U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Information & Technology Services (AIT)

FAA Microsoft Office 365 (FAA-M365)

Responsible Official

Johnny Robeaux
Email: johnny.robeaux@faa.gov
Phone Number: 405-954-2461

Reviewing Official

Karyn M. Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Federal Aviation Administration's Microsoft Office 365 (FAA-M365) is a Microsoft cloud-based Software as a Service (SaaS) solution, through which the FAA is deploys a suite of communication products. FAA-M365 includes the following Microsoft Office 365 products: Word, Excel, OneNote, Teams, OneDrive, Exchange Online (Outlook), Power Platform, Bookings, Graph, Dynamics 365, SharePoint Online, Planner, Intune, Add-Ins, Compliance Manager Module, Security Portal, eDiscovery, and Records Management. These products provide communication, collaboration and standard job tools for FAA employees and contractors while performing their job duties.

This Privacy Impact Assessment (PIA) is being performed because FAA-M365 collects, maintains, and disseminates personally identifiable information (PII) about members of the public who correspond with the FAA via email, or whose information is maintained in the various FAA-M365 collaboration tools or repositories.

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:

[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).

- *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

FAA-M365 is a cloud-based software as a service (SaaS) used by the FAA to provide enterprise messaging and collaboration solutions to support agency's business needs. FAA-M365 is deployed in the FAA Cloud Services Amazon Web Services GovCloud.

FAA-M365 is only available for use by authorized FAA employees and contractors within the FAA network or via multi-factor authentication when outside the FAA network. Users access and authenticate into FAA-M365 using their Personal Identity Verification (PIV) card through Integrated Windows Authentication (IWA). FAA-M365 Service Administrators coordinate with Global Administrators (GAs) via email to assign user roles and permissions to FAA personnel for specific services. GAs add user roles and permissions by creating a Help Desk ticket with the Service Administrator's approval. GAs can only change user settings for specific services within the FAA-M365 suite of services. FAA personnel can also access their email via http://webmail.faa.gov on a non-Government Furnished Equipment (GFE) device connected to the Internet, like a Personal laptop or smartphone, through Microsoft's multi-factor authentication (MFA). FAA personnel's use of FAA-M365 is subject to the FAA Rules of Behavior, which are included in the Security Awareness Training that each FAA employee and contractor must complete annually.

FAA-M365 Products

Microsoft Outlook/Exchange Online (including Address Book, Calendar, Tasks, Notes, and Journal)

Microsoft Outlook/Exchange Online is a messaging solution that gives all FAA employees and contractors access to email, contacts, calendars, tasks, notes, and journaling functions. Microsoft Outlook/Exchange Online integrates fully with Active Directory (FAA Directory Services), which enables system administrators to manage Microsoft Outlook/Exchange Online services across their environment. Microsoft Outlook is the email application

accessed from a user's desktop or through a web client via Integrated Windows Authentication (IWA). Users access the web client when they enter their domain/username and password. Microsoft Outlook allows users to create, read, send, reply, or forward email messages to other FAA personnel or members of the public. Senders or recipients of email messages could, at their own discretion, include personally identifiable information (PII) within the message contents or email attachments, including but not limited to: Full name, company/organization, telephone numbers (business, mobile, or personal), business fax number, physical or mailing address, department/office, FAA Contractor Officer full name, contract number, contractor company, Social Security Numbers (SSNs), Airmen Certificate Numbers, Financial Information (account numbers, credit card numbers), employee personnel information, and medical information.

FAA personnel are required to abide by the FAA Rules of Behavior regarding the disclosure of PII in email communications and will validate requestor's need-to-know before providing PII. FAA Order 1370.121A, *FAA Information Security and Privacy Program & Policy, and FAA Rules of Behavior* provides guidance specific to the use of Microsoft Outlook/Exchange and requires that:

- Users must agree to encrypt any email and attachments which contain PII before sending the email;
- Users agree not to exceed their authorized access to PII and not disclose PII to unauthorized persons; and
- Users must acknowledge that FAA Internet and email is for official use, with only incidental personal use permitted.

All outbound email messages are monitored by data loss prevention services within M365, which is used to prevent FAA senders from emailing sensitive information such as SSNs or credit card numbers outside of the agency.

Microsoft Outlook includes the following features:

Address Book - Address Book is an online contact directory that allows users to store and find names, addresses, and telephone numbers. Users can create an individual contact entry or create a group contact list. Users may forward and share contacts via email with other FAA personnel and members of the public.

Users may also use contacts to map and view an address location that is included in their contacts lists. Address Book may include the following PII: full name, company, job title, email address, web page address, business and home phone numbers, photograph, and notes. Optional fields can contain additional PII, which

occurs when the User enters the information, such as spouse's name, birthdates, anniversaries, and children, or user-defined fields (the user can create their own fields with personalized prompts (i.e., Grandmother's birthday). Address Book allows users to change privacy relationships to control how much information others can see. The default setting is *Colleagues*, which shares all work-related contact information except for meeting details, but users can choose other options to share additional information, such as home or personal cell phone numbers, if entered by the User, or block all information, except for their name and email address.

Microsoft Calendar - Microsoft Calendar is an online calendar application that allows users to schedule appointments and meetings. Users may share their calendar, request to view another user's calendar, or access group calendars in which they are a member. Users can include an email, business card (or contact), view or insert a calendar entry, insert a journal entry or note, or include a copy of a Microsoft Teams online conversation when creating a meeting invite.

Microsoft Calendar may include personal contact information, such as company name, organization, titles, personal and business phone numbers, personal or business addresses, and personal or business email addresses. Users are trained (through annual Security and Privacy Awareness Training) to limit PII disclosure based on provided guidance through the FAA Rules of Behavior (section 3) acceptance and training.

Microsoft Tasks - Microsoft Tasks allows users to create a "to do" item, organize and prioritize tasks, create notes related to the task, flag the task for follow-up, track the item to completion or create recurring tasks. Users may also create tasks for other individuals. When users create a task, they can include any Microsoft Outlook item, such as an attachment, email, calendar entry, business card (contact info), note, journal, etc.

Microsoft Notes - Microsoft Notes is a limited note taking application integrated within Microsoft Outlook that allows users to record ideas, reminders, or text. Users cannot attach any items such as calendar, journal, or business cards to Microsoft Notes.

Microsoft Journal - Microsoft Journal can be used to automatically record user-selected actions for specific contacts, placing those selections in a timeline view. Users can view emails from individuals set to be recorded in the Journal folder, and see calendar appointments, tasks, and contacts. Users can create or view a Journal

entry; they may also insert a Microsoft Outlook item into the Journal entry, such as email, attachment, business card, or calendar entry.

Microsoft O365 Apps (Word, Excel, and OneNote)

Word - Microsoft Word is a word processor that includes a variety of widely used features, including a built-in spell checker, thesaurus, dictionary and other utilities used for editing. Word documents can include any PII that the user manually inputs and can be saved in accordance with the general FAA Rules of Behavior, on various FAA drives (such as restricted drives or program specific drives), and in Microsoft OneDrive.

Excel - Excel allows users to develop and manipulate spreadsheets and has features including calculating and graphing tools and pivot tables. Excel documents can be saved in accordance with the general FAA Rules of Behavior on various FAA drives (such as restricted drives or program specific drives), and in Microsoft OneDrive.

OneNote - OneNote is a note-taking program for free form information gathering. Users can utilize shared notebooks to collaborate. Notes within OneNote can include text, pictures, drawings and tables. Users can choose to manually input any PII into OneNote, in accordance with the general FAA Rules of Behavior.

Microsoft Teams

The FAA-M365 Microsoft Teams service provides an integrated communications platform for FAA employees and contractors to video conference, voice call, instant messaging (IM), access other FAA-M365 service components (OneDrive and SharePoint), and share files and documents with others, either inside or outside the FAA organization. The DOT Teams Chat Federation component allows FAA users to collaborate with DOT users.

Any individual, either FAA personnel or a member of the public, with a business or consumer email account can participate as a guest in Microsoft Teams. Members of the public (external guests) can join meetings scheduled and hosted in Microsoft Teams. The external guest cannot download files attached to meetings in Microsoft Teams. An individual with faa.gov email credentials must admit external guests who try to access a meeting hosted in Microsoft Teams into the meeting. FAA personnel may send links to download files or copy text into an IM, provide information work status (i.e., busy, available, in a meeting, offline), and set the user's location, such as in the office, teleworking, or another location.

