U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

State Compliance Records Enterprise (SCORE) System

Responsible Official

Nikki McDavid
Chief CDL Division
202-366-0831
nikki.mcdavid@dot.gov

Reviewing Official

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The U.S. Department of Transportation's (DOT) Federal Motor Carrier Safety Administration's (FMCSA) core mission is to reduce commercial motor vehicle (CMV) related crashes and fatalities. To further this mission, FMCSA created the State Compliance Records Enterprise (SCORE). SCORE is a web-based system used to track States' implementation of Commercial Drivers' License (CDL) regulations. As part of its State CDL compliance reviews, FMCSA may collect and store Commercial Driver's License Information System (CDLIS) driver records[1] and references to Driver License Numbers (DLNs) in SCORE. The CDLIS driver record is used by FMCSA as evidence of compliance or that there is a problem that a State Driver's Licensing Agency (SDLA) needs to correct. This Privacy Impact Assessment (PIA) provides information about SCORE's collection and use of CDL information.

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.[2]

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*

[1] Documentation uploaded may either reference a Driver License Number or be a CDLIS driver record itself to demonstrate non-compliance.

[2]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).

- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

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

Introduction & System Overview

FMCSA conducts compliance reviews, both comprehensive and focused, of state CDL programs compliance with Parts 383 and 384 of the Federal Motor Carrier Safety Regulations (FMCSRs), specifically. The results of the reviews are documented as compliance findings. Should a state have issues of noncompliance, the SDLAs are required by federal law to submit a Corrective Action Plan (CAP) to FMCSA describing the State's plans to return to compliance. Once the CAPs are completed, the SDLA must work with FMCSA to validate compliance.

FMCSA uses the SCORE application to track state compliance and deficiencies. SCORE also facilitates storage and automated document exchange between SDLAs and FMCSA during compliance reviews. Documents may contain proof of compliance, evidence of non-compliance, CAPs, and certifications issued by the SDLA or FMCSA's review of the state's compliance with CDL regulations.

1.0 Personally Identifiable Information (PII) and SCORE

FMCSA may use CDLIS driver records, or references to the record, as evidence of SDLA non-compliance. Driver License Numbers (DNL) may be included in the documents developed and maintained by both FMCSA and SDLAs.

SDLAs must provide evidence of compliance or that a FMCSA finding was addressed by a corrective action and that the finding was resolved. SDLAs provide the necessary evidence of compliance or the completion of a corrective action by uploading documents directly to the SCORE repository.

Generally, FMCSA does not control the format or content of documents uploaded by SDLAs. As a result, the files submitted and maintained in SCORE may contain:

- Name
- Date of birth
- Social Security Number (SSN)
- Gender
- Height
- Weight
- Eye color

- Driver License Number
- License State-of-Record

SCORE does not contain fields requesting PII. Users are directed not to include PII in free-text fields.

However, for documentation of the State's compliance with the requirement for a lifetime disqualification of drivers who are convicted of committing a serious human trafficking violation, FMCSA will use a prescribed format in its Annual Program Review. The States will be required to provide a list of the CDL numbers with these convictions during the fiscal year. This document will be provided as an attachment and will not be searchable for PII. The purpose of this information is to allow FMCSA to validate that the convictions were made correctly.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[3], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[4].

Transparency

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

Records in SCORE are not retrieved by personal identifiers. Additionally, the purpose of records in SCORE is to document SDLA compliance. Therefore, the Department has determined that SCORE does not constitute a Privacy Act system of records.

FMCSA informs the public that their PII is collected, stored, and used by SCORE through this PIA published on the DOT website. This document identifies the information collection's purpose,

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

[4] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

FMCSA's authority to collect, store, and use the PII, and all uses of the PII collected, stored, and transmitted through SCORE.

The CDLIS database is the authoritative source for CDLIS driver records referenced in SCORE by way of the Driver's License Number. CDLIS records are maintained by SDLAs and the States are responsible for informing individual members of the public of their data management practices, including sharing with the Department of Transportation for compliance and enforcement purposes. Information on CDLIS may be found at https://www.aamva.org/CDLIS/ and in the PIA published at https://transportation.gov/privacy.

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.

State-operated CDLIS databases are the authoritative sources for all driver records found in SCORE. As such, any PII stored in SCORE originates in State-operated CDLIS databases. Information in SCORE is used as evidence of SDLA compliance, findings, or completion of a corrective action.

If SDLAs include records other than those maintained in the State's CDLIS database, that information may be submitted to SCORE. SDLAs are responsible for providing appropriate notice to individuals that their information will be included in the submission to FMCSA.

Because SCORE does not collect information directly from drivers, FMCSA does not provide CDL drivers with any additional notice, options for consent, or options to seek redress. CDLIS State-of-Record are the authoritative source for CDLIS driver records stored in SCORE. CDL drivers who wish to contest the accuracy of their information in a State-operated CDLIS database must direct their redress requests to the applicable SDLA.

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.

FMCSA may store copies of CDLIS driver records from an SDLA in SCORE as part of its compliance review process. These CDLIS driver records are stored for the sole purpose of demonstrating compliance or a problem identified by FMCSA during a compliance review. The use of this information allows the SDLA to locate specific records within their CDLIS database that demonstrate compliance or need remedial action. CDL numbers are not used to retrieve the individual's driver records in SCORE.

SCORE also contains a document repository. This repository allows SDLAs to submit documentation of compliance or reflecting the corrective action taken in response to a compliance review finding. The repository contains both the findings and information of a SDLA's level of compliance with FMCSA regulations. The documents uploaded to SCORE illustrate the SDLA's compliance history. For example, if during a future compliance review FMCSA identified a finding for a violation that was previously cited during a review, the documentation contained in SCORE would demonstrate that the SDLA has repeatedly committed specific violations over a period of time.

SCORE does not collect any data directly from the public. Users of SCORE cannot use PII to retrieve the driver's information. Instead, the FMCSA or SDLA queries whether the SDLA has compliance findings. Once the findings are found, the user may open the documents associated with the finding to discover details. If a driver's record is associated with the documentation of compliance or a finding, the SDLA may then use CDLIS to locate the specific driver record to correct the problem and close the finding. All PII contained in the system is maintained to either provide an example of a compliance or a specific finding identified in the compliance review or to demonstrate that a SDLA took corrective action.

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.

It is important to note that there is no connection or integration of SCORE into CDLIS or vice versa. Any information acquired from the CDLIS database must be acquired through a direct connection to CDLIS via authentication outside of SCORE. FMCSA may reference DLN which are stored in the CDLIS database to identify compliance or the specific issues that SDLA needs to correct. References to the DLN or an upload of the CDLIS record document the compliance or instance of non-compliance on the part of the State. Once these driver records are identified, the SDLA can take corrective action to resolve the finding.

Authorized State and FMCSA users may upload documents to the system that contain PII. These documents, which are used to document compliance or support a finding or remedial action are stored in the SCORE document repository, and potentially contain any information associated with a CDL driver that the SDLA feels shows compliance or supports of closing the finding. FMCSA does not specify what documents or information the individual SDLAs must provide (or not provide) to demonstrate that corrective action has been taken.

The records within SCORE, which contain summary reports on field activities, are retained for 20 years unless needed longer for administrative, legal, audit, or other operational purposes in

accordance with the provisions of the NARA approved FMCSA Records Disposition Schedule: NI-557-05-6, Item 7B,4.

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.

PII in SCORE may be included as an illustration of compliance or non-compliant documentation identified during FMCSA's compliance reviews of SDLA CDL programs. Users of SCORE cannot use PII, such as the DLN, to retrieve a specific driver's information. Users can query whether a SDLA has findings of non-compliance, and to provide details about these specific findings for each SDLA. This then allows the individual SDLAs to locate the specific driver record in their own database and take corrective action.

SCORE has a document repository that allows FMCSA users to upload documents as evidence of compliance or non-compliance and SDLA users to upload documents as evidence of remedial actions. While FMCSA will upload individual DLN or CDLIS Records to enable the SDLA to locate compliant or non-compliant records, FMCSA does not control the information that the SDLA submits as evidence of remediation.

The information contained within SCORE is not shared with any other Agency or Organization. No other FMCSA programs are provided access to the information in SCORE.

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).

