U.S. Department of Transportation

Office of the Chief Information Officer (OCIO)

Privacy Threshold Assessment (PTA)

Federal Railroad Administration

Web Information Services (WIS)

KARYN MARIE GORMAN

Digitally signed by KARYN MARIE GORMAN
Date: 2020.10.27 16:41:05 -04'00'

Privacy Threshold Assessment (PTA)

The Privacy Threshold Assessment (PTA) is an analytical tool used to determine the scope of privacy risk management activities that must be executed to ensure that the Department's initiatives do not create undue privacy risks for individuals.

he Privacy Threat Assessment (PTA) is a privacy risk management tool used by the Department of Transportation (DOT) Chief Privacy Officer (CPO). The PTA determines whether a Department system[1] creates privacy risk for individuals that must be further analyzed, documented, or mitigated, and determines the need for additional privacy compliance documentation. Additional documentation can include Privacy Impact Assessments (PIAs), System of Records notices (SORNs), and Privacy Act Exemption Rules (Exemption Rules).

The majority of the Department's privacy risk emanates from its direct collection, use, storage, and sharing of Personally Identifiable Information (PII),[2] and the IT systems used to support those processes. However, privacy risk can also be created in the Department's use of paper records or other technologies. The Department may also create privacy risk for individuals through its rulemakings and information collection requirements that require other entities to collect, use, store or share PII, or deploy technologies that create privacy risk for members of the public.

To ensure that the Department appropriately identifies those activities that may create privacy risk, a PTA is required for all IT systems, technologies, proposed rulemakings, and information collections at the Department. Additionally, the PTA is used to alert other information management stakeholders of potential risks, including information security, records management and information collection management programs. It is also used by the Department's Chief Information Officer (CIO) and Associate CIO for IT Policy and Governance (Associate CIO) to support efforts to ensure compliance with other information asset requirements including, but not limited to, the Federal Records Act (FRA), the Paperwork Reduction Act (PRA), the Federal Information Security Management Act (FISMA), the Federal Information Technology Acquisition Reform Act (FITARA) and applicable Office of Management and Budget (OMB) guidance.

Each Component establishes and follows its own processes for developing, reviewing, and verifying the PTA prior to its submission to the DOT CPO. At a minimum the PTA must be reviewed by the Component business owner, information system security manager, general counsel, records officers, and privacy officer. After the Component review is completed, the

[1] For the purposes of the PTA the term "system" is used throughout document but is not limited to traditional IT systems. It can and does refer to business activity and processes, IT systems, information collection, a project, program and/or technology, and proposed rulemaking as appropriate for the context of the assessment.

[2] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Component Privacy Office will forward the PTA to the DOT Privacy Office for final adjudication. Only PTAs watermarked "adjudicated" and electronically signed by the DOT CPO are considered final. Do NOT send the PTA directly to the DOT PO; PTAs received by the DOT CPO directly from program/business owners will not be reviewed.

If you have questions or require assistance to complete the PTA please contact your Component Privacy Officer or the DOT Privacy Office at privacy@dot.gov. Explanatory guidance for completing the PTA can be found in the PTA Development Guide found on the DOT Privacy Program website, www.dot.gov/privacy.

PROGRAM MANAGEMENT

SYSTEM name: Web Information Services (WIS)

Cyber Security Assessment and Management (CSAM) ID: 1086

SYSTEM MANAGER CONTACT Information:

Name: Victoria Ball

Email:victoria.ball@dot.gov

Phone Number: (202) 493-0438

Is this a NEW system?

☐ **Yes** (Proceed to Section 1)
☒ **No**
☐ **Renewal**
☒ **Modification**

Is there a PREVIOUSLY ADJUDICTED PTA for this system?

☒ **Yes:**

Date: 6/17/2019

☐ **No**

1 SUMMARY INFORMATION

1.1 System TYPE

☒ **Information Technology and/or Information System**

Unique Investment Identifier (UII): 021-255678806

Cyber Security Assessment and Management (CSAM) ID: Web Information Services (WIS) CSAM ID 1086

☐ **Paper Based:** *<< Provide a general description of the paper based documents. >>*

☐ **Rulemaking**

Rulemaking Identification Number (RIN): *<<Provide RIN assigned by OMB's electronic docketing system>>*

Rulemaking Stage:

☐ **Notice of Proposed Rulemaking (NPRM)**
☐ **Supplemental NPRM (SNPRM)**:
☐ **Final Rule**:

Federal Register (FR) Notice: *<<Provide full Rulemaking Name, Federal Register citation, and web address if available.>>*

☒ **Information Collection Request** (ICR)[3]

☐ **New Collection**

☒ **Approved Collection or Collection Renewal**

☒ **OMB Control Number:** 2130-0526

☐ **Control Number Expiration Date:** Feb. 28, 2021

☐ **Other:** <<*Describe the type of project*>>

System OVERVIEW: The Web Information Services (WIS) infrastructure is a General Support System hosted within the FRA Hosting and Operational Support Technology Services (FRA-HOSTS) environment. The WIS program provides FRA personnel and members of the general public access to FRA-related information, statistics, analytics, policies and regulations, and current events. The program consists of two parts: records management and web information services. The web information services portion consists of internet web sites, intranet sites, collaboration portals, and various internal web-enabled business intelligence and analytics tools. The records management portion consists of managing the FRA Records Management Program, including the full records life-cycle (creation, maintenance/use, and disposition) for both official hardcopy and electronic records.

The following privacy relevant changes have been made to the PTA since it was last adjudicated. The Program Management Tracker (PMT) (Internal) **(**PMT) subsystem and Financial Management System (FMS) subsystem has been removed and Gradedec.Net subsystem has been added. In addition, some of the PII elements for Information Correspondence Management System (iCMS) subsystem and Post-Accident Toxicological Testing System II (PATTS II) subsystem System have been clarified further. Social Security Number has been detailed for PATTS II Subsystem. Social Security Numbers (SSN) are an option on Form 6180.74, OMB 2130-0526, Post-Accident Testing Blood/Urine Custody and Control Form. Also, Railroad Enforcement System (RES) system interface and related data exchanges is being shut down.

The WIS information system includes the following modules within its authorization boundary:

- **Content Discovery System (CDS) (Internal)** – CDS is the trusted platform for information applications for FRA that look to drive revenue, streamline operations, and manage risk by using Schema-agnostic Enterprise NoSQL database technology, coupled with powerful search and flexible application services. It has delivered a powerful, agile, and trusted enterprise-grade NoSQL (Not Only SQL) database that enables FRA to turn all data into valuable and actionable information.
- **Information Correspondence Management System (iCMS) (Internal)** – Currently iCMS includes the following modules: Freedom of Information Act (FOIA) requests, one-time movement (HAZMAT), and Train Horn Rule correspondence (Quiet-Zones). iCMS is built on IBM's Enterprise Content Management (ECM) platform.

[3]See 44 USC 3201-3521; 5 CFR Part 1320

- **Post-Accident Toxicological Testing System II (PATTS II) (Internal)** – The post-accident testing requirement uses a contractor (Quest Diagnostics) for the forensic drug and alcohol testing laboratory to conduct the actual testing. After a railroad accident, the railroads are required by Part 219 to accomplish specimen collections, complete required paperwork, and send the specimens to the contract laboratory. The laboratory tests the specimens for the target substances and reports the results to the appropriate entities. PATTS II will enable all forms and paperwork to be stored and archived electronically and will be the repository for new and legacy FRA post-accident toxicological testing program documentation, specimen lab results, and railroad accident data. It will allow FRA alcohol and drug program personnel access to query the accident files, trend data, and develop reports to enable effective use of the data by FRA management. This project is critical to effective management and policy planning in this congressionally mandated program.
- **Railroad Safety Advisory Committee (RSAC) (External) –** The RSAC is a formally charter federal advisory committee chartered by the Secretary of Transportation and is authorized under Section 10(a)(2) of the Federal Advisory Committee Act (FACA) (Pub. L. 92-463). The RSAC's mission is to develop railroad safety regulations through a consensus process. The RSAC system supports the Committee. The RSAC website is used to provide FRA personnel, industry partners and members of the general public access to committee specific information. The RSAC website database is a SQL repository that stores RSAC membership profile/contact data and consists of a public and private area where information about the RSAC and historical meeting documents are posted. Access to the private areas is controlled to members of particular groups with members assigned by member organizations. The RSAC website enables the general public to view Committee documents and provides a window to the development of new regulatory safety standards.

- **Railroad Safety Advisory Committee Content Management System (RSAC-CMS) (Internal):** RSAC CMS is an in-house designed and built .NET website content management system. It offers multilevel granular permission control to ensure that content is managed effectively and consistently. The CMS stores all site content in a SQL database, including general information of the following; text, images and documents for simplified storage, backup and retrieval.

- **FRANet:** FRANet is FRA's Intranet. This portal is not publicly accessible and is an internal website. FRANet serves as on online library for FRANet personnel and contains information about FRA. The website provides valuable information about management and FRA's key areas of responsibilities. FRANet is a key element in the broader internal communications strategy to give employees timely information, tools, and leadership updates. The information source will provide a one-stop shop that broadens employees understanding of FRA. In addition, FRANet helps employees strengthen their workplace engagements and career development.

- **FRANet Content Management System (FRA Net CMS) (Internal):** CMS is an in-house designed and built .NET website content management system. It offers multilevel granular permission control to ensure that content is managed effectively and consistently. The CMS stores all site content in a SQL database, including general information of the following; text, images and documents for simplified storage, backup and retrieval.

- **FRA Public Site-External:** Federal Railroad Administration official website provides the general public information about FRA. This site allows the public to stay current with FRAs mission to "enable the safe, reliable, and efficient movement of people and goods for a strong America, now and in the future".

- **FRA CMS Public Site-Internal:** CMS is an in-house designed and built .NET website content management system. It offers multilevel granular permission control to ensure that content is managed effectively and consistently. The CMS stores all site content in a SQL database, including general information of the following; text, images and documents for simplified storage, backup and retrieval.
- **Identity, Credential, and Access Management (iCAM):** FRA identity credential and access management (iCAM) solution to allow all FRA internal web applications use PIV card as primary mean or DOT account with second factor authentication to login the system. The system leverages Active Directory Federation Services (AD FS) 2.1 to simplify access to applications and other systems with an open and interoperable claims-based model.

- **Railroader Sleep Website:** The Railroader's Guide to Healthy Sleep website was produced by the U.S. Department of Transportation Volpe Center (Volpe Center) in Cambridge, MA, and is sponsored by the Federal Railroad Administration (FRA), U.S. Department of Transportation (U.S. DOT). Originally launched on June 11, 2012 in collaboration with the Harvard Medical School Division of Sleep Medicine, the site was updated by the Volpe Center in 2015, serving as a major educational initiative for the railroad industry about the importance of sleep health. The Railroaders' Guide to Healthy Sleep provides articles, videos, and real-life examples that aim to help you sleep well, enjoy friends and family life, and stay connected with your community. The site provides practical steps and smart sleep tactics that you can use to combat fatigue, many of which may also benefit members of your household and extended support network and allow them to best support your sleep needs.

- **GradeDec.Net**: It is a low security impact web-based application and a decision support tool that is used for the identification and evaluation of highway-rail grade crossing upgrades, separations and closures. The system has been designed for the needs of federal, state and local authorities and its decision makers. GradeDec.Net employs benefit-cost methodologies to assess grade crossing investment alternatives at the corridor level or in a region. Third party software is used on the

GradeDec.Net server. GradeDec.Net outputs can be downloaded by FRA employees, clients, remote users and the general public. The system is used in conducting the safety and investment analyses of grade crossings. Users of GradeDec.Net can access the application through a public-facing website by accessing the following GradeDec.Net does not interconnect with any other system or share information with other agencies. However, GradeDec.Net leverages network, storage and database services from FRA-HOSTS. There is no PII stored on the system

2 INFORMATION MANGEMENT

2.1 SUBJECTS of Collection

Identify the subject population(s) for whom the system collects, maintains, or disseminates PII. (Check all that apply)

☒ **Members of the public:**

☒ **Citizens or Legal Permanent Residents (LPR)**

☐ **Visitors**

☒ **Members of the DOT Federal workforce**

☒ **Members of the DOT Contract workforce**

☐ **System Does Not Collect PII.** If the system does not collect PII, proceed directly to question 2.3.

2.2 What INFORMATION ABOUT INDIVIDUALS will be collected, used, retained, or generated?

The modules below that are within the WIS boundary, collect, use, and/or retain information about individuals:

Content Discovery System (CDS) - CDS is used to ingest the email pst files of outgoing senior leaders and index them for searching in case of FOIA requests. CDS stores the contents of emails sent and received via .gov addresses within FRA. FOIA does not collect PII, however individuals may provide PII in their request, therefore PII may be contained in the emails stored on CDS.

Information Correspondence Management System (iCMS) - Currently the following PII and business information is stored in iCMS: correspondence data stored in read only mode for historic purposes only as all iCMS correspondence modules have been transitioned to the DOT Enterprise EDMS tool.

1.**FRA** Basic information for correspondence is stored in read only mode for historic purposes only as all iCMS correspondence modules have been transitioned to the DOT Enterprise EDMS tool which is owned by DOT.

Federal DOT Employees and Public

Name of Recipient

Address of Recipient
Phone Number of Recipient
Email Address of Recipient

2.**FRA Freedom of Information Act (FOIA) Requests** – The Freedom of Information Act (FOIA) is a Federal law that establishes the public's right to obtain access to Federal agency records. FRA is an operating administration within DOT and subject to the Department FOIA Regulation, 49 CFR Part 7. FOIA does not collect PII, however individuals may provide PII in their request. PII is redacted prior to correspondence for requests.

3. FRA **Train Horn Rule Requests** – *Does not collect or store PII*. Public Authorities, governmental entity responsible for traffic control, or law enforcement at the crossings, send requests to establish quiet zones per the Train Horn Rule. Notice of Intents, Notice of Establishments, Public Authority Applications to FRA, and comments from railroads and state DOTs. All information is stored in the database, along with annual reviews of the quiet zones, and FRA correspondence to the public authorities.

4.**FRA Waiver Request** – A petition for waiver generally seeks an exception from compliance with a regulation that the petitioner believes is unnecessary or excessively burdensome under the specific circumstances. Although certain statutorily mandated requirements cannot be waived, in general FRA may issue a waiver from its regulations when it is in the public interest and consistent with railroad safety.

Railroad Industry

Name of Petitioner
Work Address of Petitioner
Work Phone Number of Petitioner
Work Email Address of Petitioner

Post-Accident Toxicological Testing System II (PATTS II) – The following PATTS II PII and business information is collected and maintained by FRA in support of Office of Safety. 49 CFR Part 219 Subpart C, post-accident testing is for the workplace industry program. This does not apply to FRA employees. All information collected and maintained for post-accident testing is from the Railroad Industry employees and/or contractors.

FRA F (6180.73) Post-Accident Toxicological Testing, OMB 2130-0526: FRA post-accident toxicological test must be conducted after any event that involves one or more circumstances including major train accident, impact accident, fatal train incident, passenger train accident, or human-factor highway-rail grade crossing accident/incident, per 49 CFR Part 219 Subpart C.

Railroad Industry

Name of Employee(s) providing specimen
Employee(s) Job Title
Specimen Set Identification Number
FRA Toxicology Box Number (Predetermined number that corresponds to each Toxicology Box that includes materials and forms for the urine/blood sample)

Name of Medical Review Officer
Work Address of Medical Review Officer
Work Phone Number of Medical Review Officer
Name of Railroad Representative
Work Address of Railroad Representative
Work Phone Number of Railroad Representative

FRA F (6180.74) Post-Accident Testing Blood/Urine Custody and Control Form, OMB 2130-0526: FRA post-accident testing blood/urine custody and control form for basic information concerning the accident/incident and any treatment administered after the accident/incident is necessary to process specimens, analyze the significance of laboratory findings, and notify railroads and employees of test results, per 49 CFR Part 219 Subpart C.

Railroad Industry

Name of Employee(s) providing specimen
Employee Identification Number or Social Security Number (SSN)
Employee Home Address
Employee Telephone Number
Specimen Set Identification Number
Name of Collector (person collecting blood/urine specimen)
Name of Person taking possession of specimen for shipment

FRA F (6180.75) Collection of Post-Mortem Toxicology Samples, OMB 2130- 0526: FRA Collection of Post-Mortem Toxicology Samples form for basic information concerning the accident/incident and information after the accident/incident is necessary to process specimens, analyze the significance of laboratory findings, and notify railroads, per 49 CFR Part 219 Subpart C. This form is specifically for fatalities of the accident/incident.

Railroad Industry

Name of Deceased Name of Collector (person collecting blood/urine specimen)
Name of person who received specimen at FRA Laboratory Specimen Set Identification Number

Medical Review Officer (MRO) Results- The MRO reviews any positive laboratory result. The MRO Results document is sent from the MRO to FRA Alcohol/Drug (A/D) Program Manager. The document includes a letter of the summary of the results, the toxicology report, Form 6180.74, and Form 6180.75 (if employee is deceased).

Railroad Industry

Name of Employee providing specimen
Quest Diagnostics Laboratory Results
Form 6180.74
Form 6180.75 (if employee is deceased)

National Transportation Safety Board (NTSB) Requests-NTSB may investigate accidents/incidents. NTSB will request for release of information/subpoena to Quest Diagnostic and/or FRA Alcohol/Drug (A/D) Program Manager requesting remaining

specimen of the employee.
Railroad Industry
Name of Employee
Date of Birth (DOB)

Quest Diagnostics Laboratory Results-Forensic Toxicology Report for FRA Railroad and/or Railroad Industry employee.
Railroad Industry
Name of Employee providing specimen
FRA Case Number Specimen
Set Identification Number

Railroad Safety Advisory Committee (RSAC) – Railroad Safety Advisory Committee (RSAC) was established to develop new regulatory standards, through a collaborative process, with all segments of the rail community working together for solutions on safety regulatory issues. The following RSAC and Railroad Industry personnel profile information is collected and maintained by FRA in support of Office of Safety. The RSAC Committee includes representatives from all of the agency's major stakeholder groups, including railroads, labor organizations, suppliers and manufactures, and other interested parties.
DOT Employees/Railroad Industry/Labor Organizations, Suppliers and Manufactures
Member Name
Member Company Address
Member Organization
Member Phone Number
Member Fax Number
Member Company Email Address
Member Type
Member Status (Active/Inactive)
Member Occupation

2.3 Does the system RELATE to or provide information about individuals?

☒ **Yes**: WIS is a General Support System (GSS) that retains information about individuals on Four (4) subsystems within its boundary. Information such as names, physical addresses, email addresses, phone numbers for correspondence and information regarding post-accident blood/urine testing is retained.

☐ **No**

If the answer to 2.1 is "*System Does Not Collect PII*" **and** the answer to 2.3 is "*No*", you may proceed to question 2.10.
If the system collects PII or relate to individual in any way, proceed to question 2.4.

2.4 Does the system use or collect SOCIAL SECURITY NUMBERS (SSNs)? (This includes truncated SSNs)

☒ **Yes:**

Authority: Social Security Numbers (SSN) are an option on Form 6180.74, OMB 2130-0526, Post-Accident Testing Blood/Urine Custody and Control Form. This form is based on DOT and Health and Human Services (HHS) Custody and Control Form for Federal Drug Testing. The use of SSNs on the Form 6180.74 is rare and OMB reviewed this form in 2017. *FRA do not have special authority to collect SSN.*

Purpose: SSN is an option in Form 6180.74. The form requests "Employee Identification Number or Social Security Number. *Smaller Railroads are using SSN in the absence of an Employee ID (EID) to uniquely identify the individual. When notified of the need to post-accident test, FRA will reach out to the railroad D&A Testing contact and strongly encourage the use of EID vs. SSN.* Approximately 200-250 Form 6180.74s are used per year and FRA estimates that only about 15% (30-38 forms) would employ the SSN annually. Smaller RRs generally use the SSNs and the larger Class I RRs use the employee ID.

☐ **No**: The system does not use or collect SSNs, including truncated SSNs. Proceed to 2.6.

2.5 Has an SSN REDUCTION plan been established for the system?

☒ **Yes:** *<< Provide the details of the reduction plan including date conducted, alternatives evaluated, determination reached and any steps taken to reduce the SSN collection and use.>>*

☐ **No:** *<< A system without an SSN reduction plan is in violation of the Privacy Act. Explain why a reduction plan has yet to be completed and provide an anticipated completion date.>>*

2.6 Does the system collect PSEUDO-SSNs?

☐ **Yes:** All forms under 49 CFR 219 will expire October 2019. SSN will be removed from the form and will only require Employee Identification Number.

☒ **No**: The system does not collect pseudo-SSNs, including truncated SSNs.

2.7 Will information about individuals be retrieved or accessed by a UNIQUE IDENTIFIER associated with or assigned to an individual?

☒ **Yes**

Is there an existing Privacy Act System of Records notice (SORN) for the records retrieved or accessed by a unique identifier?

☒ **Yes:**

SORN*:*
DOT/ALL 13 – Internet/Intranet Activity and Access Records – 67 FR 30757 – May 7, 2002, https://www.govinfo.gov/content/pkg/FR-2002-05- 07/pdf/02-10943.pdf
DOT/ALL 17 - Freedom of Information Act and Privacy Act Case Files – 84 FR 4605 – February 15, 2019, https://www.govinfo.gov/content/pkg/FR- 2019-02-15/pdf/2019-02356.pdf
DOT/FRA 132-Controlled Correspondence Manager (CCM) – 71 FR 35728- June 21, 2006**,** https://www.govinfo.gov/content/pkg/FR-2006-06- 21/pdf/E6-9733.pdf

☐ **No:**

Explanation:

Expected Publication: *<<List the expected date of publication for a SORN that will bring the system into compliance with the Privacy Act.>>*

☐ **Not Applicable:** Proceed to question 2.9

2.8 Has a Privacy Act EXEMPTION RULE been published in support of any Exemptions claimed in the SORN?

☒ **Yes**

Exemption Rule: DOT/ALL 17 - Freedom of Information Act and Privacy Act Case Files – 84 FR 4605. During a FOIA or PA action, exempt materials from other systems of records may in turn become part of the case records in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into the FOIA/PA case file, the same exemptions apply for those records, as are claimed for the original systems of records which they are a part.
https://www.govinfo.gov/content/pkg/FR-2019-02-15/pdf/2019-02356.pdf

☐ **No**

Explanation: *<< An explanation must be provided for failure to comply with all of the requirements of the Privacy Act without an Exemption Rule.>>*

Expected Publication: *<< List the expected date of publication for an Exemption Rule that will bring the system into compliance with the Privacy Act.>>*

☐ **Not Applicable**: SORN does not claim Privacy Act exemptions.

2.9 Has a PRIVACY IMPACT ASSESSMENT (PIA) been published for this system?

☐ **Yes:** *<< Provide the full PIA Name, the publication date, and the URL. >>*

☐ **No**: *<< If a previous PTA required a PIA as part of adjudication, and a PIA was not published, provide an explanation. If this is a new system, write "New System.">>*

☒ **Not Applicable:** The most recently adjudicated PTA indicated no PIA was required for this system.

2.10 Does the system EXCHANGE (receive and/or send) DATA from another INTERNAL (DOT) or EXTERNAL (non-DOT) system or business activity?

☒ **Yes:** WIS System exchanges data with Railroad Safety Information System (RSIS), Controlled Correspondence Manager (MarkLogic), FRA-Hosts and SharePoint Farm

☐ **No**

2.11 Does the system have a National Archives and Records Administration (NARA)-approved RECORDS DISPOSITION schedule for system records?

☒ **Yes:**

Schedule Identifier:
CMS & CDS: General Records Schedule 4.1

FMS: General Record Schedule 1.1

iCMS: FRA Record Schedule (Correspondence) N1-399-14-02

FOIA: General Records Schedule 4.2

PATTS II: FRA Record Schedule, Master File NI-399-08-9

RSAC: FRA Record Schedule (Committees) NI-399-07-17

Schedule Summary: CMS & CDS: Item No. 10
https://www.archives.gov/files/records- mgmt/grs/grs04-1.pdf
Retention: Temporary. Destroy when no longer needed.
FMS: Item No. 20 http://www.archives.gov/records-mgmt/grs/grs01-1.pdf
Retention: Temporary. Destroy 2 years after completion of audit or closure of financial statement /accounting treatment/issue, but longer retention is authorized if required for business use.
iCMS: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-transportation/rg- 0399/daa-0399-2014-0002_sf115.pdf and https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0399/daa- 0399-2015-0001_sf115.pdf

Retention: *System Master File*
Disposition: Temporary. Destroy between 5 and 30 years after cutoff.
Retention: *Major Correspondence*
Disposition: Permanent. Transfer to NARA 5 years after cutoff
Retention: *Correspondence – All Other*
Disposition: Temporary. Destroy 5 years after closure or when no longer needed for Agency business occurs, whichever is later
FOIA: Item No. 60 GRS 4.2-Information Access and Protection Records, http://www.archives.gov/records-mgmt/grs/grs04-2.pdf
Retention: Temporary - Destroy 1 year after final resolution, but longer retention is authorized if required for business use. DAA-GRS- 2016-0001- 0003
PATTS II: Items No. 3 Master File-Case and Testing Information https://www.archives.gov/files/records- mgmt/rcs/schedules/departments/department-of-transportation/rg-0399/n1- 399-08-009_sf115.pdf
Retention: Case details include date, location, individuals) and railroad involved m the reportable incident Testing information includes the results of the drug and alcohol testing
Disposition: Permanent - Cut off at end of each calendar year and transfer to NARA as specified in 36 CFR 1228270 or standards applicable at the time of transfer.
RSAC: Committee/Workgroup Records https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0399/n1- 399-07-017_sf115.pdf
Retention: If the recordkeeping copy is a permanent record and is maintained in an electronic format, transfer to NARA in accordance with 36 CFR 1228.270. If the recordkeeping copy is a temporary record and is maintained in an electronic format, keep the file in the office for the entire retention period in accordance with 36 CFR 1234 sec: 30-32.

☐ **In Progress:** *<< Include proposed schedule, when it will be submitted to NARA, or job code.>>*

☐ **No:** Click here to enter text.

3 SYSTEM LIFECYCLE

The systems development life cycle (SDLC) is a process for planning, creating, testing, and deploying an information system. Privacy risk can change depending on where a system is in its lifecycle.

3.1 Was this system IN PLACE in an ELECTRONIC FORMAT prior to 2002?

The E-Government Act of 2002 (EGov) establishes criteria for the types of systems that require additional privacy considerations. It applies to systems established in 2002 or later, or existing systems that were modified after 2002.

☒ **Yes**: WIS was established as an electronic system after 2002

☐**Not Applicable**: System is not currently an electronic system. Proceed to Section 4.

3.2 Has the system been MODIFIED in any way since 2002?

☒ **Yes**: The system has been modified since 2002.

☒ **Maintenance.**

☒ **Security.**

☐ **Changes Creating Privacy Risk**: *<< Describe any modification that may introduce new privacy risk, including but not limited to: paper to electronic conversions, changing anonymous information into information in identifiable form, significant system management changes (including application of new technologies), significant system or data merging, use of new authentication technologies in support of public access, commercial data sources, new interagency uses, changes in internal flow or data collection, or alternation of data characterization.>>*

☐ **Other**: *<< Describe >>*

☐ **No**: The system has not been modified in any way since 2002.

3.3 Is the system a CONTRACTOR-owned or -managed system?

☐ **Yes**: The system is owned or managed under contract.

Contract Number: *<<Contract #>>*

Contractor: *<< Contractor Name >>*

☒ **No**: The system is owned and managed by Federal employees.

3.4 Has a system Security Risk CATEGORIZATION been completed?

The DOT Privacy Risk Management policy requires that all PII be protected using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards. The OA Privacy Officer should be engaged in the risk determination process and take data types into account.

☒ **Yes**: A risk categorization has been completed.

Based on the risk level definitions and classifications provided above, indicate the information categorization determinations for each of the following:

Confidentiality:	☐ Low	☒ Moderate	☐ High	☐ Undefined
Integrity:	☐ Low	☒ Moderate	☐ High	☐ Undefined
Availability:	☐ Low	☒ Moderate	☐ High	☐ Undefined

Based on the risk level definitions and classifications provided above, indicate the information system categorization determinations for each of the following:

Confidentiality:	☐ Low	☒ Moderate	☐ High	☐ Undefined
Integrity:	☐ Low	☒ Moderate	☐ High	☐ Undefined
Availability:	☐ Low	☒ Moderate	☐ High	☐ Undefined

☐ **No:** A risk categorization has not been completed. Provide date of anticipated completion. Click here to enter text.

3.5 Has the system been issued an AUTHORITY TO OPERATE?

☒ **Yes:**

Date of Initial Authority to Operate (ATO): 3/12/2020

Anticipated Date of Updated ATO: 3/12/2021

☐ **No:** *<<Provide the anticipated ATO date.>>*

☐ **Not Applicable**: System is not covered by the Federal Information Security Act (FISMA).

4 COMPONENT PRIVACY OFFICER ANALYSIS

The Component Privacy Officer (PO) is responsible for ensuring that the PTA is as complete and accurate as possible before submitting to the DOT Privacy Office for review and adjudication.

COMPONENT PRIVACY OFFICER CONTACT Information

Name: : Elizabeth Varghese

Email: : elizabeth.varghese@dot.gov

Phone Number: 202-493-0489

COMPONENT PRIVACY OFFICER Analysis

WIS system collects and stores non-sensitive PII from the public and railroad industry employees. SSN is an option in Form 6180.74. The form requests "Employee Identification Number or Social Security Number. *Smaller Railroads are using SSN in the absence of an Employee ID (EID) to uniquely identify the individual. When notified of the need to post-accident test, FRA will reach out to the railroad D&A Testing contact and strongly encourage the use of EID vs. SSN.* Approximately 200-250 Form 6180.74s are used per year and FRA estimates that only about 15% (30-38 forms) would employ the SSN annually. Smaller RRs generally use the SSNs and the larger Class I RRs use the employee ID. FRA will initiate a PIA for WIS system.

of WIS. Based on this assessment, a Privacy Impact Analysis is recommended.

5 COMPONENT REVIEW

Prior to submitting the PTA for adjudication, it is critical that the oversight offices within the Component have reviewed the PTA for completeness, comprehension and accuracy.

Component Reviewer	Name	Review Date
Business Owner	*Eric Lovett*	*9/15/2020*
General Counsel	*John Kern*	*9/15/2020*
Information System Security Manager (ISSM)	*Elizabeth Varghese*	*10/9/2020*
Privacy Officer	*Elizabeth Varghese*	*10/9/2020*
Records Officer	*Kim Toone*	*9/15/2020*

Table 1 - Individuals who have reviewed the PTA and attest to its completeness, comprehension and accuracy.

APPENDIX J CONTROLS ASSESSMENT

-- The DOT CPO has determined the control is satisfied based on a review of the PTA and any other supplemental information referenced in the Adjudication statement

Note: Information pertinent to the controls assessment and PTA adjudication and/or information the Component is requested to review and consider. Actions not rising to the level of POA&M may be captured in Notes.

POA&M: Information in the PTA and other supplemental information indicates the control is "other than satisfied" and Component must take action as directed.

DOT PRIVACY OFFICE COMMENTS

PTA mentions systems that are no longer in use (PMT and FMS), which require System Disposal Assessments. Full assessment below.

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	DOT CPO Notes
AP-1	Authority to Collect	1.2 - Overview	X			OMB Control No 2130-0526 • WIS (ALL) - DOT/ALL 13 - Internet/Intranet Activity and Access Records - 67 FR 30757 - May 7, 2002 • CDS - DOT/FRA 132 - Controlled Correspondence Manager (CCM) - 71 FR 35728 - June 21, 2006 • CMS - DOT/FRA 132 - Controlled Correspondence Manager (CCM) - 71 FR 35728 - June 21, 2006 • iCMS - DOT/FRA 132 - Controlled Correspondence Manager (CCM) - 71 FR 35728 - June 21, 2006 • FOIA - DOT/ALL 17 - Freedom of Information Act and Privacy Act Case Files - 84 FR 4605 - February 15, 2019 • PATTS II - DOT/FRA 130 - Enforcement Case System - 65 FR 19532 - April 11, 2000 • RSAC – Based on the information provided in the PTA, the DOT PO is unable to determine whether or not RSAC is a System of Records under the Privacy Act – see TR-2.
AP-2	Purpose Specification	1.2 - Overview	X			The Web Information Services (WIS) program provides FRA personnel and members of the general public access to FRA-related information, statistics, analytics, policies and regulations, and current events. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.
AR-1	Governance and Privacy Program	Common Control	X			Addressed by DOT CPO.

AR-2	Privacy Impact and Risk Assessment	Program Management		X		**POA&M** **Issue:** WIS is comprised of multiple applications, many of which collect and maintain information about members of the public. OMB M-03-22 requires that a PIA be conducted when developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public. **Requirement:** FRA must complete and provide PIAs to the DOT Privacy Office. **Timeline:** DOT privacy Office has established timeline for PIAs based on relative risk, FRA may submit PIAs in different order, however all PIAs must be submitted within 120 days: 1. PATTS II – within 30 days of the adjudication of this PTA 2. FOIA – within 60 days of adjudication of this PTA. 3. iCMS – within 90 days of the adjudication of this PTA. 4. RSAC – within 120 days of the adjudication of this PTA.
AR-3	Privacy Requirements for Contractors and Service Providers	3.3 - Contractor System	X			The system is owned and managed by Federal employees.
AR-4	Privacy Monitoring and Auditing	Common Control	X			Addressed by DOT CPO.
AR-5	Privacy Awareness and Training	Common Control	X			Addressed by DOT CPO.
AR-6	Privacy Reporting	Common Control	X			Addressed by DOT CPO.
AR-7	Privacy-Enhanced System Design and Development	2.5 - SSN Reduction	X			**Note:** FRA must ensure there are there adequate safeguards to ensure proper protection and to minimize the risk associated with the collection of SSN and other sensitive PII.

AR-8	Accounting of Disclosures	2.7 - SORN	X			FRA is responsible for accounting of disclosures consistent with the DOT Privacy Act Regs, and applicable SORNs and Exemption Rule(s) for the system. DOT/ALL 17 - Freedom of Information Act and Privacy Act Case Files – 84 FR 4605 claims exemptions.
DI-1	Data Quality	1.2 - System Overview	X			Data quality is determined by OA information system owners. Information collected directly from individuals where applicable.
DI-2	Data Integrity and Data Integrity Board	3.4 - Security Risk Categorization			X	Activity does not constitute sharing covered by the CMA.
DM-1	Minimization of PII	2.2 – Information About Individuals		X		**POA&M** **Issue:** FRA collects the Social Security number (SSN) on Form 6180.74, Post-Accident Testing Blood/Urine Custody and Control Form, which is used by the PATTS II system. FRA plans to remove the SSN from this from the form and replace it with the EIN in October of this year. **Requirement:** FRA must review their SSN holdings and remove the SSN from the records that were entered into the PATTS II system prior to the removal of the SSN from the form. **Timeline:** 180 days from the adjudication of this PTA. Non-substantive records created for purposes of system login, audit and other security management functions are covered under DOT/ALL-13, Internet/Intranet Activity and Access Records; 67 FR 30757, May 7, 2002. OAs are responsible for following DOT Privacy Risk Management Policy and OA Privacy Program for the original

						data collection. Minimization of PII is determined by OAs and information system owners.
DM-2	Data Retention and Disposal	2.11 - Records Disposition Schedule	X			**NOTE:** FRA notes that it maintains FOIA release records under GRS 4.2, Item 60. However, this portion of the schedule is limited to "erroneous release". The FRA must apply all aspects for the FOIA schedule to its FOIA records based on the business use of the record.
DM-3	Minimization of PII Used in Testing, Training, and Research	2.2 – Information About Individuals	X			System not used for testing, training, research
IP-1	Consent	2.7 - SORN	X			Information is collected directly from individual to the extent practicable. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.
IP-2	Individual Access	2.8 – Exemption Rule	X			Exemptions claimed in SORNs have been published in Federal Register.
IP-3	Redress	2.7 - SORN	X			Redress process identified in SORN and Exemption Rules. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.
IP-4	Complaint Management	Common Control	X			Addressed by DOT CPO.

SE-1	Inventory of PII	Common Control	X			WIS is a privacy sensitive system. System categorization at Moderate Confidentiality is appropriate. The Adjudicated PTA or copy of controls/POA&Ms should be included in the risk acceptance package for the system. The Adjudicated PTA should be uploaded into CSAM as evidence that the required privacy analysis for this system has been completed. The PTA should be updated not later than the next security assessment cycle and must be approved by the DOT CPO prior to the authorization decision. Component policy or substantive changes to the system may require that the PTA be updated prior to the next security assessment cycle.
SE-2	Privacy Incident Response	Common Control	X			Addressed by DOT CPO.
TR-1	Privacy Notice	2.7 - SORN		X		**POA&M** **Issue**: FRA plans to replace the space for the SSN on form 6180.74 with a space for the EIN. Many small businesses and sole proprietorships use their SSNs as the EIN. **Requirement:** FRA must make it clear on the new Form 6180.74 that no special protection will be provided for the SSN if it is provided on the form in lieu of an EIN. **Timeline:** Prior to the PRA renewal package for the form being submitted to the DOT PRA Officer. **Note:** original date was "and not later than October 2019."

TR-2	System of Records Notices and Privacy Act Statements	2.7 - SORN		X		**POA&M** **Issue:** Information provided in this PTA was not sufficient to determine which SORN records about committee members stored in RSAC should be maintained. Requirement: Conduct an analysis of DOT and FRA SORNs to determine which SORN applies to the records. **Timeline:** 120 days (consistent w/ PIA). **NOTE:** Committee records are not subject to the Privacy Act, however biographies, credentials, resumes, etc. of individuals who are members of the Committee or testify to the Committee may be protected under DOT/ALL 16 or DOT/ALL 25.
TR-3	Dissemination of Privacy Program Information	Common Control	X			Addressed by DOT CPO.
UL-1	Internal Use	2.10 - Internal and External Use	X			Access to PII limited to those identified in referenced SORNs.
UL-2	Information Sharing with Third Parties	2.10 - Internal and External Use	X			Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13