U.S. Department of Transportation
Federal Motor Carrier Administration (FMCSA)

Privacy Impact Assessment
Coercion of Commercial Motor Vehicle Drivers; Prohibition Notice of Proposed Rulemaking

Responsible Official
Charles Medalen
Regulatory Affairs Division
Office of Chief Counsel
Federal Motor Carrier Safety Administration
202-366-1354
Charles.Medalen@dot.gov

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

5/14/2014

X Claire W. Barrett

Claire W. Barrett
DOT Chief Privacy & Information Asset Officer
Signed by: CLAIRE W BARRETT

DOT Privacy Office - Adjudicated - 051414

Executive Summary

Congress mandated that the Federal Motor Carrier Safety Administration (FMCSA) ensure that any regulations adopted pursuant to the Motor Carrier Act of 1984, 49 U.S.C. 31136(a), as amended by section 32911 of the Moving Ahead for Progress in the 21st Century Act (MAP-21), do not result in coercion of drivers by motor carriers, shippers, receivers, or transportation intermediaries. Under this MAP-21 provision FMCSA is publishing an NPRM that would to prohibit these entities from coercing drivers to operate commercial motor vehicles (CMVs) in violation of certain sections of the Federal Motor Carrier Safety Regulations (FMCSRs) or the Hazardous Materials Regulations (HMRs). FMCSA also proposes to utilize the broad authority of the Motor Carrier Safety Act of 1984 (MCSA) [49 U.S.C. 31136(a)(1)-(4)] and authorities transferred from the former Interstate Commerce Commission (ICC) under the ICC Termination Act [49 U.S.C. 13301(a)] to prohibit operators of CMVs from coercing drivers to violate certain provisions of the Agency's commercial regulations.

The major provisions of this notice of proposed rulemaking (NPRM) include prohibitions of coercion, procedures for drivers to report incidents of coercion to FMCSA, and rules of practice the Agency would follow in response to allegations of coercion. The procedures for drivers to report incidents of coercion to FMCSA would include personally identifiable information (PII). This Privacy Impact Assessment (PIA) is necessary to provide information regarding the program, the necessity to collect PII and the fulfillment of specific privacy requirements in MAP-21. This PIA will be placed in the public docket for the NPRM and on the Department's privacy website at www.dot.gov/privacy.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;

- *Accountability for privacy issues;*

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

DOT Privacy Office - Adjudicated-05142

- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & Overview

In the Coercion NPRM, FMCSA proposes to adopt regulations that prohibit motor carriers, shippers, receivers, or transportation intermediaries from coercing drivers to operate CMVs in violation of certain provisions of the FMCSRs – including drivers' hours-of-service limits and the commercial driver's license (CDL) regulations and associated drug and alcohol testing rules – or the Hazardous Materials Regulations (HMRs). In addition, the Coercion NPRM would prohibit anyone who operates a CMV in interstate commerce from coercing a driver to violate the commercial regulations. The Coercion NPRM includes procedures for drivers to report incidents of coercion to FMCSA, rules of practice the Agency would follow in response to allegations of coercion, and describes penalties that may be imposed on entities found to have coerced drivers. This proposed rulemaking is authorized by section 32911 of MAP-21 and the MCSA of 1984, as amended.

Drivers alleging illegal discrimination or discipline under regulations of the Occupational Safety and Health Administration (OSHA) [29 CFR 1978.100, et seq.], or coercion under FMCSA's proposed regulations [49 CFR 390.6], bear a substantial burden of proof. FMCSA cannot proceed without evidence and the driver will have to voluntarily provide much of that evidence. The proposed new complaint procedures in 49 CFR 386.12a and 390.6(b) allow drivers to present whatever evidence they have to substantiate an allegation of coercion.

Personally Identifiable Information and the Coercion NPRM

Drivers wishing to file a complaint of coercion against motor carriers, shippers, receivers or transportation intermediaries must provide the following PII to FMCSA;

(1) The driver's name, address, and telephone number;
(2) The name and address of the person allegedly coercing the driver;
(3) The specific provisions of the regulations that the driver alleges he or she was coerced to violate; and
(4) A concise but complete statement of the facts relied upon to substantiate each allegation of coercion, including the date of each alleged violation.

This information is used by FMCSA to follow up with the driver in order to investigate the complaint.

FMCSA provides enhanced procedural protections and remedies intended to protect drivers from actions considered coercive. If after investigation the FMCSA determines that a violation has occurred, the Agency may levy a civil penalty against the carrier, shipper, receiver or transportation intermediary.

Fair Information Practice Principles (FIPPs) Analysis

The Fair Information Practice Principles (FIPPs) are rooted in the tenets of the Privacy Act and are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs are common across many privacy laws and provide a framework that will support DOT efforts to appropriately

DOT Privacy Office – Adjudicated, 05414

identify and mitigate privacy risk. The FIPPs-based analysis DOT conducts is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v.32, which is sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council.

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their PII. Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Drivers submit coercion complaints either by email or phone call to the FMCSA Division office in the State in which the coercion allegedly occurred or in the State where the alleged coercing party has its principal place of business. FMCSA will maintain coercion complaints in the Agency's Electronic Document Management System (EDMS) FMCSA will handle complaints of coercion in a manner similar to any other enforcement complaint that results in an investigation. The investigation process is spelled out in Federal Statute 49 USC 31143(a).

FMCSA retrieves coercion complaints from EDMS by the complainant name and therefore the records are covered by the Privacy Act of 1974. The EDMS systems of records notice (SORN) was published in the Federal Register on June 21, 2006 (DOT/FMCSA 005 – Electronic Document Management System (EDMS) 71 FR 35727). FMCSA is evaluating whether to develop a separate SORN exclusive to the Coercion records or to update the current EDMS SORN. Based on this analysis, either a new SORN will be developed or the EDMS SORN will be updated to reflect the final Coercion rule once it is published.

As necessary, the EDMS PIA, published on June 6, 2006, is posted on the DOT website at www.dot.gov/privacy and will be updated to reflect the final Coercion rule once it is published. The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency into FMCSA's Coercion rulemaking. This Coercion rulemaking PIA will be updated to reflect the final Coercion rule once published.

Individual Participation and Redress

DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Anyone who submits a complaint is allowed to update or correct the information which is submitted. They are not allowed to delete the information from the database.

FMCSA continues to ensure that individuals have the right to (a) obtain confirmation of whether the Agency has PII relating to them; (b) access the PII related to them within a reasonable time, at reasonable cost, and in a manner and

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

DOT Privacy Office - Adjudicated 051414

form that is readily intelligible to them; (c) an explanation if a request made under (a) or (b) is denied and to challenge such denial; and (d) challenge PII relating to them and, if the challenge is successful, have the data erased, rectified, completed, or amended.

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

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

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

Federal Motor Carrier Safety Administration
Attn: FOIA Team MC-MMI
1200 New Jersey Avenue SE
Washington, DC 20590

Fax: (202) 385-2335
Attn: FOIA Team
E-mail: foia@fmcsa.dot.gov

Statutory Authority and Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which its collects, uses, maintains, or disseminates PII.

The authority for the Coercion NPRM is the Motor Carrier Safety Act of 1984 (MCSA) (Pub. L. 98-554, Title II, 98 Stat. 2832, October 30, 1984), as amended by the Moving Ahead for Progress in the 21st Century Act (Pub. L. 112-141;, 126 Stat. 405, 818, July 6, 2012) [49 U.S.C. 31136(a)], and the broad rulemaking authority conferred by the ICC Termination Act of 1995 (Pub. L. 104-88, Dec. 29, 1995, 109 Stat. 803, 856) [49 U.S.C. 13301(a)]. To learn more information about the authorities consult the Coercion NPRM document.

FMCSA limits its use of the PII collected as part of the Coercion complaint to the purposes detailed in the EDMS SORN pertaining to enforcement of regulations. The collection of PII is necessary to enable the Agency to contact drivers submitting a complaint to gather further information and provide them with the status of the investigation.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in

DOT Privacy Office - Adjudicated - 051414

accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule. Forms used for the purposes of collecting PII shall be authorized by the Office of Management and Budget (OMB).

Individuals filing a complaint are required to submit information about themselves as discussed in the Overview section of this PIA. FMCSA uses the information to evaluate the merits of the complaint and obtain further information on the alleged coercion from the individual initiating the claim. The FMCSA has not established a specific form that individual must use to submit a complaint and individuals are strongly encouraged not to provide any unnecessary personal data such as date of birth or social security number when filing their complaint. Complaints may be sent via email, letter, or by contacting the appropriate State Division office via telephone 1-800-832-5660 or email found at the following link: http://www.fmcsa.dot.gov/about/contact/offices/displayfieldroster.aspx. .

In accordance with the provisions of the U.S. National Archives and Records Administration (NARA) SF 115: NI-557-05-07[3], Item 4, FMCSA destroys or deletes records relating to an individual's complaint and subsequent investigation when no longer needed for administrative, legal, audit, or other operational purposes.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

The FMCSA collects data only to the extent necessary to meet the authorized safety mission of the Agency. In order to perform enforcement functions, the information collected to implement the Coercion NPRM allows authorized safety officials to use personal information to positively identify and contact the driver.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

FMCSA proposes to maintain the information voluntarily provided by the CMV driver for the purpose of pursuing a case of coercion against a motor carrier, shipper, receiver or transportation intermediary. The Agency will also update the information as necessary and verify if the driver still wishes to continue with the complaint.

All information contained in the initial coercion complaint and stored in EDMS is provided by the CMV driver pursing a complaint. The CMV driver will submit all information that he or she considers necessary to support the alleged coercion violation. FMCSA relies upon the CMV driver to ensure that the submitted information is correct. FMCSA can only ensure the confidentiality and integrity of the PII contained in the coercion complaint files once the information has been received from the individual and stored in EDMS.

DOT Privacy Office - Adjudicated - 051414

[3] NARA SF 115: NI-557-05-7, Item 4. Electronic Document Management System (EDMS) Inputs-Disposition: Destroy or delete when imported into the EDMS system and verified. Master Data Files-Record Copy – Disposition: Destroy or delete when no longer needed for reference. System Documentation – Disposition: Destroy or delete when superseded or obsolete.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

All the PII collected through a complaint is stored in EDMS, the security of the PII is dependent on the security controls in place for EDMS. The PII will be protected by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure when stored in EDMS.

Physical access to the EDMS system is limited to appropriate personnel through applicable physical security requirements of the agency. FMCSA and contract support personnel with physical access have all undergone and passed DOT background checks.

Access to information in EDMS, including PII, is determined by permission levels, and EDMS employs role-based access controls. The FMCSA controls access privileges based on whether the user is a State or Local official or an FMCSA employee. User accounts are assigned access rights based on the roles and responsibilities of the individual user. Individuals requesting access to EDMS must submit some personal information (e.g., name, contact information, and other related information) to FMCSA as part of the authorization process.

Users are required to authenticate with a valid user identifier and password in order to gain access to EDMS. This strategy improves data confidentiality and integrity. These access controls were developed in accordance with Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* dated March 2006 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, *Security Controls for Federal Information Systems* dated April 2013. Regular monitoring activities are also performed annually to provide ongoing oversight of security controls and to detect misuse of information stored in or retrieved by EDMS.

All EDMS users are made aware of the FMCSA Rules of Behavior (ROB) for IT Systems prior to being assigned a user identifier and password and prior to being allowed access to EDMS.

The EDMS is undergoing a security reauthorization process under the National Institute of Standards and Technology. The security authorization process is scheduled to be complete in April 2014.

Accountability and Auditing

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

FMCSA is responsible for training and holding Agency personnel accountable for adhering to the Agency's privacy and security policies and regulations. FMCSA will follow the Fair Information Practice Principles as best practices for the protection of information associated with the complaint records held in EDMS in the event that a complaint is filed. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees will be given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance will be provided in the form of mandatory

DOT Privacy Office - Adjudicated - 05414

annual Security and privacy awareness training as well as Acceptable Rules of Behavior. The FMCSA Security Officer and FMCSA Privacy Officer will conduct regular periodic security and privacy compliance reviews of EDMS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Audit provisions are also established to ensure that EDMS is used appropriately by authorized users and monitored for unauthorized usage. All FMCSA information systems are governed by the FMCSA Rules of Behavior (ROB) for IT Systems. The FMCSA ROB for IT Systems must be read, understood, and signed by each user prior to being authorized to access FMCSA information systems, including EDMS. FMCSA contractors involved in data analysis and research are also required to sign the FMCSA Non-Disclosure Agreement prior to being authorized to access EDMS.

Responsible Official

Charles Medalen
Office of Chief Counsel
Federal Motor Carrier Safety Administration
202-366-1354
charles.medalen@dot.gov

Reviewing Official

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

DOT Privacy Office - Adjudicated - 05141