U.S. DEPARTMENT OF TRANSPORTATION
Federal Motor Carrier Safety Administration

PRIVACY IMPACT ASSESSMENT

ELECTRONIC ON-BOARD RECORDERS (EOBRs) FOR HOURS-OF-SERVICE (HOS) COMPLIANCE

Rulemaking Contact Point
Deborah M. Freund
Vehicle and Roadside Operations Division,
Office of Bus and Truck Standards and Operations,
FMCSA
(202) 366-5370
Deborah.Freund@dot.gov

Reviewing Official
Pam Gosier-Cox,
FMCSA Office of Information Technology
(202) 366-3655
Pam.Gosier.Cox@dot.gov

November 6, 2009

TABLE OF CONTENTS

OVERVIEW OF FMCSA EOBR FINAL RULE

Introduction

The primary mission of the Federal Motor Carrier Safety Administration (FMCSA), U.S. Department of Transportation (DOT), is to reduce crashes, injuries, and fatalities involving large trucks and buses. This mission is accomplished by developing and enforcing data-driven regulations that balance motor carrier safety with industry efficiency; utilizing Federal and State safety information systems to focus on high-risk carriers and drivers to enforce safety regulations; targeting educational messages to carriers, commercial motor vehicle drivers, and the public; and partnering 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.

Statutory Authority

FMCSA and its predecessor agencies have had the authority to review drivers' and motor carriers' documents since the first hours-of-service (HOS) regulations were promulgated in 1937. Beginning with the Motor Carrier Act of 1935, Congress has recognized the Federal Government's interest in providing a higher level of safety oversight to commercial motor vehicle (CMV) drivers than to other motor vehicle drivers. CMV driver licensing, physical qualification assessments, training, driving performance, and performance of other safety-sensitive duties are subject to Federal regulation. These regulations also require documentation of all assessment results and compliance with CMV operation regulations, such as the Record of Duty Status (RODS) for documenting compliance with HOS regulations. Please refer to the preambles of the Notice of Proposed Rulemaking (72 FR 2340; January 18, 2007) and Final Rule (Insert FR when applicable) for a detailed discussion.

The HOS regulations are designed to ensure that driving time—one of the principal "responsibilities imposed on the operators of commercial motor vehicles"—does "not impair their ability to operate the vehicles safely." (49 U.S.C. 31136(a)). Personally identifiable information (PII) has always been collected by FMCSA and its predecessor agencies because of the need to identify the driver of the commercial motor vehicle in HOS records.

Electronic On-Board Recorders (EOBRs) that are properly designed, used, and maintained will enable motor carriers to track their drivers' on-duty driving hours accurately in order to prevent regulatory violations or excessive driver fatigue and to schedule vehicle and driver operations more efficiently. Driver compliance with the HOS rule helps ensure that "the physical condition of [commercial motor vehicle drivers] is adequate to enable them to operate the vehicles safely." (49 U.S.C. 31136(a)(3)) To assist FMCSA in its enforcement of HOS requirements, which in turn will improve commercial motor vehicle safety in general and highway safety in particular, FMCSA will require EOBR use by motor carriers with the most serious HOS compliance deficiencies ("threshold rate violations") as described in the EOBR final rule.

CURRENT DESCRIPTION OF AOBRDs

While the EOBR final rule requires certain motor carriers to collect electronic RODS, the Federal Highway Administration (FHWA, the agency responsible for motor carrier safety before January 2000), issued a final rule on September 30, 1988 (53 FR 38666), which revised part 395 of the Federal Motor Carrier Safety Regulations (FMCSRs) to allow, but not require, motor carriers to equip CMVs with Automatic On-Board Recording Devices (AOBRDs) instead of requiring drivers to complete a handwritten RODS (49 CFR 395.15). An AOBRD was defined under § 395.2 as "… an electric, electronic, electromechanical, or mechanical device capable of recording driver's duty status information accurately and automatically as required by § 395.15. 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."

Section 395.15(c) requires duty status and additional information to be recorded as follows:

(1) "Off duty" or "OFF" or by an identifiable code or character;

(2) "Sleeper berth" or "SB" or by an identifiable code or character (only if the sleeper berth is used);

(3) "Driving" or "D" or by an identifiable code or character;

(4) "On duty not driving" or "ON" or by an identifiable code or character;

(5) Date;

(6) Total miles driving today;

(7) Truck or tractor and trailer number;

(8) Name of carrier;

(9) Main office address;

(10) 24-hour period starting time (e.g., midnight, 9:00 a.m., noon, 3:00 p.m.);

(11) Name of co-driver;

(12) Total hours; and

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

During the course of roadside inspections and compliance reviews, FMCSA and State officials assess interstate CMV drivers' compliance with the HOS regulations using information from paper and electronic media, RODS, AOBRDs, EOBRs, and supporting documents. When these law enforcement and safety officials discover HOS violations, they document the violations and gather evidentiary material to support the charges. This evidentiary material consists of photographic and xerographic images of paper documents, screen shots of AOBRD displays, and hardcopy printouts. These images which contain PII are uploaded to FMCSA's Electronic Document Management System (EDMS). EDMS is a Privacy Act-protected System of Records.

OVERVIEW OF EOBR RULEMAKING

FMCSA is issuing a final rule ("Electronic On-Board Recorders for Hours-of-Service Compliance") establishing "safety of operation and equipment" of motor carriers and "standards of equipment" of motor private carriers. When effective, the final rule will allow all motor carriers to use EOBRs to document interstate CMV drivers' compliance with HOS requirements; will require noncompliant motor carriers to install, use, and maintain EOBRs; and will update existing performance standards for EOBRs.

This final rule helps FMCSA fulfill its mission to reduce crashes, injuries, and fatalities involving large trucks and buses by developing and enforcing data-driven regulations that balance motor carrier safety with industry efficiency and by utilizing Federal and State safety information systems to focus on high-risk carriers and drivers to enforce safety regulations. The final rule also allows for the continued collection of interstate CMV drivers' personally identifiable information, RODS, and other supporting documentation.

FMCSA has amended the FMCSRs to incorporate new performance standards for EOBRs. Only EOBRs that are compliant with these new standards shall be installed in CMVs manufactured beginning two years after the effective date of the final rule. EOBRs meeting FMCSA's current requirements and voluntarily installed in CMVs manufactured before the final rule's compliance date, two years and 60 days after the date of publication of the EOBR final rule in the Federal Register, may continue to be used for the remainder of the service life of the CMV. After the compliance date of the final rule, motor carriers that FMCSA determines to have demonstrated serious levels of HOS noncompliance will be subject to mandatory EOBR installation, regardless of the CMV's manufacture date. If FMCSA determines, based on the HOS records reviewed during a compliance review that a motor carrier has a 10 percent or greater HOS violation rate ("threshold rate violation") for any regulation in the new Appendix C to Part 385 of Title 49 of the Code of Federal Regulations, FMCSA will issue the carrier an EOBR remedial directive. The motor carrier shall then be required to install EOBRs in all of its CMVs and to use the EOBRs for 2 years unless:

(i) the carrier has already equipped its vehicles with AOBRDs meeting current requirements under 49 CFR 395.15 prior to the violation, and

(ii) the carrier demonstrates to FMCSA that its drivers understand how to, and do use the AOBRDs.

FMCSA has also changed the safety fitness standard to require carrier compliance with any applicable remedial directive.

FMCSA encourages industry-wide use of EOBRs by providing the following incentives to motor carriers that voluntarily use EOBRs in their CMVs:

(1) revising FMCSA compliance review procedures to permit examination of a random sample of drivers' RODS; and

(2) exempting carriers from HOS supporting documentation requirements if certain conditions are satisfied.

The final rule also includes changes to the type and amount of HOS data collected. The final rule requires EOBRs to record a CMV's location by referencing the nearest city, town, or village at least once every 60 minutes. Drivers who continue to use paper RODS and older AOBRDs are required to record their location by referencing the nearest city, town, or village only when changing duty status (when coming on duty, when changing from driving to on-duty-not-driving, etc.).

IMPACT OF EOBR RULEMAKING ON PERSONAL INFORMATION OF GENERAL PUBLIC

Although FMCSA has permitted the use of an AOBRD to as an alternative to the paper RODS for over twenty years, under the EOBR final rule, more CMV drivers will be required to use EOBRs. This broader use of EOBRs will assist FMCSA in its enforcement of HOS requirements, which in turn will improve commercial motor vehicle safety in general and highway safety in particular. EOBRs produce electronic RODS, which are commonly viewed as more accurate and reliable records of drivers' on-duty driving hours. Affected companies will be required to maintain the accuracy of their EOBRs, including recalibrating them as necessary.

The final rule will cause each motor carrier issued a Remedial Directive to equip all of its CMVs with EOBRs. As a result, this final rule will likely impact individual drivers who have had no or relatively few past violations of HOS requirements to use EOBRS. FMCSA made the decision to apply the requirement to carriers that had certain violation rates, rather than specific drivers who had past violations, for two main reasons. The first, and primary, reason is to prevent erosion of driver safety: FMCSA wanted to preclude the possibility that carriers could easily circumvent the requirements of a "driver-focused" EOBR Remedial Directive by having their non-covered drivers (that is, drivers whose HOS records had not been found noncompliant) work more and perhaps excessive hours to compensate for those previously noncompliant drivers whose HOS would be more closely monitored. Second, applying EOBR usage to individual drivers would present complex compliance oversight challenges for FMCSA to implement. If FMCSA were to apply the "EOBR Remedial Directive" to individual drivers, of which there are millions, each driver's period of mandatory EOBR use would be unique, and each driver's status would have to be monitored in FMCSA's IT systems. The magnitude of implementing such a status change would present significant IT challenges, not the least of which would be driver misidentification issues, and the diversion of resources from other safety-oversight IT needs. Because of these challenges, FMCSA decided to apply the EOBR mandate to motor carrier entities, rather than individual drivers.

FMCSA recognizes that this rulemaking will impact individual's privacy in the collection of HOS records by motor carrier companies. Specifically, information from EOBR will create a more accurate record of the vehicle location and therefore the individual driver of the vehicle. . Unlike AOBRDs, EOBRs must record the CMV location at least once every 60 minutes. This increases the amount of data containing PII collected by motor carriers using EOBRs voluntarily, as well as under a Remedial Directive. As discussed in the preamble to the final rule, FMCSA decided to require that EOBR should collect data every 60 minutes rather than a shorter length of time, such as the one minute interval proposed in the NPRM. FMCSA weighed the enforcement

value with the operational costs to motor carriers and the privacy impact to drivers. FMCSA believes the 60 minute interval strikes the appropriate balance between improving the accuracy and reliability of duty information without creating a costly administrative burden on the covered motor carriers and without intruding unnecessarily upon the privacy of drivers. With respect to privacy, it has determined that enhancing the accuracy of HOS records by using electronic records outweighs the risk that these records could be used for other non-safety related litigation purposes.

Additionally, FMCSA acknowledges that such electronic data required to be retained by motor carriers may be attractive for use in litigation unrelated to HOS compliance and subject to use in both Federal and State courts and administrative agencies. Therefore, FMCSA limited the type of data collected by the EOBR. For example, the final rule does not require that an EOBR collect information regarding the vehicle's speed.

Further, FMCSA emphasizes that the primary purpose for collecting HOS information recorded on EOBRs is to assist authorized Federal and State law enforcement and safety officials when they are conducting compliance assurance activities at the facilities of motor carriers subject to HOS requirements or when they are conducting roadside inspections on the CMVs. Motor carriers will not be required to upload all EOBR information into any Federal or State information system accessible to the public. Rather, interstate CMV drivers' records derived from EOBRs will be treated in a manner consistent with other types of records (handwritten RODS, timecards, electronic AOBRD files) from drivers whose records are reviewed. As in the case of other documentation for RODS, data from EOBRs will only be uploaded to Federal and State systems during the course of an appropriate law enforcement activity (e.g., compliance review). The information uploaded and retained by authorized Federal and State law enforcement and safety officials will be limited to only those motor carrier records that reflect violations of HOS requirements.

For an interstate CMV driver to log into an EOBR, the driver must enter information (such as a user ID and password) into the EOBR that uniquely identifies the driver. Alternatively, the inter-state CMV driver may use other means (such as a smart card or a biometric reader) that uniquely identifies him or her to the EOBR.

The EOBR must have the capability of displaying all of the following information:

(1) driver's name and EOBR user ID on all EOBR records associated with that driver, including records in which the driver serves as a co-driver;
(2) driver's total hours of driving during each driving period and the current duty day;
(3) total hours on duty for the current duty day;
(4) total miles or kilometers of driving during each driving period and the current duty day;
(5) total hours on duty and driving time for the prior 7-consecutive-day period, including the current duty day;
(6) total hours on duty and driving time for the prior 8-consecutive-day period, including the current duty day;

(7) sequence of duty status for each day and the time of day and location for each change of duty status for each driver using the device;

(8) EOBR serial number or other identification and identification number(s) of vehicle(s) operated that day;

(9) remarks, including fueling, waypoints, loading and unloading times, unusual situations, or violations;

(10) driver's override of an automated duty status change to driving if using the vehicle for personal conveyance or for yard movement; and

(11) other data as the motor carrier deems appropriate, including the date and time of crossing a State line for purposes of fuel-tax reporting.

A motor carrier that is required to use EOBRs under the terms of a Remedial Directive, or voluntarily chooses to use EOBRs for recording drivers' RODS in place of using hardcopy records, must ensure the EOBR meets the following additional conditions in order to address all HOS requirements in effect as of November 19, 2008 (73 FR 69567).

(1) EOBR must not permit alteration or erasure of the original information collected concerning the driver's hours of service or alteration of the source data streams used to provide that information.

(2) EOBR must be able to track total weekly on-duty and driving hours over a 7- or 8-day consecutive period.

(3) EOBR must be capable of recording separately each driver's duty status when there is a multiple-driver operation.

(4) EOBR device/system must identify annotations made to all records, the date and time the annotations were made, and the identity of the individual making them.

(5) If a driver or any other individual annotates a record in an EOBR device/system, the annotation must not overwrite the original contents of the record.

A driver's RODS must be submitted according to the following conditions:

(1) The driver must submit each RODS electronically to the employing motor carrier.

(2) For motor carriers not subject to the remedies provisions of part 385 subpart F of the final rule (Remedial Directives), each RODS must be submitted within 13 days of its completion.

(3) For motor carriers subject to the remedies provisions of part 385 subpart F of the final rule, each RODS must be submitted within 3 days of its completion.

(4) The driver must review and verify that all entries (the duty status information generated by the EOBR and the driver's annotations to same) are accurate prior to submitting each RODS to the employing motor carrier.

(5) The submission of each RODS certifies that all entries (duty status information generated by the EOBR and annotations by the driver) are true and correct.

FMCSA will continue to require motor carriers to maintain HOS compliance information (including supporting documents, when applicable) for a period of 6 months from the date the information was generated. This information must be made available to authorized Federal and

State safety and enforcement personnel during on-site compliance reviews. EOBRs will be required to display the information described above on the visual display device installed in the CMVs to ensure that authorized Federal and State safety and enforcement personnel conducting "roadside" inspections of CMVs can determine if inter-state CMV drivers are operating in compliance with the applicable HOS requirements. At the roadside, interstate CMV drivers will be required to have 8 consecutive days of EOBR records.

SUMMARY OF PRIVACY IMPACT ASSESSMENT PROCESS

This Privacy Impact Assessment (PIA) was conducted because EOBRs utilize personally identifiable information of inter-state CMV drivers. This PIA updates the PIA issued on November, 2006 in conjunction with the Notice of Proposed Rulemaking (NPRM). The NPRM and PIA are posted at:http://www.regulations.gov/fdmspublic/component/main?main=DocumentDetail&o=09000064802ca69e.

This PIA analysis reflects the framework of the Privacy Act of 1974 and the Fair Information Practice Principles (FIPPs). In addition, the FMCSA Office of Information Technology is releasing "Best Practices for the Protection of Personally Identifiable Information" (Best Practices for Protection of PII) to provide guidance on privacy and security protections consistent with the FIPPs standards and practices and equivalent to those required under the Privacy Act of 1974 (5 U.S.C. § 552a), the Federal Information Security Management Act (FISMA) of 2002, and the information security standards issued by the National Institute of Standards and Technology (NIST).

The DOT privacy management process is built upon a methodology that enables DOT/FMCSA to have the information, tools, and technology necessary to effectively protect private information while allowing FMCSA to achieve its mission. The methodology includes the following:

- Establishing appropriate authorities, responsibilities, and controls for information management with input from systems architecture, technology, security, legal, and other disciplines;
- Identifying, documenting, and addressing privacy risks;
- Developing and implementing appropriate policies and procedures, and updating them when necessary;
- Monitoring compliance with applicable laws, regulations, policies, and procedures;
- Providing training to all DOT employees and contractor personnel who will process or have access to PII; and
- Effectively maintaining the following privacy protection principles:
  (1) Openness
  (2) Individual Participation
  (3) Purpose Specification
  (4) Collection Limitation

(5) Use Limitation
(6) Data Quality and Integrity
(7) Security Safeguards
(8) Accountability and Auditing

Privacy was a significant consideration in the development of the final rule. A number of motor carriers and drivers expressed reluctance to use EOBRs because the data on these devices could be used inappropriately. Drivers objected to using EOBRs because they were concerned that their privacy could be invaded. They believed EOBRs could also be used to identify non-HOS-related violations, such as speeding. Motor carriers were concerned that data from EOBRs could be used in post-crash litigation. Both parties asked FMCSA to allow EOBR data to be used for HOS compliance enforcement only.

FMCSA recognizes the industry's concerns in this area. Therefore, only information required to determine compliance with HOS regulations will be required to be displayed on EOBRs or made available to enforcement officials. For example, the final rule does not require EOBRs to record engine speed. This information can be derived from other data.

