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

PRIVACY IMPACT ASSESSMENT

NOTICE OF PROPOSED RULEMAKING: ELECTRONIC ON-BOARD RECORDERS FOR HOURS-OF-SERVICE COMPLIANCE 2

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

Reviewing Official
Pam Gosier-Cox
Office of Information Technology,
Federal Motor Carrier Safety Administration
(202) 366-3655
Pam.Gosier.Cox@dot.gov

TABLE OF CONTENTS

OVERVIEW OF FEDERAL MOTOR CARRIER SAFETY ADMINISTRATION ELECTRONIC ON-BOARD RECORDERS AND SUPPORTING DOCUMENTS NOTICE OF PROPOSED RULEMAKING[1]

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 preamble of the Notice of Proposed Rulemaking (NPRM) 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 CMV 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

[1] FMCSA published a Final Rule on April 5, 2010 that updated the technical specifications for HOS recording devices and that requires motor carriers with serious HOS non-compliance to use these devices under the terms of a Remedial Directive. This rulemaking action is known as "EOBR 1." The follow-on rulemaking action that is the subject of this PIA would mandate use of these devices by a larger number of motor carriers and would also revise requirements for collecting and maintaining supporting documents. This new rulemaking action is known as "EOBR 2."

turn will improve CMV 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 1 Final Rule (effective June 4, 2010).

This EOBR 2 NPRM would require certain motor carriers to use EOBRs to document drivers' compliance with the HOS requirements. More information about the FMCSA's statutory authority can be found in the Legal Basis section of the EOBR2 NPRM.

With respect to supporting documents, section 113(a) of the Hazardous Materials Transportation Authorization Act of 1994 (Pub. L. 103-311, August 26, 1994, 108 Stat. 1673, 1676) (HMTAA) requires the Secretary of Transportation to prescribe regulations to improve--(A) compliance by commercial motor vehicle drivers and motor carriers with hours-of-service requirements; and (B) the effectiveness and efficiency of Federal and State enforcement officers reviewing such compliance.

CURRENT DESCRIPTION OF AUTOMATIC ON-BOARD RECORDING DEVICES, EOBR 1 FINAL RULE AND SUPPORTING DOCUMENTS

For many years before the publication of the April 2010 EOBR 1 Final Rule, which requires certain motor carriers to collect and maintain electronic RODS, DOT's Federal Highway Administration (FHWA, the Agency responsible for motor carrier safety before January 2000) allowed voluntary use of electronic RODS. FHWA issued a Final Rule on September 30, 1988, (53 FR 38666) that revised 49 CFR part 395 of the Federal Motor Carrier Safety Regulations (FMCSRs) to allow, but not to 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 49 CFR 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."

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[2]. 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.

[2] This established practice has been in place for several years- since the beginning of the Motor Carrier Safety Assistance Program.

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 the safety official determines that a citable violation exists, the safety official manually enters the cited driver's PII (driver name, CMV 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 the Motor Carrier Management Information System (MCMIS). EOBR information that shows violations of HOS rules is uploaded to MCMIS and EDMS.

FMCSA issued a Final Rule on April 5, 2010, ("Electronic On-Board Recorders for Hours-of-Service Compliance") that established the "safety of operation and equipment" of motor carriers and "standards of equipment" of motor private carriers. When effective (effective date: June 4, 2010; compliance date: June 4, 2012), the EOBR 1 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.

The EOBR 1 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 EOBR 1 Final Rule also allows for the continued collection of required PII from interstate CMV drivers with citable violations, RODS, and other supporting documentation.

FMCSA has amended the FMCSRs to incorporate the performance standards for EOBRs defined in EOBR 1. Carriers voluntarily using EOBRs that meet or exceed these standards will continue to receive the incentives through this rule that they currently receive.

The EOBR 1 Final Rule requires EOBRs to record a CMV's location by referencing the nearest city, town, or village at least once every 60 minutes.

The following table compares the information required to be recorded by a § 395.15-compliant AOBRD and a § 395.16-compliant EOBR.

Comparison of information collected by an AOBRD and information collected by an EOBR

395.15(c):Duty status and information recorded by an	395.16(b): Information recorded by an EOBR:

AOBRD:	
(5)Date.	(3) Date and time.
(6)Total miles driving today.	(5) Distance traveled.
(12)Total hours.	(9) Hours in each duty status for the 24-hour period and total hours.
(11) Name of co-driver.	(1) Name of driver and any co-driver(s) and corresponding driver identification information (such as a user ID and password). However, the name of the driver and any co-driver is not required to be transmitted as part of the downloaded file during a roadside inspection.
(9)Main office address.	
	(8) The multiday basis (7 or 8 days) used by the motor carrier to compute cumulative duty hours and driving time.
	(4) Location of CMV.

