U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA) SAFETYNET System)

Responsible Official

James Vasser
SAFETYNET System Owner
Jamie.Vasser@dot.gov

Reviewing Official

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

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
Date: 2021.03.16 13:37:18 -04'00'

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-related crashes and fatalities. To further this mission, FMCSA created SAFETYNET ; designed to manage and provide appropriate access for authorized users to crash data, roadside inspection history and data, and motor carrier and shipper identification information. SAFETYNET enables federal and state enforcement officials to access updated motor carrier, commercial motor vehicle (CMV), and CMV driver information collected in the field.

This Privacy Impact Assessment (PIA) was conducted to address privacy risks associated with the SAFETYNET system and its collection and use of Personally Identifiable Information (PII).

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;*
- *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.

[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 M-03-22 dated September 26, 2003).

Introduction & System Overview

The Federal Motor Carrier Safety Administration (FMCSA), within the Department of Transportation (DOT), has been given the responsibility to reduce crashes, injuries, and fatalities involving large trucks and buses. Since a first step in reducing accidents is to understand them, FMCSA collects and maintains commercial vehicle safety data, as well as a national inventory of motor carriers and shippers subject to the Federal Motor Carrier Safety Regulations (FMCSRs) and Hazardous Materials Regulations (HMRs). SAFETYNET supports the effective and efficient use of this information to support FMCSA analysis and safety programs.

SAFETYNET is a distributed information management system, consisting of a centralized database and desktop applications deployed in the field, that supports federal and state programs that monitor the safety performance of interstate and intrastate commercial motor carriers. The system contains census information for approximately 2.5 million active and inactive motor carriers and hazardous material shippers and receives over 3 million new inspection records pertaining to the same. SAFETYNET also includes information on freight forwarders and property brokers registered with FMCSA.

SAFETYNET is interconnected to and shares information with the Motor Carrier Management Information System (MCMIS), Safety and Fitness Electronic Records (SAFER), and Aspen. MCMIS is the primary repository for FMCSA inspection, crash, compliance review, safety audit, and registration information. SAFETYNET uploads safety performance information concerning motor carriers and CMV drivers from FMCSA field offices and state agencies to MCMIS. SAFETYNET forwards inspection reports received from FMCSA field offices and state agencies to SAFER, a data sharing system used by roadside inspectors to select CMVs and/or CMV drivers for inspection, for processing. SAFETYNET receives motor carrier snapshots, updated registration information, and compiled safety fitness ratings from SAFER for dissemination to FMCSA field offices and state agencies. Aspen is an FMCSA desktop application used by authorized federal and state officials to collect roadside inspection information and transmit this information to other systems, including SAFETYNET.

Federal, state, and local law enforcement officials transmit roadside safety inspection and crash investigation information to SAFETYNET through SAFETYNET desktop applications. SAFETYNET may also be used to generate activity reports, analyze data, and provide updates to motor carrier information.

The FMCSA and other users access SAFETYNET data and functionality to complete inspections, track issues and trends, take non-compliance actions, and create reports from crash and inspection data.

SAFETYNET maintains records that include commercial driver PII received from designated State officials that were collected on paper forms, but which State data entry representatives enter into the system. Data is also entered via electronic data submissions that are directly uploaded into SAFETYNET. SAFETYNET feeds data into the Motor Carrier Management Information Systems (MCMIS), which is a separate system of records.

SAFETYNET facilitates the updating and processing of motor carrier, commercial motor vehicle (CMV), and CMV driver information collected in the field and the dissemination of this information to federal and state enforcement officials. SAFETYNET provides federal and state enforcement officials with the following types of information:

- **Carrier Census Information**—Includes general information maintained on motor carriers and their operations (USDOT Number, company name and location, types of CMVs, number of drivers, commodities transported, etc.)
- **Compliance Reviews and Rating Information**—Includes compliance reviews of motor carrier operations, safety performance, and adherence to federal and state regulations, which are then used by other FMCSA systems to generate safety fitness ratings for motor carriers
- **Inspection Information**—Includes roadside inspection records on CMVs and CMV drivers and documents safety violations related to CMVs, CMV drivers, and hazardous materials
- **Crash Information**—Includes information collected and maintained by individual states on recordable motor carrier crashes, such as date, time, and location of crash; weather and road surface conditions; investigating agency; vehicle crash data recorder identification; motor carrier identification; driver name and license number; and crash outcome (i.e., number of people injured or killed)
- **Complaint Information**—Includes records of complaints received by federal and state agencies from various sources concerning motor carriers, CMVs, and CMV drivers
- **Assignment Information**—Includes actionable safety investigation cases assigned to federal and state inspectors.

Personally Identifiable Information (PII) and SAFETYNET

SAFETYNET contains PII such as truck/bus driver name, Employer Identification Number (EIN), driver's license number, and date of birth, as well as driver and company contact information, and vehicle identification number. SAFETYNET also collects PII from sole proprietor-drivers (owner-operators) of commercial motor carriers. Sole proprietorships are owned and run by one individual, and no legal distinction between the owner and the business exists. The PII collected from sole proprietors (also known as owner-operators) may include name, personal address and phone number, date of birth, driver license number and issuing state, and SSN if the owner-operator uses his or her SSN as the Employer Identification Number (EIN).

FMCSA receives these data from designated State officials. The data may be entered by state data entry representatives, or imported from external data collection systems. No matter how received, the information is then uploaded to MCMIS via secure file transfer protocol (SFTP).

Only designated State and local enforcement officials have access to PII maintained in SAFETYNET. SAFETYNET interfaces and sends data, including PII, to the FMCSA's central repository, MCMIS. MCMIS shares some PII, including data that comes from SAFETYNET, with appropriate individuals and organizations. Please refer to the MCMIS Privacy Impact Assessment published on the DOT Privacy website (http://www.dot.gov/individuals/privacy/privacy-impact-assessments) for additional details about the MCMIS system.SAFETYNET requires user IDs and passwords. In order to manage access and audit functions, and ensure approprate permissions based upon the individual's job role, the FMCSA collects name, contact information, organization information, and other related information. The User Name is also used internally for display on SAFETYNET-generated reports. Similarly, the organization name and address is used in system-generated letters.

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.3i, 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.

SAFETYNET contains carrier census, safety performance, driver history, and compliance information for CMV drivers commercial carrier and shipper representatives. These individuals are required by law to provide PII as part of the inspection and crash data collection process and SAFETYNET does not provide additional notice or options for consent. In addition, the system also contains first and last name of State and local officials who require access to SAFETYNET in performance of their jobs, as well as their agency's contact information. All data in SAFETYNET is either imported from external data collection systems, or in a very few instances, keyed in from paper forms submitted to State enforcement agencies by that agency's personnel or other state and local agencies within that state.

Individuals are informed of the existence of SAFETYNET on the FMCSA website (https://www.fmcsa.dot.gov/mission/information-systems/information-systems) which provides an overview of all IT systems used by the agency.

Notice is also provided to individuals through the Privacy Act System of Records Notice (SORN) for SAFETYNET published in the Federal Register (DOT/FMCSA 006 – SAFETYNET, 71 FR 68884, November 28, 2006). The SAFETYNET SORN is available to the public on the DOT Privacy Office website and from the Federal Register (http://www.gpo.gov/fdsys/pkg/FR-2006-11-28/pdf/E6-20115.pdf). These documents identify the information collection's purpose, FMCSA's authority to collect, store, and use the PII, and all uses of the PII collected, stored, and transmitted through SAFETYNET.

Finally, FMCSA informs individuals that their PII will be collected, stored, and used by SAFETYNET through this Privacy Impact Assessment published on the DOT website. The SAFETYNET PIA is available to the public at http://www.dot.gov/individuals/privacy/privacy-impact-assessments.

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.

As part of the inspection and crash data collection process, CMV drivers and carrier and shipper representatives are required by law to provide their personal information to FMCSA. Information is collected directly from individuals and then entered into SAFETYNET after the inspection or crash. SAFETYNET does not provide additional options for indiviudals to agree to the collection or use of their information.

While FMCSA does not provide redress to individuals directly through SAFETYNET, the individual can request FMCSA-collected data be modified through the DataQs process and the change requested may be implemented in SAFETYNET. FMCSA provides redress for individuals through both its MCMIS and DataQs systems.

Individuals may bypass SAFETYNETT by updating their data in MCMIS, the authoritative source for FMCSA inspection, crash, compliance review, safety audit, and registration information. Individuals can log into the MCMIS website using their PIN number, and update the information that is stored, including any PII data. Motor carriers also currently have the option of filling-out an updated MCS-150 form and mailing to FMCSA-HQ to update or change their information.

The DataQs system (https://dataqs.fmcsa.dot.gov/login.asp) is an electronic means for filing concerns about federal and state data released to the public by FMCSA. Individuals can use DataQs to challenge information included in their records within FMCSA Systems. Motor carriers, state agencies, and FMCSA offices can use DataQs to challenge information concerning crashes, inspections, compliance reviews, safety audits, enforcement actions, vehicle registrations, operating authorities, insurance policies, and consumer complaints stored in any FMCSA system, including SAFETYNET. After a challenge has been submitted, DataQs automatically forwards the challenge to the appropriate office for resolution and allows the party that submitted the challenge to monitor its status. If the information is corrected as a result of the challenge, the change will be made in SAFETYNET. MCMIS will then receive the changed information through an upload.

DataQs cannot be used to challenge safety ratings or civil actions managed under 49 CFR 385.15 (Administrative Review) or 49 CFR 385.17 (Change to Safety Rating Based upon Corrective Actions). Any challenges to information provided by state agencies must be resolved by the appropriate state agency.

Under the provisions of the Privacy Act and Freedom of Information Act (FOIA), individuals may request searches of SAFETYNET or MCMIS 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
Attn: FOIA Team MC-MMI
1200 New Jersey Avenue SE
Washington, DC 20590

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.

SAFETYNET collects CMV driver, carrier, and shipper representative PII along with inspection and crash 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 SAFETYNET 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.

For individuals with access to SAFETYNET, the FMCSA also collects the PII necessary to associate these individuals with user-created user IDs and passwords in order to authenticate users, assign roles, and restrict permissions.

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

SAFETYNET 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). SAFETYNET also contains information on intrastate carriers (carriers who collect, deliver, or transfer commodities within state boundaries only) that are registered with a State that implements SAFETYNET.The inspection and crash related 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. This data is used for analysis at the state level. A large subset of information, collected locally using the SAFETYNET desktop applications during an inspection or crash investigation, is uploaded to MCMIS . Information collected by other States, and the centralized Federal systems, are distributed to the SAFETYNET desktop applications deployed in the field.

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)*

The FMCSA minimizes its data collection to that necessary to meet the authorized business purpose and mission of the Agency. FMCSA only uses and retains data that are relevant and necessary for the purpose of SAFETYNET. As part of the inspection and crash data collection process, CMV drivers and carrier and shipper representatives are required by law to provide their personal information to FMCSA. All information fields collected have been determined by FMCSA to be necessary to complete inspections, track issues and trends, take non-compliance actions, and create reports from crash and inspection data.

SAFETYNET retains and disposes of information in accordance with the approved National Archives and Records Administration (NARA) records retention schedule, DAA-0557-2015-0009, which states that all master data files are maintained as temporary files that are destroyed or deleted three (3) years after the database is deleted or when the file is no longer needed for reference, audit and administrative, legal or 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.

SAFETYNET 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 Hazardous Materials Regulations (HMR). The following entities have access to SAFETYNET for specific uses:

- **Federal and State Enforcement Officials** - Users record crashes and compliance activities, perform research associated with safety compliance, contact individuals associated with crash or compliance activities, and create reports to analyze trends.
- **FMCSA Employees and Contractors** - FMCSA users utilize SAFETYNET data to identify trends in crashes and compliance activities, monitor and take compliance actions, and create reports.
- **FMCSA Employees and Contractors** (System administrators and developers) have appropriate access to SAFETYNET to perform their assigned roles and responsibilities (development and maintenance of the system).

As allowed by law, FMCSA may also share PII in SAFETYNET with other federal agencies to assist with national security or other compliance activities. The FMCSA evaluates each request on an individual basis and oversees the process to ensure all Privacy Act procedures are followed.

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).

The FMCSA ensures that the collection, use, and maintenance of information collected for operating the SAFETYNET system is relevant to the purposes for which it is to be used and, to the extent necessary for those purposes; it is accurate, complete, and up-to-date.

Individuals who provide their information are responsible for ensuring that the information provided is accurate when provided to law enforcement and licensing agencies. State police departments and other officials, are responsible for inputting correct information. Aspen (a subsystem of FCMSA Service Centers as discussed on page 3 within the System Overview section) ensures the integrity of data found in SAFETYNET. When an inspection is completed and verified in Aspen, the system's data checks ensure that the record is complete when it is sent to SAFETYNET. If Aspen determines that the inspection record is missing core or required data elements, then SAFETYNET will reject the uploaded information. SAFETYNET and Aspen must be in synch version wise for this process to occur. SAFETYNET administrators also have numerous default logs and reports that are used for editing inspection and violation reports or reporting anomalies with its data.

Individuals must submit PII directly to the FMCSA Program Office in order to obtain access to SAFETYNET. Program Office users may contact their approving supervisor through phone or email to request corrections to submitted information. Individuals who provide PII to FMCSA are responsible for the accuracy of the information submitted.

The redress process described in the Individual Participation and Redress section is a mechanism to maintain and improve accuracy of information.

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.

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, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013. FMCSA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. 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 SAFETYNET 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 the computer system containing the records in the SAFETYNET 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 and permissions. All records in the SAFETYNET system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the SAFETYNET system is logged and monitored.

Logical access controls restricts users of the SAFETYNET. These controls are guided by the principles of least privilege and need to know. Role-based user accounts are created with specific job functions allowing only authorized accesses, which are necessary to accomplish assigned tasks in accordance with compelling operational needs and business functions of the SAFETYNET system. Any changes to user roles required approval of the System Manager.

SAFETYNET 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 list, and other security methods; FMCSA prevents unauthorized access to data stored in the SAFETYNET system. These controls meet Federally mandated information assurance and privacy requirements.

FMCSA personnel and FMCSA contractors are required to attend security and privacy awareness training and role-based training offered by DOT/FMCSA. This training allows individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly and securely act in situations where they may use PII in the course of performing their duties. No access will be allowed to the SAFETYNET prior to receiving the necessary clearances and security and privacy training as required by DOT/FMCSA. All users at the federal and state level 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 SAFETYNET.

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 follows the Fair Information Principles as best practices for the protection of information associated with the SAFETYNET system. 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 DOT/FMCSA Rules of Behavior. The FMCSA Security Officer and FMCSA Privacy Officer conduct regular periodic security and privacy compliance reviews of SAFETYNET consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

James Vasser
SAFETYNET System Owner

Approval

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