Microsoft Teams automatically adds files shared within a Teams chat or IM to the document library, and permissions and file security options set in SharePoint are automatically reflected within Teams. Microsoft Teams identifies FAA personnel by their full name, address, and allows users to enter free-form text into Teams via IMs (including links to download file attachments), and activity feeds. Microsoft Teams may collect, based on the user's or guest's discretion, telephone numbers, company name, supervisor, office location, and other PII that could be disclosed in an IM or shared document. FAA personnel have the option of including a photograph of themselves within their profile listed in Teams. Microsoft Teams online conversations are saved in the user's Conversation Folder within Microsoft Outlook. FAA finalized the Teams Governance Plan on August 25, 2021. In accordance with the Governance Plan, Teams users are responsible for:

- Ensuring that Teams groups and content comply with all provisions of FAA Order 1370.121 or its successor, FAA Information Security and Privacy Program & Policy.
- Ensuring that permission to content is granted at the lowest level required: do not grant permissions that the person accessing the document does not need. It is the responsibility of the Team group owners and members to ensure compliance with Order 1370.121 or its successor.

SharePoint Online

SharePoint Online (SPO) provides FAA a customizable platform to securely manage, share, and collaborate on files and other content from anywhere on any FAA managed device. SharePoint Online sites remain available to all FAA employees and contractors until no longer required by the office, team, or project. SharePoint online may share information, such as PII, in the form of reports, contact information, and files. SharePoint Online allows FAA employees and contractors to share information, organize projects and teams, and discover people and information. FAA finalized the SharePoint Online Governance Plan on August 25, 2021, to provide guidance for appropriate use of the SPO environment. The FAA is working to implement data loss prevention features within M365 that will scan SharePoint Online for sensitive information and PII.

Microsoft OneDrive

FAA-M365 deploys Microsoft OneDrive as an online, cloud storage site to store work files created, edited, and/or received by an FAA employee or contractor. FAA personnel can access their OneDrive file from many locations across FAA-M365, including Microsoft Teams. All FAA employees and contractors with an FAA domain account have access to OneDrive.

OneDrive cloud storage is available from within the FAA network or while users connect to the FAA's Virtual Private Network (VPN) only. The files in OneDrive are private by default and viewable only to the file creator. Files stored in OneDrive may be shared, collaborated on, and synchronized to a user's GFE device for offline use. When the owner of a OneDrive leaves the FAA and their Active Directory account is deleted, ownership of the OneDrive content is transferred to the employee's manager on file in Employee Information System (EIS)/MyProfile for 90 days, after which it is deleted. Users can share files in their OneDrive only with other FAA employees and contractors who have an active directory account. OneDrive allows the synchronizing of files to a local computer. OneDrive allows users to store all types of electronic files, including text, graphical, audio, and video files. OneDrive may contain PII data within these stored files. The use of OneDrive is the same as the FAA's traditional use of file servers hosted in FAA data centers.

PII present on OneDrive can, but is not limited to, FAA employee/contractor name, FAA email address, business phone number, and building/location. Additionally, as a storage site, FAA employees/contractors can store electronic files relevant to their job duties, pursuant the policies described below, which could include a broad range of PII. FAA Order 1370.121A, FAA Information Security and Privacy Program & Policy, Appendix 21, and FAA Rules of Behavior provide guidance to the use of OneDrive within the FAA. FAA finalized the OneDrive Governance Plan on August 25, 2021, to ensure the system is used in accordance with its designed intent. The FAA is working to implement data loss prevention features within M365 that will scan OneDrive for sensitive information and PII.

Microsoft Power Platform

Microsoft Power Platform enables users to analyze data, deploy data and applications via dashboards, automate workflows, and integrate with data in SharePoint Online on users' desktops or file shares. Power Platform is a suite of Microsoft services comprised of Microsoft Power BI, Microsoft Power Apps, Microsoft Power Automate, and Power Virtual Agents. Only access data (FAA employees' and contractors' name, FAA email address) is maintained within the Power Platform. The FAA has implemented a new checklist process that guides users developing Apps through various security and privacy requirements, including requiring Privacy Threshold Assessments or Privacy Impact Assessments, where necessary.

> ***Microsoft Power BI -*** Power BI contains a collection of software services, apps, and connectors that work together to turn unrelated sources of data into visually immersive and interactive insights. Power BI allows data sources to be shared with any individual of the user's discretion. Power BI consists of (1) Power BI Desktop,

(2) Power BI service (online SaaS), and (3) Power BI mobile apps of Windows, iOS, and Android devices.

Microsoft Power Automate for O365 - Power Automate enables the creation of automated workflows between applications and services to synchronize files, receive notifications, and collect data.

Microsoft Power Apps for O365 - Power Apps is a suite of applications, services, connectors and a data platform that provides an environment to build custom applications for specific business needs. Power Apps allows the user to connect to their business data in the underlying data platform or in various online data sources, such as SharePoint and OneDrive.

Dynamics 365 - Dynamics 365 allow users to build their own apps by using a "point and click" app creation experience that automates developmental workflows. These applications do not directly collect any data. Developers at the FAA use the Microsoft Power Platform to develop applications. These developers may populate applications they have developed with PII from SharePoint Online, or OneDrive, but their use of that PII is governed by the FAA SharePoint Online and OneDrive Governance Plans, as discussed above.

Microsoft Graph

Microsoft Graph is an application-programming interface (API) platform that interacts and allows access to data on the following FAA-M365 cloud services: OneDrive, Excel, SharePoint, Microsoft Teams, Excel, Workplace Analytics, Outlook/Exchange, Planner, and Dynamics. The API can be used to connect plugins, scripts, or other applications to FAA-M365 data sources. Access to Microsoft Graph is provided to authorized FAA personnel and application developers through an approval process administered by the FAA's Data Governance Division (ADO-010).

Microsoft Graph does not directly collect any PII; however, the full name, job title, email address, and phone number are maintained within the application. Access requests for higher-level permissions for plugins, scripts, and applications, which would allow a user to view other data on users, requires a user to follow the appropriate governance and/or intake processes.

Microsoft Planner

Microsoft Planner is a team and task management service. It allows a user to create and assign tasks. It also allows a user to add statuses, priority, due dates, notes, checklists, etc. to tasks. Groups of users can collaborate on a task, if they have the appropriate permissions. PII on users and individuals who collaborate on tasks may include name, FAA email address, phone number, and location. Users can attach items to a task, including documents and electronic files they have downloaded from OneDrive or SharePoint. PII is expected to be present in these electronic files and documents, subject to the FAA's applicable Governance Plans and privacy and security policies.

Microsoft Intune

FAA uses Microsoft Intune as a cloud-based service for mobile device management (MDM) and mobile application management (MAM) for GFE, specifically Apple iPads and iPhones. Intune administrators manage enrolled mobile devices to restrict access, add mobile devices, and remove FAA data on lost or stolen devices. Intune integrates with FAA's Active Directory to control who has access to FAA-M365. Intune allows users to deploy Microsoft Teams or other FAA-M365 applications and services to their mobile devices. Intune sends out compliance policies and notifications to FAA personnel with registered GFE devices. A notification to change the Personal Identification Number (PIN) of a device every 90 days would be a push notification example. Intune does not collect any new information that is not already contained within FAA-M365. Intune generates tracking reports about the security health of devices. These reports contain the full names of FAA employees, work email addresses, and device IDs.

Add-Ins

FAA Uses Add-Ins to create interactive objects, such as embedded maps and charts, custom ribbons, and menu buttons in task panes. The only PII present in Add-Ins is FAA employee and contractors' name and FAA email address.

Microsoft Compliance Manager Module

The FAA's Office of Information Security and Privacy, Security Compliance Division (AIS-200) uses the Microsoft Compliance Module to assess the status and implementation of the National Institute of Standards and Technology (NIST) 800-53 Security and Privacy Controls within FAA-M365. The Compliance Manager Module manages the implementation of security controls to comply with regulations and provide audit reporting. The Compliance Manager Module calculates a "Secure Score" of implemented controls

based on the implementation actions. AIS-200 uses this score to inform and guide the implementation of key improvement actions.

AIS-200 inputs implementation notes within the module, which consists of "copying and pasting" sections of the FAA-M365 Security System Plan (SSP). Users can upload documents into this module to assist with implementation documentation of controls. No PII collection is present within the Compliance Manager Module.

Microsoft Security Portal

FAA uses the Microsoft Security Portal to identify and combat security threats by using analytics. The only PII present in the Security Portal is FAA employees' and contractors' names and FAA email addresses.

eDiscovery

FAA uses eDiscovery to search, identify, and deliver electronic information located in other FAA-M365 services to FAA's Office of the Chief Counsel (AGC) and the FAA's Office of Security and Hazardous Materials Safety (ASH) for use in legal cases. FAA personnel use eDiscovery cases to identify, hold, and export content found in mailboxes and other FAA-M365 services. eDiscovery does not create new records. PII present includes user information, such as name and FAA email address.

Microsoft Bookings

Microsoft Bookings allows users to create and publish schedules, allowing individuals to sign up for certain meetings/events, or book time slots with others. To book an event, a user will receive an email that there is an event available for booking. Users are limited to FAA employees and contractors. The user will then manually input their name, FAA email address, service location, and phone number to reserve a time slot. Once they submit their booking, an auto-generated email with their name and booking information will be sent to them. Administrators cannot search for an individual who has made a booking by personal identifier.

Microsoft Whiteboard

Microsoft Whiteboard allows Teams users to simulate a traditional whiteboard and draw pictures and charts. The pictures and charts drawn can then be shared with individuals within Teams.

MS Forms

MS Forms is an application that allows users to easily create surveys, quizzes, and polls and use built in analytics to evaluation responses as they are submitted. Forms also allows users to export data to Excel for additional analysis. The MS Forms Governance Plan specifically requires individuals creating quizzes, surveys or polls to reach out to various groups within the FAA if conditions within the product they are creating trigger the Privacy Act, the Paperwork Reduction Act (PRA), and the Children's Online Privacy Protection Act (COPPA). If necessary, users are pointed to various offices within the FAA that can provide further guidance to ensure compliance with legal requirements. Users are also instructed to not require, transmit or store any PII, sensitive Security Information (SSI) or Sensitive Unclassified Information (SUI) within the quizzes, surveys or polls.

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.

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 FAA-M365. Information about the FAA-M365 program 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

[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

protection responsibilities. FAA's Office 365 implementation is not accessible to anyone outside of FAA and, therefore, does not provide notice directly to those individuals who are not FAA users whose information it contains.

FAA-M365 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 30758. 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 provide 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.

FAA users receive notice of proper use of government systems in the form of training, instructions, Rules of Behavior, FAA M-365 governance documents, and the FAA Order 1370.121A, FAA Information, Security and Privacy Program & Policy. FAA users have access in the various FAA-M365 products to their own information. For example, Exchange Online user data can be accessed via Outlook. The Global Address Book is an aspect of Microsoft Outlook; an individual FAA user is encouraged to review their entries in the Global Address List (GAL) to make sure the information is up to date and correct. They can update certain information on FAA's Intranet site or by contacting the FAA's Helpdesk to have this information corrected on the GAL. To remove an employee from the GAL, requests must be submitted through the Help Desk.

FAA's Office 365 implementation is not accessible to anyone outside of FAA and, therefore, does not provide redress directly to those individuals who are not FAA users whose information it contains.

Additionally, individuals may request searches to determine if any records appear in any 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.

FAA-M365 collects, maintains, uses, or disseminates 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 collects and maintains information on FAA employees and contractors for the purpose of account creation and access to the system. The collection and maintenance of PII within the system for other purposes is collected and maintained when needed to further FAA business. FAA-M365 may include, but is not limited to, the following PII on FAA users and members of the public: Name and business contact information, email messages (including pictures or attachments containing any PII sent or received from an email address), logging information, the content of instant messages, and any PII present in documents saved in collaboration portals or repositories (including, for example, OneDrive, PowerPoint, or SharePoint Online). Logging information (such as usernames and Internet Protocol address) could be maintained on FAA users.

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 maintains only the minimum amount of information necessary for the FAA to perform its aviation safety, policy, personnel management and other activities. Due to the range of FAA-M365 products and the data present in those products, various retention schedules may be applicable.

The system access records are retained and disposed of by the FAA in accordance with National Archives and Records Administration General Records Schedule 3.2, item 130, *Information Systems Security Records*. These records are destroyed when business use ceases. General Technology Management Records are maintained pursuant to General Records Schedule 3.1, items 011 and 020. Records maintained under item 011 are destroyed 5 years after being superseded by a new system. Records maintained under item 020 are destroyed 3 years after the project is concluded. Records containing PII extracts are destroyed in accordance with General Records Schedule 4.2, item 130, *Information Access and Protection Records*. These records are destroyed when 90 days old or no longer needed to supervisory authorization, whichever is appropriate. Emails are retained pursuant to General Records Schedule 6.1, items 10 and 11, *Email Managed Under a Capstone*

Approach. These records are either maintained as permanent and are transferred to NARA 15-25 years after declassification review (when applicable), whichever is later, or deleted when 7 years old.[4]

Records contained within OneDrive for Business and SharePoint Online are retained and disposed of in accordance with the applicable agency records schedules or GRS approved by NARA for each type of record based on the subject or function and records series. In accordance with Order 3370.5B, FAA Close Out and Clearance Process (or successor Order), users who are departing the FAA, or moving to another position in the FAA, must notify their manager of record of their departure. Upon separation, access to their OneDrive will be transferred to their manager for 90 calendar days before it is permanently deleted.

M365 includes data loss prevention services designed to prevent users from sending PII and sensitive information outside of the Agency, via email. The data loss prevention services will also provide scanning to repositories such as OneDrive and SharePoint Online to prevent the unnecessary maintenance of sensitive PII such as social security numbers.

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.

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 form the Federal government, when necessary to accomplish an agency function related to this system of records; and

[4] The National Records and Archives Administration (NARA) recently approved FAA's Capstone records schedule; the FAA is now working to implement the retention schedule. At the time of publication of this PIA, email records are maintained indefinitely as unscheduled records.

- 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."

The FAA Directory Services (FAA DS/Active Directory) exchanges authentication data with FAA-M365 via Integrated Windows Authentication. FAA-M365 receives the FAA employee and contractor work contact information to ensure that Outlook emails are properly addressed and delivered to each recipient. FAA-M365 sends to FAA DS the user's FAA domain username and password when the user authenticates with their PIV card from their GFE. System logs are shared with the FAA Security Operations Center for security purposes.

The FAA has authorized internal sharing of all data associated with emails, including but not limited to all text, documents, and image files with the ProofPoint Federal Production Environment, for archival purposes. M365 includes data loss prevention services designed to prevent users from sending PII and sensitive information outside of the Agency, via email. The data loss prevention services will also provide scanning to repositories such as OneDrive and SharePoint Online to prevent the unnecessary maintenance of sensitive PII such as social security numbers.

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).

In most cases, employees have direct control over their FAA-M365 profile information and may edit it to maintain its accuracy at any time. Other information contained in the various components of Office 365 may be presumed accurate based on its source or corroborated via other FAA systems. The individual user within the system will need to determine accuracy based on business knowledge and need. Moreover, the collaborative nature of Office 365 provides opportunities for those working together on a document, for example, to make changes to address any inaccuracies concurrently.

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 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 NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* dated January 22, 2015.

FAA-M365 implements administrative, technical, and physical measures to protect against loss, unauthorized access, or disclosure. The principle of least privilege is used to grant access to FAA federal employees and contractors, and user actions are tracked in the FAA-M365 audit logs. M365 includes data loss prevention services designed to prevent users from sending PII and sensitive information outside of the Agency, via email. The data loss prevention services will also provide scanning to repositories such as OneDrive and SharePoint Online to prevent the unnecessary maintenance of sensitive PII such as social security numbers. Additionally, the M365 G5 Security bundle provides additional endpoint security to mitigate threats and vulnerabilities.

Specifically, within SPO, the following safeguards are present:

- SPO sites are only accessible from within an FAA facility or while connected to the FAA's Virtual Private Network.
- SPO sites are only accessible from Government Furnished Equipment unless approval is granted through the waiver process outlined in FAA Order 1370.121.
- SPO sites are only accessible to FAA employees and contractors who have an active FAA PIV card.
- SPO sites are not accessible to external non-FAA users.

Additionally, within SPO, appropriate controls and mechanisms must be implemented to protect PII/SPII; including:

- Except for low-level PII such as name and business contact information, PII/SPII may not be stored as metadata in any list or library columns or as content on any page.
- Except for low-level PII such as name and business contact information, all documents containing PII/SPII stored in any SPO document library, or contained as an attachment to any list item, must be encrypted per FIPS 140-2 methodology in

accordance with FAA Order 1370.121, FAA Information Security and Privacy Program & Policy.
- All PII/SPII issues reported by Data Loss Prevention (DLP) scans conducted by the AIT Security Office and the SPO Program Office must be reviewed and remediated.

OneDrive is only accessible to the assigned user unless they choose to share specific content with their FAA colleagues. It is the user's responsibility to manage the accessibility of shared content in their OneDrive by only sharing content with other FAA employees and contractors with an Active Directory account. Similarly, users of Teams are required to follow policies regarding screen sharing during meetings, including, exercising caution when sharing screens so that other users do not see sensitive or privileged information, and not allowing external parties the ability to access, open or execute files on the host system.

FAA-M365 was given an Authority to Operate by the FAA on June 24, 2021.

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 Security Governance Division is responsible for the administration of FAA Order 1370.121A, *FAA Information Security and Privacy Program & Policy*. FAA Order 1370.121A 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 FAA-M365 relative to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Johnny Robeaux
System Owner
Deputy Director, Infrastructure and Operations

Approval and Signature

Karyn M. Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Office