OVERVIEW OF THE EOBR 2 RULEMAKING

FMCSA is publishing an NPRM to amend the FMCSRs to require motor carriers operating CMVs in operations requiring the use of a record of duty status (49 CFR 395.8) but that are not allowed to use timecards (vehicles designed or used to transport nine or more passengers including the driver[3] and CMVs used to transport hazardous materials in bulk) to use EOBRs that meet or exceed the requirements of 49 CFR 395.16. On-board HOS recording devices meeting the requirements of 49 CFR 395.15 and voluntarily installed in CMVs manufactured before June 4, 2012 may continue to be used for the remainder of the service life of those CMVs.

The EOBRs proposed in this NPRM are subject to the same technical specifications as published in the EOBR 1 Final Rule, published April 5, 2010.

This NPRM also proposes a requirement for motor carriers to systematically and effectively monitor each driver's compliance with HOS requirements through the use of EOBR records and

[3] Except for private motor carriers – nonbusiness. These carriers are except from FMCSRs.

supporting documents. The supporting documents that motor carriers must retain are, at a minimum, the documents generated or received by the motor carrier in the normal course of business. The supporting documents that FMCSA will require motor carriers to maintain will have the following data points: (i) driver name or personal identification number; (ii) date; (iii) time; and (iv) location. These records are to be collected from the following four categories: (i) payroll; (ii) trip-related expense reports; (iii) fleet management system communication logs; and (iv) bills of lading or equivalent documents. These documents must be maintained by the motor carrier if they are generated or received during the normal course of business. These documents will be retained by the motor carrier as a part of a HOS compliance management system. In the course of an investigation, an FMCSA credentialed Safety Investigator must have access to these files, and to any files in the motor carrier's possession (as they currently do).

IMPACT OF EOBR 2 RULEMAKING ON PERSONAL INFORMATION OF GENERAL PUBLIC

Even though FMCSA and its predecessor have allowed voluntary use of electronic HOS records for more than 20 years, the April 2010 Final Rule is the first to mandate their use, albeit for a limited population of motor carriers that would be subject to a Remedial Directive and their drivers. This broader use of EOBRs will assist FMCSA in its enforcement of HOS requirements, which in turn will improve CMV 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 carriers will be required to maintain the accuracy of their EOBRs, including recalibrating them as necessary.

The EOBR 2 NPRM will expand the population of CMV drivers expected to use EOBRs but will not alter the technical specifications of the EOBRs themselves.

The EOBR 1 Final Rule will have an impact on an individual's privacy in the collection of HOS records by motor carrier companies. This is due to the increased amount of data containing PII collected by motor carriers using EOBRs voluntarily, as well as under a Remedial Directive.

Additionally, as discussed in the EOBR 1 Final Rule Privacy Impact Assessment (PIA), 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 at a level of precision to pinpoint a street address.

Further, FMCSA emphasizes that, just as in the EOBR 1 Final Rule, the primary purpose for collecting HOS information recorded on EOBRs is to assist authorized Federal and State law enforcement and safety officials. These officials use HOS information when they are conducting compliance assurance activities at the facilities of motor carriers subject to HOS requirements, and when they are conducting roadside inspections on CMVs subject to these regulations. 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 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 interstate 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.

The requirements of the April 5, 2010 Final Rule are still applicable to the motor carriers complying with EOBR 1 under a Remedial Directive or motor carriers voluntarily using EOBRs.

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) The EOBR must not permit alteration or erasure of the original information collected concerning the driver's HOS or alteration of the source data streams used to provide that information,

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

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

(4) The 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, and

(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 all of the following conditions:

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

(2) For motor carriers not subject to the Remedial Directive provisions of 49 CFR part 385, subpart F of the EOBR 1 Final Rule, each RODS must be submitted [to the motor carrier] within 13 days of its completion.

(3) For motor carriers subject to the Remedial Directive remedies provisions of 49 CFR part 385, subpart F of the EOBR 1 Final Rule, each RODS must be submitted [to the motor carrier] within three 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 six 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 of motor carriers. 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 interstate CMV drivers are operating in compliance with the applicable HOS requirements. At the roadside, interstate CMV drivers will be required to have eight consecutive days of EOBR records.

Supporting documents for HOS compliance collected by the motor carrier will be retained by the motor carrier. Currently, an Agency guidance document published November 17, 1993 (58 FR 60734) provides an interpretation of the regulatory text which provides over 30 examples of supporting documents. FMCSA never intended to require motor carriers to retain all 30-plus types of documents, but many motor carriers do treat the list as though it were a regulation, not guidance. These carriers currently maintain almost every document that they receive (and large amounts of PII). This proposed change to the regulation provides clarification by limiting the types of supporting documents motor carriers are required to maintain. These records will now be limited to: payroll, trip-related expense records and receipts, fleet management system communication logs, and bills of lading or equivalent documents.

FMCSA Safety Investigators will have access to these files during reviews (through EDMS), but this information will not be submitted on a regular basis to FMCSA. In addition, these documents would be kept during the normal course of business, and would not contain sensitive information or PII.

SUMMARY OF PIA PROCESS

FMCSA conducted this PIA because EOBRs utilize PII of interstate CMV drivers. The EOBR 1 Final Rule and corresponding PIA are posted at:

http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480acfb7f.

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, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf) 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 personal 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.

FMCSA recognizes the industry's concerns about data from EOBRs being used inappropriately, or to invade driver privacy. Therefore, only information required to determine compliance with HOS regulations is be required to be displayed on EOBRs or made available to enforcement officials. For example, the EOBR 1 Final Rule does not require EOBRs to record engine speed; the data derived will not be used to enforce non-HOS related violations such as speeding; and the vehicle location requirements are not required to be at a level of precision to identify street addresses.

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, whether they are on-duty or off-duty, and whether they are using a sleeper berth, as well being compatible with requiring use of EOBRs to accurately document 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.

PII 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 EOBR 1 Final Rule does not change the requirements concerning who must comply with HOS rules. The EOBR 2 NPRM proposes to require the collection of information about an interstate CMV driver's duty status and requires location to be recorded with frequency while the CMV is in motion. The EOBR 2 NPRM 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.The provisions of the NPRM would not change the information contained in an EOBR-generated record. As said previously, EOBR 2 merely expands the field of commercial motor vehicle drivers who are subject to it. And, although the number of regulated entities and individuals required to use EOBR to record HOS would change, the protection of PII and other personal information would continue. FMCSA also will continue to apply the privacy safeguards that the Agency has in place. There is no change in privacy impact merely because of this expansion. The privacy impact remains the same as that explained in EOBR 1.

Best Practices for Protecting PII Associated with EOBRs

The FMCSA Office of Information Technology will issue 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 future implementation of the EOBR 2 Final Rule. As this is currently in the NPRM stage of rulemaking, these best practices incorporate standards and practices equivalent to those required under the Privacy Act and other Federal and State laws that implement the FIPPs. FMCSA is developing a plan to use best practices for protecting the privacy of PII associated with the implementation of the EOBR 1 Final Rule of April 2010, as well as the NPRM for EOBR 2, because both will use the same technical specifications.

Openness Principle: FMCSA does not secretly collect PII, and FMCSA clearly discloses its policies and practices concerning the PII it possesses. The EOBR 1 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)), as applicable to this EOBR 2 NPRM. Any supporting documents collected by an investigator are maintained in EDMS.

Individual Participation Principle: FMCSA continues to ensure 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 FMCSA. Specifically, DataQs allows a filer to challenge data maintained by FMCSA on, among other things, crashes, inspections, registration, operating authority, safety audits, and enforcement actions. Through this system, data concerns are automatically forwarded to the appropriate Federal or State office for processing and resolution. Any challenges to data provided by State agencies must be resolved by the appropriate State agency. Additionally, FMCSA is not authorized to direct a State to change or alter the Motor Carrier Management Information System (MCMIS) data for violations or inspections originating within a particular State(s). 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 1 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 CMV 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 U.S.C. § 552a(b) and those that DOT has published pursuant to 5 U.S.C. § 552a(b)(3) (see 65 FR 19476 at 19477, as supplemented at 68 FR 8647 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 1 Final Rule. The collection of PII (specifically the interstate CMV driver's name) is a necessary part of the EOBR 1 Final Rule because it allows Federal and State law enforcement agencies to match an interstate 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 the Collection Limitation Principle section of this PIA.)

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 of this topic, see the Information Sharing section of this PIA.)

Collection Limitation Principle: FMCSA only collects PII necessary for official purposes as stated in the EOBR 2 NPRM. 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 EOBR 1 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 interstate CMV drivers who may never have violated the HOS regulations. However, FMCSA acknowledges that it cannot affect by a rulemaking 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 interstate CMV driver information under the Freedom of Information Act (FOIA) are not affected by this rulemaking but may be affected 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 among accuracy, affordability, and impacts to privacy.

In addition to limiting the number of motor carriers that must collect this data electronically, the EOBR 1 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 six 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 seven 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 2 NPRM 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 EOBR 1 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 interstate 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 six 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 1 Final Rule consistent with Privacy Act SORNs for MCMIS and 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 officials. 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 1 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 or her certification, then he or she could be liable for civil penalties pursuant to 49 U.S.C. 521.

The provisions of the EOBR 1 Final Rule 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 five 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 49 CFR 395.16 also add a provision for automatically recording the location of the CMV. The EOBR 1 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 49 CFR 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 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 (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf) . As stated in the April 5, 2010 EOBR 1 Final Rule (75 FR 17208), 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.

FMCSA operates MCMIS and EDMS in accordance with the E-Government Act (Public Law 107-347), the 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 EOBR 1 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 five-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 or EDMS that is not covered by the existing SORN.