U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Finance & Management, Financial Services (AFN-ABA)

Corporate Work Plan (CWP)

Responsible Official

Fred Gomez
Email: fred.gomez@faa.gov
Phone Number: (202) 267-3237

Reviewing Official

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

Executive Summary

Corporate Work Plan (CWP) is part of the FAA's Office of Finance & Management, Financial Services (AFN-ABA). CWP is an FAA system used for managing the full lifecycle of programs/projects associated with the establishment, modernization, and sustainment of the National Airspace System (NAS) and infrastructure projects from inception through capitalization. The system is used by project managers and others who have a need for the project management information. CWP is authorized under 49 United States Code (U.S.C.) 40101; 49 U.S.C. 40104; and 49 U.S.C. Chapter 471.

The FAA is publishing this Privacy Impact Assessment (PIA) for the CWP 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, who are vendors who conduct business with the FAA and may use their own name, address, phone number for their business contact information, including the Data Universal Numbering System (DUNS) Number. The vendor information is imported from the FAA Comprehensive Procurement Management System (PRISM), and is imported to PRISM from other systems, not directly from the vendors.

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

[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).

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.*

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 FAA has a significant number of programs and projects focused on keeping the National Airspace System (NAS) and infrastructure safe and efficient. These programs and projects include FAA airspace and procedures initiatives, airport-specific efforts, along with traditional automation, communications, navigational, surveillance and weather programs. These are complex and challenging programs, and therefore, must be integrated and coordinated across the agency. In order to have effective and standard program and project management processes and practices, the agency needed to improve its ability to look across programs and organizations to effectively integrate, coordinate, and leverage opportunities to improve program/project planning and execution. Thus CWP, part of the FAA's Office of Finance & Management, Financial Services (AFN-ABA), was created to manage the full lifecycle of programs/projects associated with the establishment, modernization, and sustainment of the NAS and infrastructure projects from inception through capitalization.

The majority of the PII in CWP is FAA employees' and contractors' names and email addresses which are used to facilitate CWP business processes. The information is used for task assignments and to notify users of stages of project management. The remaining PII, including vendors name, address, phone number, and Data Universal Numbering System (DUNS) Number, is from members of the public, which are vendors that conduct business with the FAA. This vendor information is not collected directly from the vendors and is from a data exchange with the FAA Comprehensive Procurement Management (PRISM) System.

Transactions in CWP all relate to maintaining project management data for projects. To begin, a need/project is identified and entered into the CWP system via the Origination process, which includes selecting the names of the FAA employees and contractors who will be part of the Project Team. Once the need has been validated and approved, a standard

project schedule is attached. Once the schedule is created, a Project Charter is generated. The initial planning funding for a project may be requested in the Funding Request process, and once completed, the FAA staff for planning and implementation can execute planning activities such as site surveys to obtain more information on the project to help further define/refine the project scope, schedule, and cost.

At this point, CWP is used by the FAA to further refine the Project Charter, enter and create Cost Estimates, manage the Project Team, assign implementation organizations, and work with the FAA technical staff to tailor and refine the project schedule. Once the project is sufficiently detailed and planned, the project will then go through the Baseline Scope process to become a baselined project. A project is baselined with the project scope, schedule, and cost. Through the baseline scope process, the Project Scope Agreement is created, and the project schedule is baselined. At this point, execution funding for the project is requested.

As the project moves from the planning phase to the execution phase, the Work Authorization process is used to hand-off the project details and funding to the FAA implementation staff. If, at any time during project planning or execution, the project needs to be put on hold, cancelled, or its descriptive information/attributes changed, those functions are also performed in CWP. Throughout the business transaction, CWP sends email notifications to the relevant Project Team members: Origination, Project Team, Baseline Scope, Funding Request, Work Authorization, and Project Information.

CWP includes several ad hoc project management and financial reports. CWP uses the FAA's Tableau system, via a data exchange, for generating reports that include resource information (organization, FAA employee names, emails, phone numbers) and other non-PII scheduling and funding information. FAA employees and contractors use CWP to get information on a particular project and/or for statistical and planning analysis. Users may not notice that they log in to a separate Tableau application because of single sign on. Permissions are the same as in CWP, so reports can only be generated by users who have access to the project data and Tableau.

Data retention is all based on the CWP records being temporary. CWP is not a system of record. Records are kept as long as needed for business purposes, with seven years being the longest retention after they are no longer needed.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a

framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

CWP is a privacy-sensitive system because it maintains, uses, disseminates PII from members of the public which are vendors that conduct business with the FAA and may use their own name, address, phone number for their business contact information, including the DUNS Number. All PII maintained in CWP comes from other systems and is not collected from the individual by CWP. All consent mechanisms, including Privacy Act Statements (PAS), are handled by the systems that collect the information.

The substantive information in CWP is not subject to the Privacy Act because it is not retrieved by individual name, address, phone number, or any other PII field.

Records for login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the CWP program and/or manage the system are subject to the Privacy Act and covered by SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002).

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.

[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

CWP is only available on the FAA intranet, and only accessible by FAA employees and contractors. When a FAA employee or contractor user first attempts to login and gain access to CWP, CWP initially collects (name, FAA phone number, FAA email, and their FAA manager) via a data exchange with Active Directory. Once logged into CWP, using their Personal Identity Verification (PIV) card, FAA employees and contractors can only change, or request changes, to their own PII in the system (e.g., user's work phone number). CWP has staff who handle any Helpdesk questions, including any errors in data.

Members of the public (vendor) information is imported from PRISM, where it is not directly obtained from the vendor. There is no facility in CWP to validate or overwrite the vendor information automatically. Only the project manager can have the vendor information modified and they must contact the helpdesk to have the vendor information changed. The Helpdesk staff verify the identity and legitimacy of the need before changing any vendor information.

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 FAA Administrator to develop systems and/or tools that manage the project management lifecycle to meet FAA's business needs. CWP addresses the unique demands of the FAA's workforce and operates under 49 United States Code (U.S.C.) 40101; 49 U.S.C. 40104; and 49 U.S.C. Chapter 471.

CWP contains project management information about various FAA projects. The system notifies FAA employees and contractors, who are on projects in the system of updates and requirements for their attention. The PII below is used to allow CWP and the other members to manage projects and contact individuals on the projects. The information is all work-related:

- FAA User ID
- Full Name
- Title
- FAA Phone Number
- FAA Email Address
- FAA Manager Name
- FAA Manager FAA Phone Number

CWP also has information about vendors that conduct business with the FAA. If the vendor is using their personal information for their business, it is maintained in CWP. This information is used to contact the vendor or manage projects. The PII below is used to allow

CWP and the other members to manage projects and contact individuals on the projects. The information is all work-related not collected directly from the vendor.

- Vendor/Business Name (could be an individual's name, ex. Sole Proprietor)
- Customer ID
- Business Phone Number
- Business Email
- DUNS Number

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.

CWP receives, via data exchanges, and maintains the minimum amount of information from FAA employees and contractors and members of the public (vendors that do business with the FAA) to support FAA's project management needs.

CWP is used to manage FAA projects, and the information maintained is used only for the systems with that specific information. If an employee and/or contractor is involved in more than one project, their name and contact information will be available for both projects, but not any other project. Only FAA employees and contractors, who are approved by a project manager, are allowed to access to the information in CWP. Vendor information is only maintained for specific vendors used by the projects that are included in CWP.

Information in CWP for the primary purpose of the system is covered under National Archives and Records Administration (NARA) N1-237-09-23, *Financial Records Disposition Schedule*. *Financial Reporting records*, Item 8a, are temporary, with a cut off at the end of the Fiscal Year in which records supports. The records are destroyed seven years after cut-off in accord with applicable federal standards in accord with limitations on civil actions by or against the U.S. Government (28 United States Code 2401 and 2415) if no longer required for business purposes. All other related electronic records may be retained as long as needed for business purposes and no longer than 7 years after the cut off period. Additionally, *Reimbursable records*, Item 5, are temporary, with the cut off at the end of the Fiscal Year (FY) in which the reimbursable agreement was closed. Destroy seven years after cut off in accord with applicable federal standards in accord with limitations on civil actions by or against the U. S. Government (28 U.S.C. 2401 and 2415) if no longer required for business purposes. All other related electronic records may be retained as long as needed for business purposes and no longer than seven years after the cut-off period.

Information in CWP such as login credentials, audit trails, and security monitoring are retained until business use ceases in accordance with NARA GRS 3.2, *Information Systems*

Security Records, *System Access Records*, which are temporary records to be destroyed when business use ceases, under DAA-GRS-2013-0006-0003.[4]

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 FAA/DOT limits the scope of information maintained in CWP to support the FAA's project management business needs. CWP only collects business contact information about FAA employees and contractors as needed for the projects in the system. The information is used when appropriate in the project reports, and to contact the members about any changes in the project or project responsibilities. The vendor information is only maintained for a specific project, and only used by project members to verify or contact the vendor. There are no other uses of the PII, and permissions are set such that only the members of a project can only see the information for their project.

Access, authentication, and audit log records within CWP are handled in accordance with SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002). In addition to other disclosures generally permitted under 5 U.S.C. §552(a)(b) of the Privacy Act, all or a portion of the records or information contained in the 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 an approved investigation of improper access or usage of DOT computer systems.

The Department has also published 15 additional routine uses that apply to all DOT Privacy Act systems of records, including this system. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, and 77 FR 42796, July 20, 2012, under "Prefatory Statement of General Routine Uses."

Finally, the FAA periodically reviews the collection, use, and disclosure of PII through its periodic review of this PIA and a Privacy Threshold Analysis (PTA).

[4] Approved January 2023.

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).

Most PII is not entered into CWP by any user but obtained via data exchanges. CWP automatically obtains FAA employee and contractor user information from Active Directory, via a data exchange, when a user first logs into CWP. The data is assumed accurate when it is transferred from Active Directory. Users can change some of their information themselves or contact the Helpdesk to change it.

The members of the public (vendors that do business with the FAA) information is obtained indirectly from a data exchange and is assumed accurate when it is transferred from PRISM. For vendor information, only the appropriate managers of a given project can contact the Helpdesk to change that information.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020 (includes updates as of Dec. 10, 2020).

All the data in CWP is encrypted at rest and in transit. Data is only accessible to people with a need to know (such as people on a project can see the vendor information and member contact information for that project). Segregation of duties is done so that CWP administrators cannot make changes that are not noted by other administrators. The hardware of the system is in a locked machine room, detailed in the System Security Plan (SSP).

Implementation of various operational and technical controls assures user accountability, including annual user security awareness training, user acknowledgement and adherence to the Rules of Behavior, interconnection agreement or Memorandum of Understanding (MOUs) with downstream systems, and the system administrators regularly reviewing the system/application logs for anomalous activity.

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 needed as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with CWP 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, as well as FAA Order 1370.121B. The FAA conducts periodic privacy compliance reviews of CWP as related to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource.*

Responsible Official

Fred Gomez
System Owner
Manager, Capital Systems Budget Branch (ABP-330)

Prepared by: Barbara Stance

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer