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

Privacy Impact Assessment (Update)
Coercion of Commercial Motor Vehicle Drivers; Prohibition Final Rule

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

12/2/2015

X Claire W. Barrett

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

Executive Summary

Congress required the Federal Motor Carrier Safety Administration (FMCSA) to ensure that any regulations adopted pursuant to the Motor Carrier Safety Act of 1984 (MCSA), 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 a Final Rule that prohibits 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 is also using the broad authority of the 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 motor carriers that operate CMVs from coercing drivers to violate certain provisions of the Agency's commercial regulations.

The major provisions of this Final Rule include prohibitions of coercion, procedures for drivers to report incidents of coercion to FMCSA, and rules of practice the Agency will follow in response to allegations of coercion. The information required of drivers reporting incidents of coercion to FMCSA 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 requirements in MAP-21. This PIA will be available for public review in the public docket for the Final Rule and on the Department's privacy website at http://www.transportation.gov/privacy.

Reason for the PIA Update

This PIA is being published to update the previous PIA that accompanied the Notice of Proposed Rulemaking (NPRM) on "Coercion of Commercial Motor Vehicle Drivers; Prohibition," published on May 13, 2014 (79 FR 27265), and in support of the Final Rule of the same name published on November 30th (80 FR 74695).

While no fundamental changes were made to the provisions of the NPRM, this revised PIA codifies the privacy protections in place and provides the public with information regarding the Coercion rule and the associated collection, use, and maintenance of PII.

What is a Privacy Impact Assessment?

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

[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).

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

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

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

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

Introduction & Overview

FMCSA adopts 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 HMRs. In addition, the Coercion rulemaking prohibits anyone who operates a CMV in interstate commerce from coercing a driver to violate the commercial regulations. The Coercion rule includes procedures for drivers to report incidents of coercion to FMCSA, rules of practice the Agency will follow in response to such allegations, and penalties that may be imposed on entities found to have coerced drivers. The 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 and final 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 386.12(e) and 390.6(b) allow drivers to present whatever evidence they have to substantiate an allegation of coercion.

Personally Identifiable Information and the Coercion Final Rule

As stated in the Coercion NPRM PIA, 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 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.

FMCSA uses this information to follow up with the driver in order to investigate the complaint.

The Final Rule provides procedural protections and remedies intended to protect drivers from coercion. 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 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 alleging coercion must submit a written complaint to FMCSA's National Consumer Complaint Database (NCCDB) at www.nccdb.fmcsa.dot.gov or the FMCSA Division Administrator for the State where the driver is employed. Information on filing a written complaint may be obtained by calling 1-800-DOT-SAFT (1-800-368-7238). A written complaint must be filed within 90 days after the incident occurred. FMCSA will maintain coercion complaints in the NCCDB. FMCSA will handle these complaints like any other enforcement complaint that results in an investigation. The requirement to investigate is set forth in 49 U.S.C. 31143(a).

FMCSA retrieves coercion complaints from the NCCDB by the complainant's name, and the records are therefore covered by the Privacy Act of 1974. The SORN for the NCCDB (DOT/FMCSA 004 – National Consumer Complaint Database – 75 FR 27051, May 13, 2010) will be revised to cover the collection of information affected by this rule and published in the Federal Register with a request for comment not less than 30 days before the becomes effective. Additionally, the FMCSA will revise the PIA for the NCCDB posted on June 6, 2006, and an updated PIA will be available to the public on the DOT website athttp://www.transportation.gov/privacy.

FMCSA has provided notice to the public through the NPRM published for comment in the Federal Register, the FMCSA website (www.fmcsa.dot.gov), and the Final Rule and accompanying PIA.

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

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

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.

As stated in the Coercion NPRM PIA, FMCSA ensures 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 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 rectified, completed, or amended.

FMCSA has adopted effective and timely procedures to permit each driver to examine his or her PII on file with the Agency 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.

As stated in the NPRM PIA, the authority for the Coercion rulemaking is the MCSA of 1984 (Pub. L. 98-554, Title II, 98 Stat. 2832, October 30, 1984, 49 U.S.C. 31136(a)(1)-(4)), as amended by MAP-21 (Pub. L. 112-141, 126 Stat. 405, 818, July 6, 2012, 49 U.S.C. 31136(a)(5)), 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 about the authorities, consult the Coercion Final Rule.

As stated in the NPRM PIA, FMCSA limits its use of the PII collected as part of the Coercion complaint to the purposes detailed in the NCCDB 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 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).

As stated in the NPRM PIA, CMV drivers filing a complaint are required to submit information about themselves and the reported coercion, as discussed in the Overview section of this PIA. FMCSA uses the information to evaluate the merits of the complaint and obtain further information from the driver. FMCSA has not established a specific form that driver 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 a complaint. Complaints may be initiated by submitting a written complaint to FMCSA's NCCDB at http://www.nccdb.fmcsa.dot.gov or the FMCSA Division Administrator for the State where the driver is employed. Information on filing a written complaint may be obtained by calling 1-800-DOT-SAFT (9-800-368-7238).

The NCCDB system's complaint files are retained in accordance with the provisions of the U.S. National Archives and Records Administration (NARA) SF 115: NI-557-05-13, Item 1. Records of the initial complaint are retained temporarily and destroyed or deleted 36 months after the information has been converted into an electronic medium, backed up, and verified. Master data files of NCCDB are maintained temporarily and deleted 6 years after the end of the calendar year in which a case is closed or when no longer needed for reference, whichever is sooner.

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.

As stated in the NPRM PIA, 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 rulemaking allows authorized safety officials to use personal information to positively identify and contact the driver.

As stated previously in this PIA, the data collected as a result of the coercion complaints will be stored in the NCCDB system. The SORN for the NCCDB (DOT/FMCSA 004 – National Consumer Complaint Database – 75 FR 27051, May 13, 2010) details the routine uses for information stored in the system. In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in NCCDB may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

1. Information may be shared with Federal, State, and local government agencies for the purposes of enforcing the safety of motor carriers and HHG transporters.

2. Information may be shared with the accused party in the course of an investigation if such information is determined to be essential to the furthering the investigation.

If appropriate, additional information regarding the use and disclosure of information collected may be made in accordance with the U.S. Department of Transportation (DOT) Prefatory Statement of General Routine Uses published in the Federal Register on July 20, 2012 (77 FR 42796), under "Prefatory Statement of General Routine Uses" (available at http://www.transportation.gov/privacy).

This SORN will be revised to cover the collection of information affected by this rule and published in the Federal Register with a request for comment not less than 30 days before the becomes effective. As a result of this final rule and a biennial review of the system, the current SORN will be updated to reflect: (1) the addition of coercion complaints to the types of complaints able to be filed in the system, (2) an expansion of the system purpose to include the ability to file coercion complaints, (3) the addition of a routine use to enable information to be shared with the accused party during the investigation of a complaint, and (4) non-substantive changes to clarify previous language contained in the SORN. No changes to the identified routine uses of NCCDB information will be made as a result of the Coercion final rule. While these SORN changes do not alter the privacy risk associated with the NCCDB system, the changes do broaden the scope of the system to enable additional individuals to file coercion complaints with FMCSA. This will in turn increase the number of individuals whose PII is stored in the system.

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).

As stated in the NPRM PIA, FMCSA will maintain the information voluntarily provided by the CMV driver for the purpose of investigating an allegation, and possibly pursuing a case, of coercion against a motor carrier, shipper, receiver or transportation intermediary. The Agency will update the information as necessary and verify if the driver still wishes to continue with the complaint.

The CMV driver reporting coercion provides all information contained in the initial complaint and stored in NCCDB. The driver will typically submit whatever information he or she considers necessary to support the allegation. FMCSA expects the CMV driver to provide correct information, but will also conduct an independent investigation of the alleged coercion. FMCSA can only ensure the confidentiality and integrity of the PII contained in the coercion complaint files once the information is received from the individual and stored in NCCDB.

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 PII collected through a complaint is stored in the NCCDB and the security of the PII is dependent on the security controls in place for the NCCDB. Reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure will protect the PII when stored in the NCCDB.

Physical access to the NCCDB 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 the NCCDB, including PII, is determined by permission levels, and NCCDB 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 NCCDB 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 NCCDB. 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 from NCCDB.

All NCCDB 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 NCCDB. Users must read and sign the ROB acknowledging they understand the stated rules before being authorized to access the system.

The NCCDB have safeguards that protect PII provided to FMCSA. These protections include privacy training provided to FMCSA personnel on the appropriate use of PII. Additionally, FMCSA provides annual security awareness training to FMCSA personnel on system access rights and responsibilities. Role-based privacy and security training is provided to appropriate FMCSA personnel that have significant security and privacy responsibilities.

NCCDB is authorized to operate through the Security Authorization Process under the National Institute of Standards and Technology. After a review of the security and privacy controls, NCCDB was last authorized to operate (ATO) on June 23, 2014. The system is currently in continuous monitoring and one third of the security and privacy controls for the system will be reassessed each year beginning in 2015.

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.

As stated in the NPRM PIA, FMCSA is responsible for training and holding Agency personnel accountable for adhering to the Agency's privacy and security policies and regulations. FMCSA follows the Fair Information Practice Principles as best practices for the protection of information associated with the complaint records held in NCCDB. In addition to these practices, policies and procedures are consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance is provided in the form of mandatory annual Security and

privacy awareness training as well as Acceptable Rules of Behavior (ROB). The FMCSA Security Officer and FMCSA Privacy Officer conduct regular periodic security and privacy compliance reviews of NCCDB 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 established to ensure that NCCDB 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 NCCDB. FMCSA contractors involved in data analysis and research are also required to sign the FMCSA Non-Disclosure Agreement prior to being authorized to access NCCDB.

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