U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Reimbursable Toolset System (RTS)

Responsible Official

Aaron Anthony
Email: aaron.anthony@faa.gov

Reviewing Official

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

Executive Summary

The Federal Aviation Administration's (FAA) Reimbursable Toolset System (RTS) supports the management and execution of the FAA Reimbursable Agreement (RA) lifecycle from planning and forecasting through creation, approval, execution, funding, implementation, and closeout. An RA is a contractual relationship under which the FAA provides products or services, and the costs are paid by the recipient. This Privacy Impact Assessment (PIA) is being completed as RTS maintains Personally Identifiable Information (PII) on individuals who work with companies that do business with the FAA.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *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.*

[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).

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 Federal Aviation Act of 1958, as amended, gives the Federal Aviation Administration (FAA) the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. The FAA is responsible for:

- Regulating civil aviation to promote safety;
- Encouraging and developing civil aeronautics, including new aviation technology;
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- Regulating U.S. commercial space transportation. The Drug Abatement Division has been given the responsibility to carry out safety programs to regulate the aviation industry.

RTS program personnel use the system to create an RA. To start an RA, the FAA employee/contractor navigates to https://rts.faa.gov and logs into the system. To create the RA, the user manually enters information into RTS, which could include information about members of the public, in their business context, such as: customer/company name, customer/company number, sponsor, type of work, company contact name and business email address, business address, Data Universal Numbering System (DUNS) number, Tax ID number (TIN), and funding and grant information. This information is received directly from the FAA contracts.

Once the RA is created, an agreement number is generated to track the RA. The RTS program personnel must then request funds for the RA, and manually enter non-PII funding information from the DOT system, Delphi. No funds are managed in RTS. RAs must be signed by a Contracting Officer (or Delegated Official) and will include their name, office location, business email address, and business telephone number. This Personally Identifiable Information (PII) is entered into RTS via a data exchange with the FAA's Corporate Work Plan (CWP)[2].

Prior to the execution of a RA, agreements must be approved by FAA legal counsel and the Reimbursable Oversight Program Liaison and Budget Oversight. These reviews happen within RTS. Once the RA has been concluded, it is closed out.

To authenticate to the system, FAA Directory Services sends to RTS the user ID, business location, and business e-mail address.

RTS has a data exchange agreement with Tableau for the purpose of creating reports, which could include Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs).

[2] CWP has a PIA that can be located at https://www.transportation.gov/individuals/privacy/corporate-work-plan-cwp-0

The system does not require users to add an SSN, but it also does not restrict users from adding an SSN used as a TIN.

RTS also shares data with CWP for those projects where a customer pays the FAA for engineering and architecture services rendered. This data could also include TIN.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on 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 risks. 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[3], 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[4].

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.

RTS collects PII that is discussed in the Overview section of this PIA during the creation of an RA. Transparency is provided via FAA business processes that require users to submit invoices for transactions. The public has no access to RTS. The publication of this PIA further demonstrates DOT's commitment to providing appropriate transparency regarding the handling of such information.

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.

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

Substantive records within RTS do not require SORN coverage as they contain business information only. Substantive records are not retrieved by an identifier linked to an individual, and the records are not about individuals and are therefore not subject to the Privacy Act. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.

Under the provisions of the Privacy Act, individuals may request searches to determine if any records have been added that may pertain to them. Individuals wishing to know if their records appear in a system may inquire in person, or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington, DC 20591

Included in the request must be the following:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records

Individuals wanting to contest information about themselves that is contained in RTS should make their requests in writing, detailing the reasons why the records should be corrected to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington, DC 20591

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 RTS is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

RTS maintains PII on FAA employees/contractors who use the system and on companies doing business with the FAA. RTS collects PII that is discussed in the Overview section of this PIA during the creation of an RA. Transparency is provided via FAA business processes that require users to submit invoices for transactions. The public has no access to RTS.

Business TINs are maintained within RTS. In some circumstances, a business TIN could be the SSN of the business proprietor. RTS is part of the FAA's SSN Reduction Elimination

Plan, v.18, and is authorized to maintain TIN/SSN ("vendor code"). The SSN Reduction Elimination Plan is an initiative to reduce or eliminate using social security numbers as individual identifiers. The system does not require users to add an SSN, but it also does not restrict users from adding an SSN used as a TIN. The FAA has performed activities to ensure the safeguarding of PII through encryption and limited network access.

Substantive records within RTS do not require SORN coverage as they contain business information only. Access and authentication information is covered by DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002, 67 FR 30757. MyAccess is used for RTS system access, and account roles and responsibilities must be approved and monitored by the System Administrator. The RTS system collects information on members of the public such as sole proprietors. Substantive records are not retrieved by an identifier linked to an individual, and the records are not about individuals and are therefore not subject to the Privacy Act. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.

Legal authority to collect information is covered by 49 U.S.C. § 106(l)(6) for reimbursable agreements, as well as 49 USC 40101 and 49 USC 40103 for general authority.

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.

The FAA collects and retains PII that is relevant and necessary to create RAs. TINS are maintained, but access controls limit visibility to only users who have access to the overarching RA.

RTS maintains records in accordance with National Archives and Records Administration (NARA) FAA Financial Records Schedule N1-237-09-23 approved June 10, 2010, and NARA General Record Schedule (GRS) 3.2, Information Systems Security Records, approved September 2016.

Disposition: Cut off at the end of the Fiscal Year in which policy is superseded or obsolete. Destroy three years after cut-off in accordance with applicable federal standards, and in accordance with limitations on civil actions by or against the U.S. Government (28 U.S. Code 2401 and 2415). All other related electronic records may be retained as long as needed for business purposes and no longer than seven years.

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.

Business TINs are maintained within RTS. In some circumstances, a business TIN could be the SSN of the business proprietor. RTS is part of the FAA's SSN Reduction Elimination Plan, v.18, and is authorized to maintain TIN/SSN ("vendor code").

RTS does not maintain convenience copies (copies of official FAA records used in support of job duties) of records but does have discrete data exchanges of data elements with other FAA systems.

- CWP: RTS receives via transmission control protocol (TCP) the FAA employee's name, business telephone, business email, and tasks, facility codes, job control number status from CWP; RTS receives the RA, project, funding data, task number, and TIN/SSN used for projects where a business pays the FAA for engineering and architecture services rendered.
- Tableau: Tableau exchanges all RTS data fields, including PII, using TCP to create reports. This includes the TIN number which may be the SSN for individuals using their SSN in place of a TIN.
- Delphi: RTS has a manual data exchange of non-PII funding information with Delphi.
- MyAccess: RTS exchanges the FAA employee and contractor username and business email with MyAccess using Hypertext Transfer Protocol for authentication and access purposes.

Substantive records within RTS do not require SORN coverage as they contain business information only. Substantive records are not retrieved by an identifier linked to an individual, and the records are not about individuals and are therefore not subject to the Privacy Act. Profile and logging PII collected by the FAA is used only as specified by the FAA's system of records notice, DOT/ALL 13, *Internet/Intranet Activity and Access Records*. In addition to other disclosures generally permitted under 5 U.S.C. §552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

- To provide information to any person(s) authorized to assist in approved investigations of improper access or usage of DOT computer systems;
- To an actual or potential party or his or her authorized representative for the purpose of negation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings;
- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records; and
- To other government agencies where required by law.

The Department has also published 15 additional routine uses applicable to all DOT Privacy Act systems of records. These routine uses are published in the Federal Register at 75 FR

82132, December 29, 2010, and July 20, 2012, 77 FR 42796, under "Prefatory Statement of General Routine Uses."

RTS maintains a data-sharing agreement with Tableau.

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).

RTS receives information that is accurate, relevant, timely, and complete. RTS receives information from other FAA systems discussed in the Overview of the PIA. The information is provided daily, and the data and accuracy of information are ensured through those systems. Information in the system is presumed to be correct because it was provided directly by the companies executing the contracts with FAA. Data is transferred electronically, which reduces the likelihood of inadvertent mistakes that could occur during manual entry.

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.

The FAA protects PII 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, dated September 2020.

RTS has met all requirements and has been certified with an Authority to Operate (ATO) by DOT/FAA. RTS was granted its ATO on September 27, 2021, after undergoing the National Institute of Standards and Technology (NIST) security assessment and authorization (SA&A). The RTS system is audited by FAA Security Personnel to ensure FISM compliance through an annual assessment according to NIST standards and guidance.

Access to RTS is limited to authorized staff members and support personnel. Physical access to the RTS system is limited to authorized personnel. FAA and support personnel with physical access have all passed DOT background checks. In addition, access to RTS PII is limited according to job function.

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.

FAA Order 1370.121B, FAA Information Security and Privacy Program & Policy, implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance. In addition to these practices, the FAA will implement additional policies and procedures as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with RTS are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy training awareness training, as well as FAA Order 1370.121B. The FAA will conduct periodic privacy compliance reviews of RTS as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Aaron Anthony
RTS System Owner

Approval and Signature

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