U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

DataQs System

Responsible Official

Scott Valentine, FMCSA-MC-RRA
DataQs Business Owner & Data Quality Program Manager
Scott.Valentine@dot.gov
(202) 366-4869

Reviewing Official

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

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 created the DataQs web-based system (https://dataqs.fmcsa.dot.gov/) to collect and maintain records on all users who submit requests to review federal and state data released to the public concerning: crashes, inspections, compliance reviews, safety audits, enforcement actions, vehicle registrations, operating authorities, insurance policies, and consumer complaints. The system also accepts the Crash Preventability Determination Program requests and the Drug and Alcohol Clearinghouse petitions.

This Privacy Impact Assessment (PIA) is conducted in accordance with the E-Government Act of 2002 and is necessary to provide information regarding the DataQs system and its collection and use of Personally Identifiable Information (PII) as well as to provide information regarding the cloud infrastructure in which the system is hosted.

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:

[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).

- *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 & System Overview

The mission of the FMCSA is to reduce crashes, injuries, and fatalities involving large trucks and buses. To further this mission, FMCSA created DataQs to satisfy the requirements of the Information Quality Act (Section 515 of Public Law 106-554) by implementing the Administration's core principle of an open and transparent Federal Government. DataQs (https://dataqs.fmcsa.dot.gov) is an electronic means for submitting "Requests for Data Review (RDR)" or "Inspection Report Request (IRR)" for federal and state data released to the public by FMCSA.

Commercial Motor Vehicle (CMV) drivers, motor carriers, federal and state enforcement officials, and the general public can use DataQs to request and respond to reviews of the accuracy of information, and subsequent data correction concerning crashes, inspections, compliance reviews, safety audits, enforcement actions, vehicle registrations, operating authorities, insurance policies, and consumer complaints maintained by FMCSA, other federal agencies, and state agencies released to the public by FMCSA. Users can also file Crash Preventability Determination Program requests and Drug and Alcohol Clearinghouse petitions.

Individuals requesting data corrections must create an account in DataQs, which requires the provision of the individual's name, address, phone number, and email address. Additionally, individuals must establish a username and password used in conjunction with their system ID to access the DataQs system on subsequent visits, and security questions in case they forget their passwords.

Employees representing a motor carrier can request access to DataQs through the FMCSA Portal (https://portal.fmcsa.dot.gov). Each motor carrier has an Organization Coordinator assigned within their company to approve or deny access of a requestor to that company's information contained within FMCSA systems. Once authenticated, the Portal shares information with DataQs to either create or update an associated profile.

Once registered with DataQs, individuals may initiate an RDR, IRR, or petition and provide supplemental information and supporting documentation as necessary. FMCSA provides limits on document formats and file-size uploaded by the users as evidence to support a request. Because all documentation uploaded to DataQs is up to the user's discretion, the supporting documents may also contain PII such as a name or driver's license number. Users of DataQs can monitor the progress of their data correction request, communicate with case managers, and submit additional information as needed.

Individuals consent to the collection, use, dissemination, and retention of their PII by registering with DataQs.

This system will be included in DOT's inventory of record systems.

DataQs registrants may dispute information contained in the core FMCSA systems:

- Analysis and Information (A&I) Online
- Enforcement Management Information System (EMIS)
- Licensing & Insurance (L&I)
- Motor Carrier Management Information System (MCMIS)
- Performance and Registration Information Systems Management (PRISM)
- Query Central (QC)
- Safety and Fitness Electronic Records (SAFER)
- SAFETYNET
- National Consumer Complaints Database (NCCDB)
- Drug & Alcohol Clearinghouse
- Pre-Employment Screening Program website

After an RDR, IRR, or petition is submitted, DataQs automatically forwards the request to the appropriate office for resolution and allows the party that submitted the request to monitor its status. Requests are routed back to the state agency that submitted the information or to the FMCSA program office responsible. Once requests are received by the appropriate office, they are retrieved from a 'to do' grid which may be filtered by registration information (e.g., last name) or the date on which the report was submitted. Any challenges to data provided by state agencies must be resolved by the appropriate state agency. Once a state agency decides on the validity of a request, FMCSA considers that decision as the final resolution of the request. FMCSA cannot change state records without state consent.

Personally Identifiable Information (PII) and DataQs

All users must register with DataQs, or via the FMCSA Portal, to establish a user account for submitting and viewing data requests. The first step in registering with DataQs is to create a Login.gov account. Once created, Login.gov will send authentication information

to DataQs. DataQs then grants access to the user's account associated with the email address. If a user, based on their email address, has more than one account, the user must select a username and provide the password associated with the account.

For users without a DataQs account, the following elements are collecting during the registration process:

- Username
- Password
- First Name
- Middle Name
- Last Name
- Email Address
- Telephone number
- Business or Home Address
- Fax (optional)
- User-chosen personal security questions and responses

During submissions of Drug and Alcohol petitions, the additional data elements are collected about the CDL driver:

- Driver Name (first, middle, and last)
- Mailing address (address, country, city, State, zip)
- Phone
- Email
- License number
- License country
- License issuing State
- Clearinghouse Record ID

During the submission of other requests, a "driver name" may also be collected (optional field).

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.

DataQs is the FMCSA system that allows registrants to request and track a review of federal and state data published by FMCSA that they feel may be incomplete or incorrect. The DataQs website has a link to DOT Privacy Policy that contains all the protection and advisories required by the E-Government Act of 2002. The Privacy Policy describes DOT information practices related to the online collection and the use of PII.

The agency does not use personal identifiers to retrieve records from DataQs. Therefore, DataQs is not a Privacy Act protected system of records; however, FMCSA maintains DataQs in accordance with the Fair Information Practice Principles. FMCSA informs the public that their PII is collected, stored and used by DataQs through this Privacy Impact Assessment (PIA) published on the DOT website. 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 DataQs. The DataQs PIA is available at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

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.

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

[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

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.

FMCSA provides redress for individuals whose records may be stored on the FMCSA Cloud Environment and all the FMCSA applications through its DataQs system (https://dataqs.fmcsa.dot.gov). Individuals implicitly consent to the collection, use, dissemination, and retention of their PII by voluntarily registering with DataQs. The DataQs website includes instructions on how to contact FMCSA if corrections are required. 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. 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 because of the challenge, the change is made in the respective system.

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.

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.

The DataQs system was established in February 2004 in accordance with the Office of Management and Budget (OMB) Guidelines for Implementing Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554). OMB directed Federal agencies subject to the Paperwork Reduction Act (44 United States Code Chapter 35) to establish and implement written guidelines to ensure and maximize the quality, utility, objectivity, and integrity of the information they disseminate. FMCSA and state partners use driver information provided through requests and supplemental documentation to determine the proper outcome of a request. Driver information is used to validate a requestor's concerns regarding the accuracy of information within FMCSA's information systems (see Introduction and System Overview). FMCSA uses driver information to associate the proper action (inspection/crash/violation/etc.) with the correct

driver in the event that multiple drivers are involved, or when the wrong driver has been identified.

FMCSA uses DataQs account information to verify information and security questions if a user has been locked out of the system. FMCSA also uses DataQs account information to determine patterns of behavior detrimental to the system (e.g., fraudulent or frivolous requests).

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.

FMCSA collects, uses, and retains only that data that are relevant and necessary for the purpose of DataQs. The DataQs system collects data and supporting documentation submitted by individuals to request a review of information contained in his or her records maintained by FMSCA. In addition, the DataQs system collects data from entities required to register with DataQs to request a review of information on record with FMCSA.

Business information is collected from these entities when they register with FMCSA pursuant to Federal regulations. The business information allows FMCSA to positively identify those entities under its jurisdiction and manage FMCSA processes for which the information was collected.

Records will be retained and disposed in accordance with the provisions FMCSA's National Archives and Records Administration NARA retention disposition schedule NI-557-11-003 Item #2. Resolved RDR's will be transferred to the archival system after 3 years. Electronic records will be deleted two years after transfer to archival data file, or when no longer needed for business, legal, reference or administrative operations.

URL: http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0557/n1-557-05-007_sf115.pdf

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.

FMCSA limits the use of PII within DataQs as defined within this document. PII is used to support FMCSA and State efforts to resolve Requests for Data Review, and to ensure that the proper information is provided to the correct individual. FMCSA uses DataQs account

information to verify information and security questions if a user has been locked out of the system. FMCSA also uses DataQs account information to determine patterns of behavior detrimental to 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).

The FMCSA ensures that the collection, use, and maintenance of information collected for operating the DataQs 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. The information submitted to DataQs by subject individuals, or entities acting on subjects' behalf, are responsible for the accuracy and completeness of the provided information.

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, 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 DataQs 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 DataQs 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 DataQs system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the DataQs system is logged and monitored.

Users are required to authenticate with Login.Gov to gain access to DataQs. FMCSA personnel and FMCSA contractors are required to attend security and privacy awareness training and role-based training offered by DOT/FMCSA. No access will be allowed to the DataQs 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 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 DataQs 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 will conduct regular periodic security and privacy compliance reviews of the DataQs consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Audit provisions are also included to ensure that DataQs 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 DataQs. FMCSA contractors involved in data analysis and research are also required to sign the FMCSA Non-Disclosure Agreement prior to being authorized to access DataQs.

Responsible Official

Scott Valentine
System Owner
DataQs Business Owner & Data Quality Program Manager, FMCSA-MC-RRA

Prepared by: Pam Gosier-Abner (FMCSA Privacy Officer)

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.04.22 14:24:13 -04'00'