FMCSA's interest in promoting highway safety and preventing CMV accidents is compatible with requiring use of EOBRs to accurately document the number of hours interstate CMV drivers are driving, are on duty or off duty, and are using a sleeper berth as well as the time and location of changes in duty status. Except in the context of an investigation of a crash or a complaint of alleged FMCSR violations, FMCSA does not inquire into an interstate CMV driver's off-duty activities. FMCSA is interested only in whether the driver was afforded an off-duty period and had an opportunity to obtain restorative sleep. A RODS that documents the date, time, and location at each change of duty status is used by FMCSA to reconstruct travel itineraries of interstate CMV drivers in order to determine compliance with HOS regulations. Only HOS records showing violations will be retained by enforcement and safety officials and transmitted to FMCSA systems, for FMCSA's use in reconstructing itineraries and proving violations.

PERSONALLY IDENTIFIABLE INFORMATION AND RULEMAKING

In order to perform HOS compliance-assurance and enforcement functions, Federal and State law enforcement and 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. The final rule does not change the requirements concerning who must comply with HOS rules. While the EOBR final rule does require the collection of more information about an interstate CMV driver's duty status, and requires location to be recorded with greater frequency while the CMV is in motion, the final rule does not require any additional information from EOBRs concerning drivers' activities and the location of such activities that are beyond the scope of the HOS rules.

Best Practices for Protecting PII Associated with EOBRs

The FMCSA Office of Information Technology has issued best practices to assist the Office of Enforcement and Program Delivery and the Office of Policy and Programs in protecting the privacy of PII associated with the implementation of the EOBR final rule. These best practices incorporate standards and practices equivalent to those required under the Privacy Act and other Federal and State laws that implement the Fair Information Principles. FMCSA's best practices for protecting the privacy of PII associated with the implementation of the EOBR final rule include the following:

Openness Principle: FMCSA does not secretly collect PII, and FMCSA clearly discloses its policies and practices concerning the PII it possesses. To that end, FMCSA has provided the public with a description of the information practices associated with the implementation of the EOBR final rule through the NPRM. As noted in the preamble to the final rule, FMCSA received 752 comments on the NPRM. The final rule addresses the comments received during the 60-day public comment period. In response to the comments, and in accordance with the narrow scope of the NRPM, FMCSA determined that it would not exercise "the full extent of its authority at this time" [e.g., to require all motor carriers to use electronic HOS records], "however, and [would] instead propose a more targeted approach of mandating EOBR use for only those carriers with deficient safety management controls, as demonstrated by repeated patterns of hours-of-service violations." (72 FR 2341) The final rule does not require all motor carriers to install and use EOBRs, but it is consistent with the NPRM in targeting only those carriers found by the DOT to have substantial HOS noncompliance and associated deficient safety management controls. The final rule and this PIA fully describe the nature and type of PII collected and used pursuant to the Motor Carrier Act of 1935 (Public Law 74-255, 49 Stat. 543, August 9, 1935, now codified at 49 U.S.C. 31502(b)).

Individual Participation Principle: FMCSA ensures that individuals have the right to (a) obtain confirmation of whether or not FMCSA has PII relating to them; (b) access the PII related to them within 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 concerning him or her and to obtain a copy of such information upon request. FMCSA has a redress process in place, the DataQs system, which provides an electronic means to file concerns about Federal and State data released to the public by the FMCSA. Specifically, the DataQs system allows a filer to challenge data maintained by FMCSA on crashes, inspections, registration/operating authority/insurance matters, compliance reviews, safety audits, enforcement actions and household goods mover complaints. DataQs cannot be used as a substitute for challenging safety ratings/civil actions that are handed through 49 CFR 385.15 or 385.17 (Administrative Review). Through this system, data concerns are automatically forwarded to the appropriate Federal or State office for resolution. Any challenges to data provided by State agencies must be resolved by the appropriate State agency. Once a State office makes a determination on the validity of a challenge, FMCSA considers that decision as the final resolution of the challenge. FMCSA

cannot change State records without State consent. The system also allows filers to monitor the status of each filing.

With respect to EOBR data, FMCSA does not collect or retain comprehensive EOBR records, but only those portions of EOBR and other HOS records necessary for enforcement actions. Under the DataQs process, FMCSA does not "correct EOBR records" that are stored in the motor carrier's information systems. However, 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 Principle: FMCSA specifies at the time of inspection the purpose(s) for collecting PII. Unless individuals are given written notice of, and provide express written consent to, any proposed change to these purposes, the subsequent use of the PII is limited to the fulfillment of those purposes or to purposes that are compatible with the EOBR final rule. Unless otherwise authorized by applicable law, FMCSA limits its use of PII related to the implementation of EOBR regulations to the performance of official responsibilities pertaining to law enforcement, the verification of personal identity, or highway and commercial motor vehicle safety.

FMCSA informs drivers that PII in the EOBR record may be transmitted to law enforcement agencies only if such disclosure is related to the performance of official responsibilities pertaining to law enforcement, the verification of HOS pertaining to highway and motor vehicle safety, or any other official use expressly authorized by law. Possible uses include those described in 5 USC 552a(b) and those that DOT has published pursuant to 5 USC 552a(b)(3) (see 65 FR 19476 at 19477 for General Routine Uses applicable to all DOT systems; see the System of Records Notices (SORNs) for MCMIS and EDMS for system-specific routine uses.

The authority for this rulemaking is described in the Overview section of the preamble to the EOBR Final Rule. The collection of PII (specifically the interstate CMV driver's name) is a necessary part of the final rule because it allows Federal and State law enforcement agencies to match an inter-state CMV driver's name with his or her HOS record. Generally, EOBR records containing PII will be collected by Federal and State law enforcement and safety officials during compliance reviews and roadside inspections, two types of enforcement activities. During a compliance review, a Federal or State official will review multiple interstate CMV drivers' RODS that cover a six month period. The purpose of this review is to identify violations of HOS regulations by the carrier and individual driver. However, a law enforcement or safety official will only collect EOBR data containing PII if a violation exists. (See Collection Limitation Principle Section).

During the roadside inspection, the EOBR data, without the PII, is transferred through a wireless connection to a law enforcement or safety official's laptop computer. The law enforcement or safety official reviews one (or two, in the case of team drivers) interstate CMV driver's RODS data that covers eight consecutive calendar days. Software analyzes the EOBR data and the law enforcement or safety official reviews the results of the data analysis to determine if a citable violation exists. If the official determines that there are no citable violations, the record is deleted on the laptop. If one or more citable violations are found, the law enforcement or safety

official manually enters a unique personal identifier to link [electronically attach] the violation or violations with an individual driver. The record is then uploaded to a Federal or State system. Generally, the purpose of this review is to identify violations of HOS regulations by individual drivers. However, to protect an interstate CMV driver's privacy from being inadvertently transmitted to unauthorized parties, FMCSA has determined the driver's name must not be included in the wireless transmission at roadside (For a more detailed discussion see Information Sharing Section.).

Collection Limitation Principle: FMCSA only collects PII necessary for official purposes as stated in the EOBR final rule. In addition, FMCSA only obtains such PII by lawful and fair means and, to the greatest extent possible, with the knowledge or consent of the individual.

FMCSA considered the potential use of EOBR data in litigation unrelated to HOS violations because of its evidentiary value (i.e., more accurate and reliable). Additionally, FMCSA recognizes that the final rule causes those motor carrier companies with a certain pattern of HOS violations to collect more data containing PII and causes motor carrier companies to collect electronic records on inter-state CMV drivers who may never have violated the HOS regulations. However, FMCSA acknowledges that it cannot by a rulemaking affect the rights of private litigants to seek discovery from motor carriers, States or FMCSA in Federal and State judicial or administrative proceedings. Similarly, existing provisions governing FMCSA disclosure of motor carrier and inter-state CMV driver information under the Freedom of Information Act (FOIA) are not affected by this rulemaking, but may be under State/local information access laws.

In consideration of these factors, FMCSA limited the collection of PII by requiring only that information relevant to CMV safety regulation be collected (49 CFR 395.16(b)). Specifically, FMCSA is only requiring motor carriers to use EOBRs to collect, along with the driver's name, location data at each change of duty status and at intervals at least every 60 minutes while the CMV is in motion. FMCSA decided on this location-recording interval to ensure travel distance and the associated driving time are recorded and reported at a level of accuracy appropriate to ensure HOS compliance. Based on the information provided by commenters and the Agency's decision to continue to require that on-board recorders be integrally synchronized with the vehicle's engine use status, FMCSA believes the new requirement achieves an appropriate balance between accuracy, affordability and impacts to privacy.

In addition to limiting the number of motor carriers that must collect this data electronically, the final rule does not revise the record retention requirements applicable to motor carriers required to use EOBRs. The record retention requirements for HOS will remain at 6 months for all motor carriers. At the roadside, an interstate CMV driver will only be required to have in his or her possession HOS records for the current day and the previous 7 days.

FMCSA also plans to follow past practices in releasing individual driver information collected from EOBRs. In response to past FOIA requests for driver RODS from motor carriers, FMCSA redacts all information that reveals the identity of an individual driver when the FOIA personal privacy exemption allows it to disclose HOS records in a redacted form.

Use Limitation Principle: FMCSA only uses PII for the purposes and uses originally specified in the EOBR final rule except (a) with the express consent of the individual, or (b) as authorized by law.

The only information FMCSA requires EOBRs to collect is that which is necessary to determine interstate CMV driver and motor carrier compliance with HOS regulations. For that reason, FMCSA does not require EOBRs to collect data on vehicle speed, braking action, steering function, or other vehicle performance parameters. FMCSA requires automatic recording of CMV location information only to the level of precision (State, county, and populated place) found in the National Standard for Named Physical and Cultural Geographic Features maintained by the Department of the Interior's United States Geological Survey. The final rule requires location tracking only once every 60 minutes while a CMV is in motion in order to allow enforcement personnel to determine an inter-state CMV driver's HOS compliance. When conducting roadside inspections, authorized law enforcement and safety officials will view eight consecutive days of RODs pertaining to one or two drivers and when conducting compliance reviews, authorized law enforcement and safety officials will view 6 months of RODS pertaining to multiple drivers.

FMCSA will limit its disclosure of PII collected and stored on DOT systems as a result of the EOBR final rule consistent with Privacy Act System of Record Notices for Motor Carrier Management Information System (MCMIS) and Electronic Docket Management System (EDMS). HOS information recorded on EOBRs will be examined by Federal and State authorized law enforcement and safety officials when conducting compliance reviews or roadside inspections. Although motor carriers are not required to upload this information into any Federal or State information system accessible to the public, EOBR information that contains HOS violations will be uploaded into a Federal or State system by an authorized Federal or State law enforcement and safety official. EOBR information that shows violations of HOS rules will be uploaded to MCMIS and EDMS.

Data Quality and Integrity Principle: FMCSA ensures that PII collected, used, and maintained related to the implementation of the EOBR final rule 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. Data accuracy concerning interstate CMV drivers' RODS will improve as a result of the rule, which establishes new performance standards for EOBRs and mandates the use of EOBRs by motor carriers with chronic non-compliance with Federal HOS rules. Interstate CMV drivers and their employing motor carriers are responsible for the accuracy of the information collected by EOBRs, as they would be if they used handwritten RODS. Drivers will have the opportunity to review all information generated by EOBRs and to make additional annotations (entries to augment, but not overwrite, other recorded data) as needed to clarify situations where there may be inconsistencies in the data. Interstate CMV drivers will also certify the accuracy of the duty status information generated by EOBRs. If a driver knowingly falsifies his certification, then he could be liable for civil penalties pursuant to 49 USC 521.

New provisions include the default status for EOBRs and audit trails. The "default" status for an EOBR is defined by FMCSA as on-duty not-driving (ODND) when the vehicle is stationary (not moving with the engine off) for 5 minutes or more. When the CMV is stationary and the driver is in a duty status other than the default status, the driver must enter the duty status manually on the EOBR. The performance requirements of § 395.16 also add a provision for automatically recording the location of the CMV. The final rule requires a recording interval no greater than 60 minutes. FMCSA believes that this interval (rather than, for example, 15 or 30 minutes) strikes the appropriate balance between improving the accuracy and reliability of ODND status information and off-duty information without intruding unnecessarily upon the privacy of the driver. Drivers will still be required to record the location of each change of duty status, as currently required under §§ 395.8 and 395.15. Finally, as stated in the NPRM (72 FR 2352), FMCSA recognizes that the need for a verifiable EOBR audit trail—a detailed set of records to verify time and physical location data for a particular CMV—must be counterbalanced by privacy considerations.

Security Safeguards Principle: This principle requires that PII be protected by reasonable security safeguards against loss or unauthorized access, destruction, misuse, modification, or disclosure. These safeguards incorporate standards and practices required for Federal information systems under FISMA and the information security standards issued by NIST, including the Federal Information Processing Standards Publication (FIPS PUB 200) and the NIST Recommended Security Controls for Federal Information Systems (NIST 800-53). FMCSA has a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate for the protection of data. These safeguards are designed to achieve the following objectives:

- Ensure the security and confidentiality of PII related to HOS regulations.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII.
- Protect against unauthorized access to or use of PII.

As a general matter, any HOS violation information that authorized Federal or State law enforcement and safety officials collect from EOBRs, save on their portable computers at roadside or at carrier facilities, and transfer to FMCSA, will be uploaded and stored in MCMIS and the EDMS, both of which are FMCSA Privacy Act Protected Systems of Records.

Accountability and Auditing Principle: FMCSA is accountable for compliance with the Federal Government privacy and security policies and regulations. In addition, FMCSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to Agency privacy and security policies and regulations. FMCSA follows the Best Practices for the Protection of Personally Identifiable Information Associated with Implementation of the EOBR Devices and Information Security Best Practices. As stated in the September 2004 NPRM (69 FR 53386, at 53392, Sept. 1, 2004) and reiterated under Audit Trail/Event Log in the NPRM preamble (72 FR 2340, at 2351, January 18, 2007), the Agency recognizes that the need for a

verifiable EOBR audit trail – a detailed set of records to verify time and physical location data for a particular CMV – must be counterbalanced by privacy considerations.

Any HOS violation information that authorized Federal or State law enforcement and safety officials collect from EOBRs, save on their portable computers at roadside or at carrier facilities, and transfer to FMCSA, will be uploaded and stored in MCMIS and the EDMS, both of which are FMCSA Privacy Act-protected systems of records.

FMCSA operates MCMIS and EDMS in accordance with the E-Government Act (Public Law 107-347), the Federal Information Security Management Act (FISMA) of 2002, and other required policies, procedures, practices, and security controls for implementing the Automated Information System Security Program.

Only authorized Federal and State government personnel and contractors conducting system support or maintenance may access records in these systems. Access to records is password protected, and the scope of access for each password is limited to the official need of each individual who is authorized to access the systems. Additional protection is afforded by the use of password security, data encryption, and a secure network.

These systems capture sufficient information in audit records to establish what events occur, the sources of the events and the outcome of the events. These events are identified by type, location or subject. This type of auditing ensures accountability and support after-the-fact investigations of security incidents. Access to the audit logs are restricted and controlled by system administrators.

INFORMATION SHARING

FMCSA has developed several software tools to facilitate the roadside safety inspection process. Authorized law enforcement and safety officials use the Aspen software (and States' equivalent systems) to collect information concerning the driver and vehicle to generate an electronic inspection report. The development of a new software tool, eRODS, will allow enforcement and safety officials to assess HOS information rapidly and accurately at roadside to determine whether or not the driver is in compliance with the HOS regulations. The process of transferring EOBR data, including PII, at the roadside using eRODS is described in the following paragraphs.

During a roadside inspection, authorized law enforcement and safety officials would use the eRODS software to download the information stored in an EOBR device, and then to determine if a driver is in compliance with HOS regulations. Access to an EOBR device can be either via a wireless or a wired protocol. The preferred method to access the EOBR is via a wireless connection – the law enforcement and safety official would use a wired connection only if the wireless transfer fails. The eRODS software does not download the name of the driver or any personal identifier, but rather transfers duty status, time, and miles driven. The final rule specifically excludes PII from the EOBR files downloaded at roadside so as not to subject PII transmitted by wireless means to inadvertent or deliberate capture. The eRODS software then analyzes the EOBR HOS files and displays a graph that represents the data and highlights areas

of violation. The eRODS software also generates a summary of interstate CMV driver activity and HOS violations.

Once the law enforcement or safety official reviews the results of the eRODS analyses of the EOBR records, he or she determines whether a citable violation actually exists (for example, if the analyses generate one 5-minute violation of a single 10-hour off-duty period, it would not be likely that a citation would be written). If no citable violation exists, the law enforcement or safety official immediately deletes the entire EOBR file. If the safety official determines that a citable violation exists, the safety official manually enters the cited driver's PII (driver name, license number, issuing jurisdiction) into the Aspen software, along with the citable HOS violations identified by eRODS. The law enforcement or safety official completes the inspection, notes any other safety violations (additional driver violations, such as an expired medical card, and vehicle violations such as brakes out of adjustment or inoperative lighting devices) into the Aspen application.

The inspection record is saved, and the EOBR file is also saved as an attachment to the inspection record. The entire inspection record is then uploaded to MCMIS.

FMCSA's interest is that each driver used by a motor carrier is uniquely identified for purposes of recordkeeping and that each motor carrier ensures that drivers enter duty status information accurately. How individual drivers are identified internally—by name, by employee number, or by another code—are left to a motor carrier's discretion. However, FMCSA very strongly discourages a motor carrier from using a Social Security number or driver's license number because of the potential for persons to obtain access to information that is not relevant to HOS compliance assurance. It is a motor carrier's responsibility to select and implement information security policies — including issuing and updating identification and information system access codes — appropriate to its own operations.

It is worth noting, however, that by eliminating the use of individual names in the wireless transmitted EOBR record, it becomes more difficult for unauthorized users to capture that information from a stream of transmitted information and easily tie it to a specific individual. For this reason, the driver's name is not transmitted wirelessly from the EOBR to the roadside officials' portable computer. The official will then manually enter the name of the driver (and the name of the co-driver if applicable) into the portable computer. The transmission of data from the official's portable computer to MCMIS takes place later, and the information is encrypted for transmission.

SYSTEM OF RECORDS

This rulemaking will not result in a new or revised Privacy Act System of Records for FMCSA. This rulemaking does not cause or require new or additional information to be collected in MCMIS and EDMS that is not covered by the existing SORN.