U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Financial Services (ABA)
Purchase Request Information System (PRISM)

Responsible Official

Mike Winebrenner
mike.winebrenner@faa.gov
(405) 954-8889

Reviewing Official

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

Executive Summary

The Federal Aviation Administration's (FAA) Financial Services (ABA) Purchase Request Information System (PRISM) is used to process and track procurement documents such as purchase requests (PRs), procurement contracts (PCs), and purchase orders (POs) for products and services for the FAA. PRISM supports FAA's business needs through the use of electronic document routing (procurement documents) and approvals, requisitioning, electronic notifications, contract management, post award processing and close-outs in order to streamline the FAA procurement processes. PRISM addresses the unique demands of the FAA's workforce and operates under the authority of 5 United States Code (U.S.C.) 301; and 49 U.S.C. 40110 and 106(f).

The FAA is publishing this Privacy Impact Assessment (PIA) for the PRISM system in accordance with Section 208 of the E-Government Act of 2002 because the system processes Personally Identifiable Information (PII) from members of the public, outside vendors/businesses[1] that have a contracting relationship 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.[2]

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

[1] Some individuals owning sole proprietorships may choose to use their Social Security Number (SSN) as their Taxpayer Identification Number (TIN).
[2]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The DOT/FAA's Financial Services (ABA) Purchase Request Information System (PRISM) supports DOT/FAA's business needs through the use of electronic routing (procurement documents) and approvals, requisitioning, electronic notifications, contract management, post award processing and close-outs to streamline the DOT/FAA procurement process. PRISM functionality allows users to interface with procurement documentation and process orders for goods and to perform other procurement related tasks. PRISM is used to process and track procurement documents such as PRs PCs, and POs for products and services for the DOT/FAA.

PRISM is an internal DOT/FAA system, which is only accessible and used by FAA employees and contractors. There are no external users who *access* the system; however, the system *contains* PII from members of the public who are external vendors/businesses who have a contracting relationship with the DOT/FAA. PRISM contains personally identifiable information (PII) pertaining to vendors; however, the bulk of PII is not collected directly by PRISM, except for the information needed for access and authentication data. PII retained within the PRISM system may include the following PII, where a vendor uses PII in identifying themselves in a business-related entrepreneurial capacity:

- Vendor/Individual Name
- Date of Birth (DOB)
- Social Security Number (SSN) (only if they use the SSN as their Taxpayer Identification Number (TIN))
- Business Mailing Address
- Business Financial Account Information

An individual's PII enters the PRISM system when the vendor submits a proposal or invoice, or when DOT/FAA enters a relationship with an individual (in a business capacity) or organization that requires an accounting relationship through the procurement of goods or services. DOT/FAA employee or contractor information enters the PRISM system for access/authentication purposes and to manage the PRISM system/program. DOT/FAA

employees' PII can also be entered into the system with regards to the use of a Government Purchase/ Credit Card[3] (P-Card). Typically, the information is added to and exists in DELPHI and is made available to PRISM through a system-to-system transfer.

All data maintained in PRISM, except system access data, is obtained via data exchanges with other DOT/FAA systems and is from external vendors/businesses that have a contracting relationship with the DOT/FAA. PRISM does not collect PII directly from these vendors/businesses. PRISM has data exchanges with several other systems internal to DOT/FAA for routine DOT/FAA business purposes such as facilitating system access, obtaining data pertinent to procurements, and supporting internal security and investigations activity.

Business Process for PRISM:

There are two types of authorized PRISM users: DOT/FAA employees and contractors, who are administrative users that manage the program and DOT/FAA employees who are P-Card users. For a DOT/FAA employee to request initial access to PRISM or request a P-Card, the user must complete the PRISM web-based training in the DOT/FAA Electronic Learning Management System (eLMS) and complete the DOT/FAA PRISM User ID Request Form. For a DOT/FAA contractor, they must also complete the web-based training in eLMS and fill out the DOT/FAA Contractor PRISM User ID Request Form. The forms are completed by the users and then emailed to the PRISM administrator for their region or DOT/FAA Headquarters.

As mentioned, PRISM is designed to process and track PRs, PCs, and POs including approvals, requisitioning, electronic notifications, contract management, post award processing, and close-outs to streamline the DOT/FAA procurement processes. When a DOT/FAA program office has a need for products or a service, they gain access as described above and log into PRISM to create a requisition. The requisition contains a description, dollar value, and the accounting stream and is saved into PRISM. They then route it through the approval process within PRISM, which starts with the FAA employee, who is the fund certifier. The fund certifier logs into PRISM and approves the funding source. Next, the requisition is routed to the DOT/FAA approver. PRISM notifies the fund certifier and approver via email that they need to log into PRISM review and approve the requisition. Once the requisition is approved in PRISM, it is automatically validated and uploaded to Delphi via a data exchange. Once the requisition is approved in Delphi, it is released back to PRISM. The requisition is then assigned to the DOT/FAA contracting officer (CO) and they log into PRISM and use the requisition to create the award document (delivery task/purchase

[3] The FAA uses the purchase card for nearly all micro-purchases ($10,000 or below) for commercial supplies, construction, and services.

order) and then the CO approves the award document. The award document is then emailed to the requesting DOT/FAA program office.

