U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)
SafeSpect Pilot/Proof of Concept

Responsible Official

John Lohmeyer
Email: John.Lohmeyer@dot.gov
Phone Number: 202-366-0493

Reviewing Official

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

March 18, 2022

Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is an Operating Administration (OA) within the U.S. Department of Transportation (DOT) with a core mission to reduce commercial motor vehicle-related crashes and fatalities. To further this mission, FMCSA developed the SafeSpect pilot/proof of concept to ensure compliance with the Federal Motor Carrier Safety Regulations (FMCSR) and Hazardous Materials Regulations (HMR). SafeSpect is FMCSA's new system for collecting data related to the inspection of a commercial motor vehicle (CMV), the motor carrier, and its driver. These inspections follow a set of standards set by an alliance of Federal and State enforcement personnel and the motor carrier industry. These inspections determine the roadworthiness of the vehicle in operation and the driver's eligibility and fitness to drive.

FMCSA is publishing this Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002 to address the privacy risks associated with the SafeSpect pilot/proof of concept and its collection and use of Personally Identifiable Information (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]

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;*

[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).

- *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 & System Overview

SafeSpect is FMCSA's new system for collecting data related to the inspection of a commercial motor vehicle (CMV), the motor carrier, and its driver to ensure compliance with the Federal Motor Carrier Safety Regulations (FMCSR) and Hazardous Materials Regulations (HMR). The system collects the name and address of the motor carrier, the manufacturer, model year, VIN, and state registration of the vehicles inspected, the location and date and time of the inspection, driver information, and citations of violations noted at the scene. The collection of this information is necessary to validate the status of the driver's license and compliance with the Drug and Alcohol Clearinghouse.

The current launch of SafeSpect is a pilot/proof-of-concept version. The pilot consists of approximately 20-25 field users, including State and local enforcement officials, and is set to launch March 21, 2022. In the long run, SafeSpect will replace FMCSA's Aspen and SAFETYNET systems and parts of SAFER and MCMIS. This is done to bring these applications up to current technology standards using a web-based user interface to conduct business in more efficient manner, making the system independent of the device or operating system being used. Both Aspen and SAFETYNET are still reliable, but they require a specific operating system, and SAFETYNET requires substantial hardware for its application and database. Furthermore, the current technology requires transferring data from Aspen to SAFER to SAFETYNET to MCMIS, which at any point could cause data loss and data corruption.

SafeSpect allows certified State and Federal inspectors to begin an inspection with any current web browser, and the date and time are automatically entered. The system presents the inspector's current location on a map for the inspector to validate. The location is then matched to a known fixed location or a roadway route and mile point. Meanwhile the inspector has searched the motor carrier's information by a lookup against FMCSA's authoritative motor carrier census, and the system returns the motor carrier's status and safety performance information. The inspector will enter the vehicle's VIN and the system performs a search and returns the vehicle manufacturer, model year, and validate the VIN for accuracy. Upon input of the driver's license number and state, the system queries the status of the commercial driver's license, the record of the driver's medical card, and the status of the driver in the Drug and Alcohol Clearinghouse. The inspector then does a physical inspection of the vehicle noting any violations found. Violations are noted

according to a set list of potential violations using a standard description to which the inspector only adds specifics. Violations have specific business rules to ensure accuracy of the violation cited. Once completed, the inspector can then add any specific notes to the record and submit it to the database.

At that point, a user designated as a "reviewer" reviews the data submitted and accepts or rejects the inspection. When accepted, the inspection is available in FMCSA's existing MCMIS database for use in compliance algorithms and safety ratings.

Personally Identifiable Information (PII) and SafeSpect

The system collects and processes driver information that could include the following PII:

- Driver Name (First, Middle Initial, Last name)
- Date of Birth
- State of issue
- Driver's license number
- Vehicle identification number

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[2], 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[3].

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.

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

The FMCSA does not secretly collect or store PII. The FMCSA clearly discloses its policies and practices concerning the PII collected and held associated with the implementation of this pilot/proof of concept. The FMCSA provides notice to individuals through this PIA published on the DOT's privacy program's website at www.transportation.gov/privacy. This document identifies the information collection's purpose, FMCSA's authority to store and use the PII, and all uses of the PII stored and transmitted through the SafeSpect.

Records in SafeSpect are retrieved by the individual's name and other personal identifiers and are subject to the provisions of the Privacy Act. FMCSA maintains these records in accordance with the Department's published System of Records Notice (SORN), DOT/FMCSA 001, Motor Carrier Management Information System (MCMIS) System of Records - Federal Register, Vol. 78, No. 186, September 25, 2013. The SORN provides notice as to the conditions of disclosure and FMCSA's routine uses for the information collected in the system. The SORN also requires that any dissemination of information maintained within the system be compatible with the purpose for which the information was originally collected. In addition, FMCSA provided periodic updates at industry outreach events related to the SafeSpect.

The publication of this PIA further demonstrates FMCSA's commitment to providing appropriate transparency into the SafeSpect. This PIA is available to the public on the DOT website at http://www.dot.gov/privacy.

Individual Participation and Redress

DOT provides 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 they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

FMCSA ensures that individuals have the right to (a) obtain confirmation of whether or not FMCSA has PII relating to him or her; (b) access the PII related to him or her within a reasonable time, cost, and manner and in a form that is readily intelligible to the individual; (c) obtain an explanation if a request made under (a) and (b) is denied and challenge such denial; and (d) challenge PII relating to him or her and, if the challenge is successful, have the data erased, rectified, completed, or amended.

The FMCSA clearly discloses its policies and practices concerning the PII collected and held associated with the implementation of this pilot/proof of concept.

During this pilot/proof of concept, 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 record must be in writing (either handwritten or typed), and may be mailed, faxed, or emailed. 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 FOIA/PA program may be found on the DOT website (https://www.transportation.gov/privacy).

MCMIS is the authoritative source of information in SafeSpect. Under the provisions of the Privacy Act and Freedom of Information Act (FOIA), individuals may request searches of SafeSpect to determine if any records have been added that may pertain to them. This is accomplished by sending a written request directly to:

Federal Motor Carrier Safety Administration

U.S. Department of Transportation

Attn: FOIA Team MC-MMI

1200 New Jersey Avenue SE

Washington, DC 20590

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 it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

During this pilot/proof of concept, SafeSpect collects CMV driver, carrier, and shipper representative PII along with inspection information. This information is uploaded to MCMIS and used to track CMV safety-related data. Once the information has been uploaded to MCMIS, companies, agencies, individuals, and other authorized organizations with access to MCMIS are able to view the information to help enhance truck/bus driver safety. FMCSA maintains SafeSpect in accordance with 49 U.S.C. 31136(e), Motor Carrier Safety Act of 1984 and 49 U.S.C. 31315, Transportation Efficiency Act for the 21st Century, TEA–21.

State and local enforcement officials use SafetSpect to search for truck driver history, review inspection results, record and track inspection data, research compliance issues, and contact appropriate individuals or companies/organizations to request additional information regarding the inspection or take compliance action.

SafeSpect is used to collect records of the safety performance of interstate carriers and hazardous materials shippers that are subject to the Federal Motor Carrier Safety Regulations (FMCSR) or Federal Hazardous Material Regulations (HMRs). The inspection information containing the CMV driver and carrier/shipper representative PII is instrumental in determining the safety performance of the interstate carriers and hazardous materials shippers that are subject to the FMCSRs and HMRs.

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.

SafeSpect collects CMV driver and carrier inspection information. This information is uploaded to MCMIS and used to track CMV safety-related data. Once the information has been uploaded to MCMIS, companies, agencies, individuals, and other authorized organizations with access to MCMIS are able to view the information to help enhance truck/bus driver safety. FMCSA maintains SafeSpect in accordance with 49 U.S.C. 31136(e), Motor Carrier Safety Act of 1984 and 49 U.S.C. 31315, Transportation Efficiency Act for the 21st Century, TEA–21.

During this pilot/proof of concept, SafeSpect records are managed in accordance with the MCMIS retention schedule. MCMIS records are retained and destroyed in accordance with applicable NARA retention schedule N1-557-05-07 Item #5. The master backup tape is designated for deletion under this retention schedule when 5 years old, when no longer needed, or when information is superseded or becomes obsolete, whichever is sooner.

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

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 minimizes its data collection to that necessary to meet the authorized business purpose and mission of the Agency. The system collects the name and address of the motor carrier, the manufacturer, model year, VIN, and state registration of the vehicles inspected, the location and date and time of the inspection, driver information, and citations of violations noted at the scene. The collection of this information is necessary to validate the status of the driver's license, and compliance with the Drug and Alcohol Clearinghouse.

SafeSpect is not the authoritative source for the PII data, PII data is collected from other FMCSA systems for statistical analysis of historical data. It will be used by Federal and State enforcement personnel, as well as the motor carrier industry, insurance companies, and the public.

During this pilot/proof of concept, SafeSpect will receive information from the following systems:

- Motor Carrier registration information and status from MCMIS;
- Motor Carrier insurance and operating authority status from L&I;
- Records of previous inspections of the Motor Carrier, the Vehicle, or the Driver from SAFER;
- Vehicle configuration information from NHTSA's VPIC;
- Commercial Driver License status from CDLIS;
- Driver eligibility status from the Drug and Alcohol Clearinghouse;
- Intermodal Equipment Provider registration status from the Global Intermodel Equipment Registry (GIER).

SafeSpect will send completed inspection data to the SAFER and MCMIS environments. The Analysis and Insurance system will read inspection data elements for analysis.

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 ensures that the collection, use, and maintenance of PII for implementing the SafeSpect is relevant to the purposes for which the data is to be used and, to the extent necessary for those purposes, it is accurate, complete, and up-to-date. The Agency has a variety of protocols in place to validate and verify that the information collected in the SafeSpect is associated with the correct person to ensure the accuracy and reliability of the data collected.

SafeSpect provides some internal data quality and completeness checks. The users participating in the pilot test are responsible for inputting correct information for their drivers. In addition, the inspection data is received from other MCMIS and SAFETYNET. Therefore, it is the responsibility of the drivers and state official to ensure accuracy.

Security

DOT shall implement administrative, technical, and physical measures to 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.

PII is protected by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and

practices required for Federal information systems under the Federal Information System Management Act (FISMA) and are detailed in 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, and Recommended Security Controls for Federal Information Systems and Organizations, dated April 2013. The FMCSA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. All required authorizations (e.g., to operate, analysis) were established before the SafeSpect was deployed. These safeguards are designed to achieve the following objectives:

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

Records in the SafeSpect are safeguarded in accordance with applicable rules and policies, including all applicable DOT and FMCSA automated systems security and access policies. Strict controls are imposed on all DOT/FMCSA systems to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in the SafeSpect is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. All records that are stored in the SafeSpect will be protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the SafeSpect is logged and monitored.

SafeSpect maintains an auditing function that tracks all user activities in relation to data, including access and modification. Through technical controls including firewalls, intrusion detection, encryption, access control lists, and other security methods, FMCSA prevents unauthorized access to data stored in the SafeSpect. These controls meet federally mandated information assurance and privacy requirements.

All FMCSA personnel and FMCSA contractors completes security and privacy awareness training and role-based training offered by DOT/FMCSA. This allows individuals with varying roles to understand and retain knowledge of how to properly and securely act in situations where they may use PII while performing their duties. No user is allowed access to SafeSpect prior to receiving the necessary clearances and security and privacy training as required by DOT/FMCSA.

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 FMCSA employees and contractors accountable for adhering to FMCSA privacy and security policies and regulations. FMCSA follows the Fair Information Practice Principles as best practices for the protection of PII associated with the implementation of the SafeSpect pilot/proof of concept version. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees is given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training as well as the DOT/FMCSA Rules of Behavior. The FMCSA Information System Security Officer and FMCSA Privacy Officer conducts periodic security and privacy compliance reviews of the SafeSpect consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Responsible Official

John Lohmeyer
System Owner
Transportation Specialist, State Programs Division

Prepared by: Pam Gosier-Cox FMCSA Privacy Officer

Approval and Signature

Karyn Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer