveled.
(6) Name and USDOT Number of motor carrier.
(7) 24-hour period starting time (e.g., midnight, 9 a.m., noon, 3 p.m.).
(8) The multiday basis (7 or 8 days) used by the motor carrier to compute cumulative duty hours and driving time.

(9) Hours in each duty status for the 24-hour period, and total hours. (10)Truck or tractor and trailer number.

(11) Shipping document number(s), or name of shipper and commodity.

On February 1 2011, FMCSA published a new NPRM on EOBR use (76 FR 5537). The NPRM had three components: (1) requiring EOBRs to be used by considerably more motor carriers and drivers than those covered by the previously published final rule; (2) codifying the requirement that motor carriers develop and maintain systematic HOS oversight of their drivers; and (3) clarifying supporting document requirements. The NPRM relied on the technical standards for device performance already promulgated in the April 2010 final rule.

In August 2011, the United States Court of Appeals for the Seventh Circuit vacated the April 2010 final rule, including the device performance standards. See Owner-Operator Independent Drivers Association v. Federal Motor Carrier Safety Administration, 656 F.3d 580 (7th Cir. 2011), available in the docket.

Component Reviewer	Name	Review Date

Business Owner		
General Counsel		
Information System Security Manager (ISSM)		
Privacy Officer*	Pam Gosier-Cox	6/11/2015
Records Officer		