All information received from the individual SDLAs and stored in SCORE is provided by CDLIS. There are open fields that allow text and the upload of files. Notices have been added to SCORE to caution users to avoid posting PII or sensitive information where those fields exist in the system. This information includes driver records that support the specific SDLA's CDL compliance review compliance, findings, and finding close-out actions (remediations).

SDLAs upload all information considered necessary to document compliance or present their case that the finding cited in the compliance review has been corrected. FMCSA relies upon the SDLA to ensure that the information it uploads is correct.

Only authorized personnel are provided access to the SCORE system. Authorized users may be a representative from that state's SDLA, the designated FMCSA Division personnel in charge of Compliance Reviews for that region, and a select group of Headquarters personnel.

SCORE relies on the SDLAs for the quality and integrity of the CDLIS data, as the information is collected, owned, and maintained by each individual SDLAs. As FMCSA is not the owner of the data, it can only ensure the confidentiality and integrity of PII contained in SCORE once the information is received from the individual SDLAs.

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.

The FMCSA Office of Information Technology has provided guidance to assist the contractor in protecting the confidentiality, integrity, and availability of information, including PII, stored in or retrieved by SCORE. FMCSA implements security and privacy requirements in SCORE accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53, Privacy and Security Controls for Federal Information Systems and conducts regular assessments of their implementation.

The data center in which SCORE operates is a restricted access facility. Physical access to the SCORE system is limited to appropriate personnel through applicable physical security requirements of the agency. FMCSA and contract support personnel with physical access have all passed DOT background checks.

All information stored in or retrieved by SCORE is protected from unauthorized access through appropriate administrative, physical, and technical safeguards. Electronic files are stored in databases secured by passwords, firewalls, and operating systems to which only authorized personnel with a "need to know" have access. The SCORE login screen warns users of penalties for unauthorized access, and all access to information retrieved by SCORE is logged and monitored.

The SCORE document repository is only accessible to authorized FMCSA and State users. SCORE is designed for role-based access for FMCSA employees and State users with appropriate levels of access. Documents are stored on approved service provide servers, with dedicated disk space and servers. The servers have restricted access requiring one of two methods of access; 1. State user (and/or non-PIV holders) must access the system through an approved Two-Factor Authentication service approved by DOT; 2. Federal employees utilizing PIV enabled access. The information/data is physically encrypted at rest to prevent unauthorized access to the data.

User access controls have been developed to ensure that the number of individuals with access to restricted information stored in or retrieved by SCORE is kept to a minimum and is limited to only those individuals with a "need to know." Access to information in SCORE, including PII, is strictly limited to specified authorized personnel and is determined by permission levels. User accounts are assigned access rights based on the roles and responsibilities of the individual user. Individuals

requesting access to SCORE must submit some personal information (e.g., name, contact information, and other related information) to FMCSA as part of the authorization process. HTTPS protocols are used when accessing the data when it is in motion, and the disk is encrypted when at rest.

Access to SCORE is via Two-Factor-Authentication, either by PIV or Login.gov. 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 NIST Special Publication (SP) 800-53 Rev. 4, Recommended 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 SCORE.

All SCORE users are required to acknowledge understanding 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 SCORE. The general public does not have access to SCORE.

Accountability and Auditing

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

FMCSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to FMCSA privacy and security policies and regulations. FMCSA will follow the Fair Information Practice Principles as best practices for the protection of information associated with the SCORE system. 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 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. The FMCSA Security Officer and FMCSA Privacy Officer will conduct regular periodic security and privacy compliance reviews of SCORE consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Audits are performed to ensure that SCORE 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. SCORE administrators with the OCIO's office may revoke access to SCORE if a user is not in compliance with the ROB for IT Systems. The FMCSA ROB for IT Systems must be read, acknowledged as understood, and signed by each user prior to being authorized to access FMCSA information systems, including SCORE. FMCSA contractors

involved in data analysis and research are also required to sign the FMCSA Non-Disclosure Agreement prior to being authorized to access SCORE.

Responsible Official

Nikki McDavid
Chief CDL Division
202-366-0831
nikki.mcdavid@dot.gov

Approval and Signature

Karyn Gorman
Actin Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov