U.S. Department of Transportation

Privacy Impact Assessment
Federal Aviation Administration
Office of Information & Technology Services (AIT)
Proofpoint Federal Production Environment (FPE)

Responsible Official

Rhitu Bhardwaj
Email: rhitu.bhardwaj@faa.gov
202-875-9516

Reviewing Official

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

Executive Summary

The Federal Aviation Administration's (FAA) Proofpoint Federal Production Environment (FPE) is a cloud-based service that, before November 1, 2022, provided secure archiving, search and e-discovery, and enforcement capabilities for email messages that were processed through the FAA's email system, Microsoft Office 365 (M365). This Privacy Impact Assessment (PIA) is being performed because FPE maintains personally identifiable information (PII) on members of the public who corresponded with the FAA through email.

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 Proofpoint Federal Production Environment (FPE) is a commercial-off-the-shelf (COTS) email archiving system that previously archived all FAA emails since the FAA's migration to Outlook. Copies of all emails sent or received through FAA email accounts were created and stored in FPE, including the email of FAA and other government employees, contractors, and members of the public who corresponded with the FAA through email.

As of November 1, 2022, the FAA transitioned to a new email archiving solution, and no new archiving is occurring in FPE. Therefore, the archive is now static. Emails archived between 2013 and November 1, 2022, remain stored in FPE, where they will remain available to the FAA until they are eligible for destruction or transfer to the National Archives and Records Administration (NARA).

Email messages stored in FPE could include the user's full name, email address, and any other information contained within the message or included as an attachment. The FAA anticipates that the content of email messages and attachments could include social security numbers (SSN), credit card numbers, financial information, and other sensitive personally identifiable information (PII), included at the discretion of the email's sender. FPE archived email messages and their attachments; it did not archive other M365 data, such as calendars and instant messages.

FAA's M365 used a method of email archiving called "Mail Journaling," which is the process of creating a copy of all email traffic. A typical FPE transaction occurred each time a message was sent or received in M365, a copy of the incoming or outgoing message was created and sent to FPE via a secure channel before the message gets delivered to the intended recipient. FPE is maintained by approximately seven authorized users, with privileged roles as system administrators, security administrators, and eDiscovery administrators. There are also general support personnel (FAA employees and contractors) who have non-privileged read-only access. All access to the FPE requires the use of a Personal Identity Verification (PIV) card. The FAA emails archived in FPE are encrypted. Proofpoint, the FAA contractor that owns FPE, cannot access the encryption keys to decrypt these messages. Therefore, Proofpoint does not have access to any FAA email content.

FPE provided a limited reporting capability and produced reports regarding the size of the message archive, number of messages archived, number of users, system uptime/downtime, etc., which system and network administrators used to monitor the FPE performance.

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 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[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.

The FAA employs multiple techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains their PII within FPE. Information about responsibilities in emailing is provided to FAA employees and contractors via broadcast communications. The FAA also requires all employees and contractors to take annual security training, which includes information about data protection responsibilities. The FAA's FPE implementation is not accessible to anyone outside the FAA. It, therefore, does not provide notice directly to those individuals who are not FAA users whose information it contains. FAA users also receive notification of the proper use of government systems through training, instructions, Rules of Behavior, FAA M365 governance documents, and the FAA Order 1370.121B, FAA Information Security and Privacy Program & Policy.

FPE's access-related records about FAA users are maintained in accordance with the Department's Privacy Act System of Records Notice (SORN), DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002, 67 FR 30757. FAA-M365 is not a Privacy Act system of records that maintains Privacy Act records about members of the public.

The publication of this PIA further demonstrates DOT's commitment to providing appropriate transparency regarding handling such information.

[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

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 who send emails to FAA email accounts do so voluntarily and are responsible for the accuracy of the information they send to the FAA. Once the FAA receives an email and it is archived in FPE, it cannot be deleted. If an email contains a virus or is otherwise corrupt, authorized FAA employees with high-level administrative access to FPE can effectively hide the email from view or access from anyone but that single administrative user. However, individuals wishing to correct information within emails already sent to the FAA are not able to correct them in FPE. They may, however, send follow-up emails to the intended recipients to explain any inaccuracies.

Finally, additional information about the Department's privacy program may be found at www.transportation.gov/privacy.

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

FPE, as the M365 emailing archive, maintains PII about FAA users, as well as members of the public, pursuant to the Administrator's authority under 49 United States Code 322, *General Powers*, and 49 United States Code 40101, *Policy*. The FAA collected and still maintains information on FAA employees and contractors for the purpose of account creation and access to the system. The collection and maintenance of emails, including those containing PII, within the system furthers FAA business and allows employees and contractors a communication method to perform their official duties. Data in FPE may include but is not limited to, the following PII on FAA users and members of the public: Name and business contact information, email addresses, and email messages (including pictures or attachments containing any PII sent or received from an email address).

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 collected and still maintains in FPE only the minimum amount of information necessary for the FAA to perform its aviation safety, policy, personnel management, and other activities.

The FAA adopted the National Archives and Records Administration (NARA) Capstone approach in December 2020, and this was approved by the Archivist of the United States on February 12, 2021 (this approach allows an agency to categorize and schedule email based on the work and/or position of the email account owner) and General Records Schedule (GRS) 6.1, *Email Managed Under a Capstone Approach* (currently in draft format) to manage official email. There will be two email retention dispositions:

- Capstone Officials: Permanent for senior-level officials
- Non-Capstone Officials: Temporary (7 years), but longer retention is authorized if required for business use.
- Support and/or administrative positions: Temporary. Delete when 3 years old, but longer retention is authorized if required for business use.

This NARA approved GRS 6.1 schedule has been deployed within the FAA's M365 Exchange Online Environment and has not been adopted within the FPE. FAA is currently working towards implementing its Capstone email retention policy; at this time, archived emails within FPE - spanning from 2013 to November 1, 2022 - have yet to be subject to GRS 6.1 retention dispositions.

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.

Emails, and the information contained in them, are not considered Privacy Act records. However, PII and Privacy Act information could be contained within emails or their attachments. The FAA shares Privacy Act information contained within emails in accordance with the Privacy Act and the system of records notice (SORN) that applies to that particular Privacy Act information. Likewise, the FAA shares PII internally only with those who have a need to know.

The FAA shares email records containing PII and Privacy Act information only with those who have a need to know for official business purposes. For example, the Office of Security and Hazardous Materials Safety (ASH) has administrative access to emails within FPE; ASH can search and collect archived emails for internal FAA or DOT security, personnel, or other investigations.

This information is shared outside of the Department of Transportation in accordance with applicable law and FAA and DOT policy, depending on its contents. Information within emails might be disclosed to the public pursuant to Freedom of Information Act requests if it does not fall under a FOIA exemption. ASH can also search and collect data to share with other government entities in response to law enforcement, security, and oversight requests. Finally, the Office of Chief Counsel preserves, searches, and collects data for litigation support. The information may be disclosed as part of litigation proceedings.

With respect to FAA user account information, 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 an approved investigation 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 negotiation 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, 77 FR 42796, July 20, 2012, and 84 FR 55222, October 15, 2019, under "Prefatory Statement of General Routine Uses."

FPE authentication is done via MyAccess (SiteMinder). M365 receives the FAA employee and contractor work contact information to ensure that Outlook emails are adequately addressed and delivered to each recipient. System logs are shared with the FAA Security Operations Center for security purposes.

The FAA has authorized the internal sharing of all data associated with emails, including but not limited to all text, documents, and image files between M365 and FPE. M365 includes data loss prevention services designed to prevent users from sending PII and sensitive information outside of the Agency via email.

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).

The archive is now static. All emails are maintained as "read-only." However, when the system was active, data quality assurance activities were performed by the users of M365 and the individuals who corresponded with the FAA.

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.

FPE implements administrative, technical, and physical measures to protect against loss, unauthorized access, or disclosure. The principle of least privilege (which limits access to only that which is required to perform job duties) is used to grant access to FAA federal employees and contractors, and user actions are tracked in the M365 audit logs. All data is maintained in "read only" format. FPE PII is hosted in a Federal Risk and Authorization Management Program (FedRAMP) cloud environment, which has advanced requirements and processes in place for the protection of PII.

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.

The FAA's AIS Governance Division is responsible for the administration of FAA Order 1370.121B, *FAA Information Security and Privacy Program & Policy*. FAA Order 1370.121B defines the various privacy requirements of the *Privacy Act of 1974*, as amended (the Privacy Act), the *E-Government Act of 2002* (Public Law 107-347), the *Federal Information Security Management Act (FISMA)*, DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information technology management policies and procedures.

In addition to these, other policies and procedures will be consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance on their duties as they relate to collecting, using, processing, and security privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training. In addition, staff are required to acknowledge understanding of the FAA Privacy Rule of Behavior (ROB) and agree to them before being

granted access to FAA information systems. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of FPE relative to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Rhitu Bhardwaj
System Owner
Manager, AIF-510 - 365 Productivity

Approval and Signature

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