U.S. Department of Transportation

Privacy Impact Assessment

Federal Railroad Administration (FRA)

Railroads Compliance System (RCS)

Responsible Official

Rachell Horton – RCS Business
Email: rachell.horton@dot.gov
Phone Number: (202) 493-6030

Reviewing Official

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

Executive Summary

The Federal Railroad Administration (FRA) enables the safe, reliable, and efficient movement of people and goods throughout the Nation's railroad industry. To support our mission, the FRA Cloud Component Services (FCAS) is a collection of Software as a Service (SaaS) and Platform as a Service (PaaS) tools with its subsystems hosted within the Azure and Appian cloud and provides access to FRA personnel and its external customers. Railroads Compliance System (RCS) is the only tool within FCAS that collects, stores, or processes Personally Identifiable Information (PII). RCS supports the Office of Chief Counsel attorneys in the issuance of civil penalties, and documenting violations of railroad safety laws. RCS replaced the legacy Railroad Enforcement System (RES) application formerly known as "Enforcement Case System."

This Privacy Impact Assessment (PIA) is conducted in accordance with the E-Government Act of 2002 because RCS collects, stores, and maintains PII on members of the public. This PIA discusses why and how PII within RCS is stored and used and how the PII is protected.

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 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 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

Railroads Compliance System (RCS)

The primary purpose of RCS is to provide computerized support for the Office of Chief Counsel (RCC) attorneys in the issuance of civil penalty demand letters and other documents related to the violations of railroad safety laws and in the compilation of reports related to the railroad safety enforcement process. RCS system is accessible only to authorized FRA staff. RCS collects, stores and/or processes FRA forms with PII as part of the violation packages that include recommended civil penalties against railroads and shippers from the Office of Railroad Safety (RRS). The Transmittal Form Region (TFR) and its assigned violation packets consists of two parts: the structured data is passed from the FRA Railroad Safety Information System (RSIS) to RCS in the form of an XML data file, and the associated documents and evidence, generally in Portable Document Format (PDF) format, are placed into a shared SharePoint database to be picked up by RCS. Then, the violation packet is transmitted to RCS through a two-way path using an internal, SSL encrypted web page over the local area network.

The forms and PII collected are described in the "PII Collection" section of this PIA.

RCS replaced the legacy Railroad Enforcement System (RES) application formerly known as "Enforcement Case System." The RCS tool is hosted on a Department of Transportation (DOT) instance of Microsoft Dynamics 365 and Microsoft SharePoint Online. RCS has three major components:

1. **Civil Penalty and Individual Liability Case Management System**

   Provides data entry, update, and query screens for case generation; look-up screens for supporting information; and various reports used for tracking violation reports and cases. Individual Liability Cases is designed for actions against individuals in violation of the safety laws, including civil penalties, disqualification orders, and warning letters.

These cases rely on DOT internal form 6180.80 that collects PII information that is used to provide notice to individuals regarding violations of Federal railroad safety laws or regulations. The 6180.80 form plays a central role in processing of the information between the RCC attorney at the DOT Headquarters, the field inspector, and the Office of Railroad safety and has an assigned case number.

2. **Case Document Repository**

   Supported by Microsoft SharePoint Online, this repository is segregated into two site collections: internal and external. The case supporting documentation consists of TFR reports, violation reports, case generated documentation, and uploaded supporting case evidence files. Additionally, these case documents support attorney penalty assessments, transmitted settlement charges, and negotiations with the respondents. Case documents located in the external SharePoint Online location can be viewed by external users through the Respondent Portal.

3. **Respondent Portal for External User Access (Web Portal)**

   Provides respondents the ability to access case documents on SharePoint online externally.

PII Collection

The RCS tool collects and stores the below PII information about individuals that are in violation of the safety laws, that could result in civil penalties, disqualification orders, and warning letters. The intended use of the information is to correctly identify individuals who have been identified by railroad inspectors as having acted in negligence. Under authority of the Federal railroad safety and hazardous materials transportation laws, FRA collects this information for inclusion in its records concerning violations of the Federal railroad safety and hazardous materials transportation laws by individuals. Those records may be used to support enforcement actions against individuals and may be disclosed to other government agencies, the public, the railroad industry, or Congress in the interest of promoting compliance with the safety laws. Listed below are the details about PII data elements collected and stored in RCS as required.

Form FRA 6180.80 – Notice to Individual Regarding Violation (s)

- Office of Management and Budget (OMB) 2130-0509 – Expires: N/A
- Respondent's Name
- Respondent's Home Address

- Respondent's Date of Birth
- Respondent's Occupation
- Respondent's Employee ID Number
- Inspector's Name
- Inspector's ID Number

Form FRA 6180.33 – Violation of Hours-of-Service Law

- OMB 2130-0509 – Expires 11/30/2025
- Inspector's Name
- Inspector's ID Number
- Employee's Name
- Employee's Address

Form FRA 6180.98 – Railroad Employee Injury and/or Illness Record

- OMB 2130-0500 – Expires 5/31/2025
- Preparer's Name
- Preparer's Telephone Number
- Employee's Name
- Employee's Birthdate
- Employee's Home Address
- Employee's Injury/Condition/Treatment

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

[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

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.

FRA executes due care, and due diligence to ensure transparency. DOT System of Records Notices (SORNs) provide transparency about privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about individuals covered under the Privacy Act of 1974, as amended. The information in RCS is covered under DOT/FRA 130 - Enforcement Case System - 65 FR 19532 - April 11, 2000. RCS was formerly known as Enforcement Case System.

The RCC Administrative Specialist Assistant (ASA) is notified electronically in RCS that a new violation packet has been received in RCS. The RCC ASA logs in and verifies if the correct reports were received within the violation packet. If verified, the RCC ASA generates a case number to the violation packet and assign an attorney from RCC in RCS. Once the attorney completes his or her review and agrees with the provided evidence, a notice of probable violation letter is generated. Major railroads may receive documents supporting the charges against them through an on-line portal, implemented in SharePoint Online. There, they have read-only access to documents associated with all open cases against them. Once the case is closed, their access is removed.

Paperwork Reduction Act (PRA) statements exist on all forms, or on separate forms retained by individuals, to provide additional formal notice to individuals from whom any PII is collected. Furthermore, FRA and RCS public websites indicate what information is collected, why it is collected, how the information is used, how it is shared, with whom it is shared, choices the individual has regarding the collection of their PII, privacy information practices for children, the use of cookies and other tracking devices; how privacy information is secured, individual rights under the Privacy Act, and how to find out more or comment on FRA privacy practices. To further bolster FRA's attempts at transparency, the DOT Privacy Office publishes PIAs to the DOT Privacy Website.

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.

FRA complies with the Privacy Act of 1974 and provides individual reasonable opportunities for informed decisions on PII collected, using approved OMB forms, pertaining to rail safety regulations.

a. All RCS forms that collect PII provide a means for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection. Each form is approved by OMB. An example of OMB language is below:

   This collection of information is mandatory under 49 CFR 225 and used by FRA to monitor national rail safety. Public reporting burden is estimated to average two hours per response, including the time for reviewing instructions, searching existing databases, gathering, and maintaining the data needed, and completing and reviewing the collection of information.

   The information collected is a matter of public record, and no confidentiality is promised to any respondent. Please note that an agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number. The OMB control number for this collection is 2130-0500.

b. FRA provides the appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII. This is provided at each login site.

c. FRA obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

d. FRA ensures that individuals are aware of, and where feasible, consent to all uses of PII not initially described in the public notice, that was in effect at the time the organization collected the PII.

Individuals may request access to their own records maintained in a records system under FRA control by writing a letter of request:

Federal Railroad Administration
Attn: FOIA/PA Team
1200 New Jersey Avenue SE
Washington, DC 20590
or email; frafoia@dot.gov or Fax: (202) 493-6068.

The request must include the following information:

- Full Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records
- A statement under penalty of perjury that the requester is the individual who he or she claims to be.

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 Department's programs and information systems are restricted in the collection and use of PII, or activity impacting privacy, to that which is authorized by law. Under authority of the Federal railroad safety and hazardous materials transportation laws, FRA collects this information for inclusion in its records concerning violations of the Federal railroad safety and hazardous materials transportation laws by individuals. RCS is authorized for data collection under OMB Control Numbers 2130-0509 and 2130-0500. Each RCS form identified in the Introduction & System Overview section of this PIA clearly specifies this authority and purpose of collection and usage.

RCS data is used consistent with the purposes for which it was collected as described in the SORN DOT/FRA 130 – Enforcement Case System – 65 FR 19532 – April 11, 2000.

Internal Sharing

Unless otherwise limited by statute, information collected by a DOT Component will be considered an information asset of the entire Department. Unless explicitly authorized or mandated by law, DOT will permit internal sharing of PII only for a purpose compatible with the original purpose of collection, specified at the time of initial collection for authorized purposes. For actions against individuals in violation of the safety laws, which could result in civil penalties, disqualification orders, and warning letters, Railroad Inspectors collect the information from individuals to populate DOT internal form 6180.80, Individual Liability Cases. The inspectors submit the form to their Regional Administrator. The Regional Administrator mails the form 6180.80 via FedEx certified mail services to the FRA RCC attorney, located at DOT Headquarters. After the attorney reviews the form, the FRA RCS Business Owner manually enters data from the electronic 6180.80 form in RCS and a tracking number is automatically assigned to the form. The Business Owner then assigns the attorney to the tracking number for further internal review.

Once the RCC attorney completes the review of the individual liability case, he or she provides detailed information to the Office of Railroad Safety (RRS) to draft a violation report. RRS sends the violation report to the RCC attorney for approval. When RCC approves the report, the individual is notified and is allotted time to respond. If the respondent's justification is not valid, the case file can be listed as completed in RCS. The RCS Business Owner is notified by the RCC attorney to generate the following documents

in RCS: Chief Counsel Warning Letter, Penalty Demand Letter, or Notice of Proposed Disqualification, and assembles the case file.

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.

FRA only collects the minimum PII necessary as listed in the Introduction & System Overview section of this PIA. Identified elements are relevant and necessary to accomplish the legally authorized purpose of collection. The FRA Privacy Officer evaluates PII holdings via risk management security assessments.

Retention of information that contains PII, is maintained according to NARA standards. For RCS, the retention of information is identified in the schedules below:

1. **Schedule Identifier:**
N1-399-08-008 Railroad Compliance System (RCS), 3/23/2008 https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0399/n1-399-08-008_sf115.pdf and N1-399-08-002 Chief Counsel's Office – Safety Law Division https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department- of-transportation/rg-0399/n1-399-08-002_sf115.pdf.

2. **Schedule Summary:**
N1-399-08-008
Item 1.b.: Master file: System data consists of violation related proof, some attorney notes, violation details, penalty information, railroad information, and tracking details date range is 1991-present.

    1. **File Attachments:** File attachments consist of all Violation related proof and some attorney notes.

    Disposition: **Temporary.** Cut-off file at end of fiscal year in which case is closed or when fine or settlement amount has been paid, whichever is later. Delete 3 years after cutoff.

    2. **Case and Tracking Information:** Case details include violations details, penalty information, railroad information, attorney information. Tracking information consists of when case sent to /reviewed by attorney, expert attorney, railroad earner and when it was mailed and settled.

    Disposition: Temporary. Cut off file at end of fiscal year when case is closed or when fine or settlement amount is paid, whichever is later, as

noted in 1b(l), File Attachments, above Delete 30 years after this cut off or when no longer needed, whichever is later.

N1-399-08-002
Item 9: Enforcement -Individual Liability Files:

Disposition: **Temporary.** Close files at end of the fiscal year when case is closed.

If paper: Transfer to FRC 5 years after closure Destroy 30 years after closure.

If electronic: Delete 30 years after closure.

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.

DOT discloses RCS information outside of DOT in accordance with SORN DOT/FRA 130 - Enforcement Case System – 65 FR 19532 – April 11, 2000. FRA shares PII with appropriate FRA representatives, other federal government agencies, or other designated representatives as needed only for authorized purposes. Program and field personnel have completed initial and annual security and privacy awareness training to ensure protection of PII, pertaining to sharing PII with third parties. However, RCS does not share information with third parties. The FRA Office of Safety minimizes its data collection to what is necessary to meet the authorized business purpose and mission of the Agency.

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).

FRA complies with the Privacy Act of 1974, data quality and integrity requirements, by ensuring Program Offices confirm to the best of their knowledge that collection of PII is accurate, relevant, timely and complete. PII is collected directly from individuals whenever possible. The FRA Privacy Officer provides guidelines to the Program Offices that are compliant with DOT standards and requirements.

The FRA Privacy Officer performs continuous privacy and security risk assessments, ensures integrity of data through the implementation and enforcement of appropriate security controls. Access to data and the application is strictly limited to those who has a verified and authorized need to perform their duties in support of the FRA mission. FRA

ensures PII is protected, collected, and retained in accordance with Federal privacy policies and laws.

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.

FRA has appropriate security safeguards in place to protect PII against risks such as loss, unauthorized access, use, destruction, modification or unintended or inappropriate disclosure. FRA protects all records against reasonably anticipated threats or hazards that may result in harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained. At a minimum, all PII is protected using controls consistent with the requirements at Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards where loss of confidentiality may result in serious adverse effects to agency's operations, assets, individuals and PII data not publicly available. Microsoft Dynamics 365 provides for RCS data entry, update, and query screens for case generation; look-up screens for supporting information; and various reports used for tracking violation reports and cases. Dynamics 365 is offered as SaaS to DOT by Microsoft Azure Cloud services which is FedRAMP certified at the high security impact level.

DOT and Microsoft Azure implement and operate an extensive set of security configurations and controls to safeguard the confidentiality and integrity of the data in accordance with the National Institute of Standards and Technology (NIST) standards. This includes documenting the management, operational, and technical processes used to secure the system and data.

The DOT Chief Privacy Office may, in accordance with FIPS 199, increase or decrease the accepted confidentiality risk of PII in a particular information system on a case-by-case basis, based on a determination about the risk of reasonably anticipated threats in Privacy Risk Management DOT Order 1351.18, page 10 of 23, or hazards that could result in harm to the individual or the Department because of unauthorized access or use of the PII. The confidentiality protection requirements of Sensitive PII (SPII) may not be reduced.

Encryption of data in transit and at rest protections are implemented and enforced using NIST certified cryptographic modules for RCS, unless authorized in writing, by DOT's Deputy Secretary or a Senior DOT Official.

Since the RCS tool is developed using FedRAMP certified Microsoft Dynamics 365, data at rest is stored at datacenters physically located only in the United States. FRA established strict authentication and authorization controls to provide RCS availability to personnel who require need-to-know access.

FRA will not print records containing PII unless required to support the DOT mission. FRA follows DOT Incident Response Plan that provides an organized and effective response to all security and privacy incidents. FRA ensures all personnel are provided with a clear definition of what constitutes a breach involving PII and are aware of how, where, what information is needed to report the loss, inappropriate access, use or sharing of PII.

In the event of unauthorized PII access, use or disclosure, FRA takes immediate action to deter further damage or disclosure. FRA ensures appropriate and prompt notification of affected individuals in the event of a breach of SPII proportionate with the risk of harm to the individual(s) and consistent with Federal and DOT standards and requirements.

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.

Effective governance, monitoring, risk management, security safeguards and controls demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals. FRA is responsible for identifying, training, and holding Agency personnel accountable for adhering to DOT privacy and security policies and regulations. FRA follows the Fair Information Practice Principles as best practices for the protection of information associated with the RCS tool.

In addition, these practices, policies, and procedures are consistently assessed, improved, and applied to assure proper protection, retention, and destruction of records. Federal and contract employees are given clear guidance in their duties in accessing, 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.

Responsible Official

Rachell Horton
RCS Business Sponsor
Administrative Officer, Deputy Chief Counsel
Federal Railroad Administration (FRA)

Prepared by: Elizabeth Varghese (FRA 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: 2024.10.11 09:31:00 -04'00'