The requisition process is used when a contract is needed, which requires a CO, for example, building a tower or real estate purchases. Although the process to acquire a P-Card is outside of the PRISM system, P-Card users log into PRISM and document their purchases. PRISM uses information from another financial system, OBIDWAN to produce financial reports containing data from Delphi, which could contain vendor/business name, business mailing address, Universal Entity Identification (SAM UEI), TIN/SSN, and Data Universal Numbering System (DUNS) number. The reports can include DOT/FAA employee and contractor username, document number, commitment amounts, and purchase description. There are also reports that show when a new user was created and when they logged in. It shows the names of the new/existing user Information is pre-populated with PRISM data, which originates in PRISM, but is accessed via the OBIWAN Reporting Tool, which is a part of the OBIDWH system. and the PRISM administrator that created the user. All reports are only available internally to the DOT/FAA.

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[4], 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[5].

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.

[4] https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

PRISM is a privacy-sensitive system because it maintains collects, uses, disseminates, and retains PII from members of the public, external vendors/businesses that have a contracting relationship with the DOT/FAA to fulfill accounting functions relating to the requisition of goods or services. Policies, procedures and practices for information storage, data use, access, notification, retention and disposal are described herein this PIA.

The DOT/FAA protects records subject to the Privacy Act in accordance with the following Department's Published System of Records Notices (SORNs):

DOT/All 7, *Departmental Accounting and Financial Information System* (DAFIS) and *Delphi Accounting System*, 66 FR 65236 (December 18, 2001) covers accounting functions and requisition of goods or services records for vendors/businesses that have a contracting relationship with the DOT/FAA or DOT/FAA employees that are P-Card users.

DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002) cover login credentials, audit trails, and security monitoring records for DOT/FAA employees and contractors who are part of the PRISM program and/or manage the system.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the PRISM system.

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.

Individuals submit information directly to the DOT/FAA; however, they submit information to systems and locations other than PRISM. Each of those "source systems" have their own processes for ensuring individual participation and redress, which are detailed in those systems' PIAs.

In addition, under the provisions of the Privacy Act, individuals may request searches of the PRISM system to determine if any records have been added that may pertain to them and if such records are accurate.

For all inquiries related to the information contained in the PRISM, the individual may appear in person, send a request via email (privacy@faa.gov), or in writing to:

Privacy Office

800 Independence Avenue, SW

Washington, DC 20591

The request must include the following information:

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

If an individual believes information maintained in PRISM is inaccurate, they can make a request in person, or through mail or email, to the source system that provides the information to PRISM. If they are unsure of what source system provided the information in question to PRISM, they can make requests to the Privacy Office at the locations identified above.

If you have comments, concerns, or need more information on DOT/FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.

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.

Congress has authorized the DOT/FAA Administrator to develop systems and/or tools to support business needs through the use of electronic document routing (procurement documents) and approvals, requisitioning, electronic notifications, contract management, post award processing. PRISM addresses the unique demands of the DOT/FAA's workforce and operates under the authority of 5 U.S.C. 301; 49 U.S.C. 40110 and 106(f).

PRISM maintains the following PII on federal employees and contractors for PRISM system access and program management and/or P-Card users: Name/FAA Manager/Supervisor Name, FAA Phone Number, FAA Email Address, PRISM User ID, Digital Signature of FAA Employee, Organizational routing code, Digital Signature of Supervisor or Contracting Officer's Technical Representative (COTR for Contract Employees, Previous/Existing User ID (if applicable), Internet Protocol (IP) Address, Username, and Password.

The FAA uses this access information for purposes of creating and validating login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the PRISM program and/or manage the system. This use is consistent with the

description in the "purpose" section in the applicable system of records notice, DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002).

In addition, PRISM maintains the following PII on members of the public (vendors and businesses that have a contracting relationship with the DOT/FAA): Vendor/Business Name, Contract Name and Number, County, Business Email Address, Business Phone Number, Business Mailing Address, SAM UEI, DUNS Number, Award Number, Vendor Code, TIN/SSN, DOB, Contract and Task Order Number.

PRISM uses this information in accordance with the purposes for which it is collected: to process and track PRs, PCs, and POs including approvals, requisitioning, electronic notifications, contract management, post award processing, and close-outs from vendors/businesses that have a contracting relationship with the DOT/FAA. This information is used in accordance with the description in the "Purpose" section of the applicable system of records notice, DOT/All 7, *Departmental Accounting and Financial Information System* (DAFIS) and *Delphi Accounting System*, 66 FR 65236 (December 18, 2001).

The PII in the PRISM system is not routinely used for any other purposes.

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 DOT/FAA maintains the minimum amount of information from individuals to support PRISM account access, P-Card usage, and to process and track PRs, PCs, and POs including approvals, requisitioning, electronic notifications, contract management, post award processing, and close-outs. The DOT/FAA maintains these records in accordance with following National Archives and Record Administration (NARA) approved General Retention Schedules[6] (GRS):

- *Payment and Reimbursable Records* are temporary and are destroyed seven years after the end of the Fiscal Year in which the payment is made or debt is satisfied. Information may be maintained for longer timeframes if required for business purposes.[7]

[6] General retention schedules are used by the FAA to determine how long to maintain an individual's records and/or when to delete the individual's records and in order to promote consistent retention practices.
[7] NARA Big Bucket Title: Financial Management Flexible Schedule, n1-237-09-023_sf115 (14)

- DOT/FAA employee and contractor *System Access and Audit Log Records* are maintained in the system as temporary records and are destroyed when business use ceases.[8]

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.

The PII in PRISM is used for account access, P-Card usage, and to process and track PRs, PCs, and POs including approvals, requisitioning, electronic notifications, contract management, post award processing, and close-outs from vendors/businesses that have a contracting relationship with the DOT/FAA. The DOT/FAA does not routinely use the PII for any other purpose. PRISM receives PII via data exchanges with multiple internal DOT systems including Logistic Center Support System, Corporate Work Program System, Real Property Financial Management Tool System, Oracle Business Intelligence Wide Accounting Network, Investigation Tracking System, National Airspace Infrastructure Management System, and the DOT Delphi System. The DOT/FAA maintains Memorandum of Understandings (MOUs)/ PII data sharing agreements to provide appropriate controls.

The DOT/FAA limits the scope of PII maintained in PRISM about members of the public to support the purpose specified in SORN DOT/All 7, *Departmental Accounting and Financial Information System* (DAFIS) and *Delphi Accounting System*, 66 FR 65236 (December 18, 2001). DOT/FAA may share the information in the system with the DOT/FAA accounting office personnel to:

- Provide employees with offline paychecks, travel advances, travel reimbursements, and other official reimbursements
- Facilitate the distribution of labor charges for costing purposes
- Track outstanding travel advances, receivables, and other non-payroll amounts paid to employees
- Clear advances that were made through the system in the form of offline paychecks, payments for excess household goods made on behalf of the employee, garnishments, overdue travel advances, etc.

The Department has also published 17 additional routine uses that apply to all DOT Privacy Act systems of records, including this system. These routine uses are published in the

[8] NARA GRS 3.2, approved September 2014, *Information Systems Security Records*, Item 30 (DAA-GRS-2013-0006-0003).

Federal Register at 75 FR 82132, December 29, 2010, 77 FR 42796, July 20, 2012, and 84 FR 55222, October 15, 2019 under "Prefatory Statement of General Routine Uses."

Access and authentication records within PRISM are routinely disclosed in accordance with the routine uses identified in SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002), and consistent with the General Routine Uses identified above.

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).

PRISM collects, uses, and retains data that is relevant and necessary for the purpose for which it was collected. Much of the information regarding an individual is provided by that individual through the System for Award Management[9] (SAM) and thus it is assumed to be accurate. In some cases, a DOT employee may manually enter the information using the DOT DELPHI system. However, most of the data, except access and authentication data, comes from data exchanges with the other DOT/FAA and DOT systems, which are listed in the overview of this PIA. Because the data is received utilizing automated process, the data is assumed to be accurate as each of those systems have processes and mechanisms in place to ensure data quality and integrity, which includes the responsibility to ensure data accuracy. Accuracy of information in PRISM is ensured through managerial review of the data.

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 DOT/FAA protects PII with 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 Security 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 the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and*

[9] This is the Federal government's E-procurement system.

Privacy Controls for Federal Information Systems and Organizations, dated September 2020 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of the PRISM system to test security processes, procedures and practices. The system operates on security guidelines and standards established by NIST and only DOT/FAA personnel with a need to know are authorized to access the records in PRISM All data in-transit is encrypted and access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessment to test and validate security process, procedures and posture of the system. Based on the security testing and evaluation in accordance with the FISMA, the DOT/FAA issues PRISM an on-going authorization to operate.

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.

DOT/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 DOT/FAA information and information technology management procedures and guidance.

DOT implements 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.

In addition to these practices, the DOT/FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with PRISM 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 awareness training and in DOT/FAA Order 1370.121B. The DOT/FAA also conducts periodic privacy compliance reviews of PRISM as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Mike Winebrenner
System Owner

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer