



Privacy Impact Assessment for

Microsoft Office 365

September 30, 2026

Contact

Gwendolyn Wilson
Deputy Clerk of the Board
Merit Systems Protection Board
1615 M Street, NW
Washington, DC 20419
privacy@mspb.gov

Reviewing Official

Gina K. Grippando
Clerk of the Board &
Senior Agency Official for Privacy

Abstract

Microsoft Office 365 (Office 365) is a cloud-based Software as a Service (SaaS) solution through which the Merit Systems Protection Board (MSPB) will deploy various communication, collaboration, and office productivity applications for MSPB in the cloud. Office 365 has successfully completed the Federal Risk and Authorization Management Program (FedRAMP) assessment process and is FedRAMP certified. As the cloud subscriber, MSPB does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings. Office 365 includes licensing of the desktop version of the latest Office applications such as Outlook, Word, Excel, and PowerPoint, as well as OneDrive, Teams, Teams Phone, Teams Mobile Application, SharePoint, Forms, Power BI, Visio, and Copilot. MSPB does not use Office 365 to collect or maintain personally identifiable information (PII) directly from members of the public. MSPB is conducting this Privacy Impact Assessment (PIA) because Office 365, in part, collects, maintains, disseminates, or processes PII about members of the public who communicate with MSPB via email, or whose information is maintained in the various Office 365 collaboration tools or repositories.

Overview

The MSPB Office of Information Resources Management (IRM) is deploying Office 365 to provide a robust and standardized enterprise-wide suite of collaboration, communication, and office productivity tools for MSPB employees, contractors, interns, and other non-employees (collectively, “MSPB users”). Office 365 will allow MSPB to manage, access, and protect information, as well as provide scalability.

This PIA evaluates the privacy implications for MSPB’s use of the cloud-based Office 365 applications for Outlook, Word, Excel, PowerPoint, OneDrive, Teams, Teams Phone, Teams Mobile Application, SharePoint, Forms, Power BI, Visio, and Copilot. Any office or system using collaboration tools that require information beyond basic business contact information will require their own privacy compliance documentation.

Office 365 is available only for MSPB users with an MSPB username, password, and approved multifactor authentication application. MSPB Office 365 administrators coordinate with IRM via SharePoint (using the e-Support tool) to assign roles and permissions by creating an e-Support ticket. IRM staff and MSPB’s Office of Financial and Administrative Management (FAM) will determine the legitimacy of the request and assign or refuse permissions in accordance with their own internal Role Assignment Standard Operating Procedures. MSPB users may access their MSPB Office 365 account on the Web at <https://portal.microsoft.online.com> on non-Government Furnished Equipment connected to the internet. Use of Office 365 by MSPB users is subject to acceptance of the MSPB Rules of Behavior and completion of privacy awareness training, both of which MSPB provides at the time of onboarding and at least annually thereafter. See below for a detailed description of available Office 365 applications.

Office Applications

Office 365 provides the latest version of the Microsoft Office applications that MSPB personnel are familiar with, such as Outlook, Word, Excel, and PowerPoint.

- **Outlook** is a software application that manages emails, calendars, tasks, contacts, and collaboration tools. It is plugged into Office 365 and the cloud, which permits the selection of how to share the files – as an email attachment or by sending links to documents – to allow participants to work simultaneously on the same document.
- **Word** is a word-processing software application that can create, format, and edit documents, review with track changes, and share files.
- **Excel** is a software application that is a spreadsheet editor that enables users to format, organize, and calculate data in a spreadsheet.
- **PowerPoint** is a software application that allows users to create slideshow presentations from scratch or a template that combines text, images, and multimedia.

OneDrive

OneDrive is a cloud-based file storage system that offers online editing and collaboration tools for Office 365 documents. It supports more than 270 file types. Using OneDrive, MSPB users can save all their files in the cloud, which allows access from anywhere and provides protection from loss due to disk drive failure or a lost device. Due to the nature of OneDrive, users may store all types of electronic files including reports, correspondence, briefing papers, meeting minutes, contracts, audits, manuals, studies, and other documents.

Teams

Teams is a real-time, chat-based collaboration platform that is made up of channels that can be built by topic, department, or offices. Teams enables MSPB users to communicate and collaborate with colleagues in real time; share and store artifacts that they generate; access multiple collaboration tools, such as Chat and Calendar; and participate in meetings, accessing collaboration tools and content as needed to hold meetings, have conversations, and share files. Files can be shared in the channel conversation allowing the entire team to work and edit it at the same time. Chat allows users to start a new private conversation or make a video call directly from a chat or audio call. Teams Calendar syncs with Outlook's calendar and has the feature to Join a virtual meeting if the Join option is selected. During the meeting, employees can share their screen, record meetings, and request controls. Activity allows users to view alerts for unread messages, "@" mentions, replies, and voicemails. The command box allows users to search for specific items, and people, as well as launch apps.

Teams Phone

Teams Phone provides public switched telephone network (PSTN) connectivity with Teams to enable external calling and phone system capabilities in the Microsoft 365 cloud. With Teams Phone, MSPB users can make and receive calls directly from the Teams application, eliminating the need to switch between different applications.

Teams Mobile Application

The Teams Mobile Application complements the desktop experience. It allows MSPB users to access all their activities from a mobile device. On Teams Mobile, users can continue to work and collaborate with an optimized experience on their personal mobile phones. Using this application allows MSPB users to continue conversations initiated from their desktop. The mobile application allows them to record audio messages, edit and send pictures, and scan documents using their mobile phone camera. They can attend meetings on their personal or MSPB-issued mobile phone, transfer those meetings to/from their desktop, add devices, and attend meetings using Apple CarPlay or other smartphone integration software if they are in an equipped vehicle. Users can manage preferences, set up and silence notifications, see the Calendar, and join meetings directly from the Calendar.

SharePoint

SharePoint provides online collaborative sites that are visible to MSPB users and can be used to share information, some of which may contain PII, in the form of reports, contact information, training lists, and other information.

- **e-Inventory:** MSPB created e-Inventory using SharePoint to track IRM equipment. It can send selected users a private link, to which IRM manages access, to add the equipment in use.
- **e-Support:** MSPB created e-Support using SharePoint to track technical support requests. Users enter a support category, choose an issue type, rank the issue severity, enter a narrative description of the issue, and can upload files if they wish.

Forms

Forms is a web-based application that allows users to create forms, digital surveys, quizzes, polls, questionnaires, and use built-in analytics to evaluate responses as they are submitted. Forms also allow users to export data to Excel for additional analysis.

Power BI

Power BI is a unified, scalable platform for self-service and enterprise business intelligence.

Visio

Visio is a diagramming software for drawing a variety of diagrams, including flowcharts, organizational charts, building plans, floor plans, data-flow diagrams, process-flow diagrams, business-process modeling, swim-lane diagrams, 3D maps, and more.

Copilot

Microsoft O365 Copilot is a generative artificial intelligence assistant that helps users with tasks like writing, editing, summarizing, and creating. It uses large language models and integrates with a user's Office 365 data and permissions to provide real-time assistance and enhance productivity. Copilot operates within the MSPB tenant boundary, ensuring no co-mingling of data with commercial clouds or public endpoints. Sensitive information never leaves the secure MSPB instance.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The e-Government Act of 2002, section 208, *Privacy Provisions*; the Federal Information Security Modernization Act of 2014; the Paperwork Reduction Act of 1995; the Clinger Cohen Act of 1996; the Federal Information Technology Acquisition Reform Act; Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service Security Authorization of Information Systems in Cloud Computing Environments* (Dec. 8, 2011); Office of Management and Budget (OMB) Circular No. A-130, *Managing Information as a Strategic Resource*; and OMB Memorandum M-15-14, *Management and Oversight of Federal Information Technology* (June 10, 2015).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Office 365 does not require a SORN because it does not create a new system of records. Office 365 does not collect information directly from individuals, and it does not create any new information through the systems about individuals. There are specific SORNs that cover the information contained in the source systems performing the original collection.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The Chief Information Officer (CIO) completed the assessment of the system with the authority to operate (ATO) until March 2028.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, MSPB maintains records in Office 365 in accordance with applicable MSPB records disposition schedules and General Records Schedules (GRS) that NARA has approved. Due to the nature of Office 365, there may be multiple records schedules with different retention schedules, each with different retention requirements, applicable to the records created and maintained by Office 365 users. MSPB has approved plans and procedures to destroy records in conformance with applicable records schedules and NARA guidance.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not applicable.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

MSPB collects, uses, disseminates, or maintains contact information of MSPB users, other federal employees, and members of the public who communicate with MSPB via Office 365. This information may include the following data elements:

MSPB users and other federal employees

- First name
- Last name
- Middle name or middle initial
- User ID
- Office email address
- Office phone number
- Work address
- Email messages (including any attachments)
- Message log information (including IP address of sender, date, and time)
- Instant messages, which may contain a variety of information, to include PII about MSPB employees, other federal employees, and members of the public; and information stored in collaboration portals/repositories (such as spreadsheets, word processing, and PowerPoint documents)
- Logs of MSPB user activity
- Device identifiers and serial numbers

IT Technical Support - Internal to MSPB users

- First name
- Last name
- Middle name or middle initial
- MSPB office
- MSPB email address
- Office phone number

Members of the public – when submitting a disclosure request via email

- First name
- Last name
- Middle name or middle initial
- Mailing address
- Telephone number
- Email address
- Zip code
- Facsimile number

2.2 What are the sources of the information and how is the information collected for the project?

The principal sources of the information are MSPB users (employees, contractors, interns, and other non-employees), other federal employees, and members of the public. MSPB users provide the information during the onboarding process.

MSPB users may upload data during the onboarding process. User-created data may also contain information in the user's profile, emails, calendar, and other information voluntarily stored within Office 365.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Office 365 does not collect information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

MSPB relies on its users to ensure the accuracy of data, which MSPB receives directly from current employees, contractors, and interns; MSPB applicants for employment; and prospective contractors. Considering the nature of the system and the expected extensive use of these services across Office 365, each user is responsible for ensuring the accuracy of the data at the time of creation, collection, or use. MSPB will not generally check Office 365 for accuracy, completeness, or quality.

System administrators ensure that MSPB users' account information is accurate in Microsoft Entra ID, but they will not ensure that the data users create or enter is complete, accurate, or current.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: A privacy risk associated with the system is that users may store all types of electronic files that could include reports, correspondence, briefing papers, meeting minutes, contracts, MSPB hearing audio recordings or transcripts, audits, manuals, studies, or other documents.

Mitigation: This risk is partially mitigated. MPBS relies mainly on its employees who are the end users and have responsibility for their content. MSPB provides IT security and privacy awareness training at onboarding and as part of annual mandatory training.

Privacy Risk: There is a privacy risk that MSPB may receive more information than is needed.

Mitigation: This privacy risk is partially mitigated. Each MSPB user is responsible for entering or otherwise storing only the information needed to perform their authorized duties.

Privacy Risk: There is also a privacy risk that the information in the system may not be accurate.

Mitigation: This risk is partially mitigated. Office 365 is primarily dependent on end users who are responsible for the content that they create. The collaborative nature of the system and its applications naturally provide a platform where MSPB users are able to correct inaccuracies.

Privacy Risk: There is also a privacy risk of misuse of data by authorized users.

Mitigation: This privacy risk is mitigated. Before gaining access to MSPB's network, all users are required to read and accept MSPB's Rules of Behavior.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Internally – MSPB requires PII when verifying the identity of MSPB candidates for employment who send this information by password-protected email to their assigned Human Resources Specialist in FAM.

MSPB requires individuals' PII when creating their user account in MSPB's network after receiving clearance from FAM. This is necessary to control access to information entering and

accessible within MSPB's network. All MSPB offices use Office 365 to communicate and collaborate.

Externally, MSPB requires members of the public to provide PII to confirm their identity and need-to-know for any information requested under the Privacy Act or the Freedom of Information Act (FOIA).

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how MSPB plans to use such results.

MSPB does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

Apart from IRM, there are no other offices assigned with roles and responsibilities within the system. The Rules of Behavior apply to all MSPB users.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that information collected and maintained in Office 365 may be used for purposes other than its original purpose.

Mitigation: This risk is mitigated. MSPB limits inappropriate use of the information collected by limiting access and user roles within the system.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

MSPB provides its users with training and requires them to sign Rules of Behavior before accessing the system. In addition, before logging on to any MSPB system, users see the MSPB warning banner, which stipulates that users do not have a right to privacy while using the system, including internet and email services.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

MSPB does not use Office 365 to collect information, including PII, directly from the public. However, MSPB users use Office 365 to perform their assigned duties, so information collected through other sources, including PII, is maintained in Office 365. In addition, members of the public and other federal employees may provide information to MSPB, and it is totally up to the individual to determine how much or how little information they provide in any communication with MSPB involving Office 365, e.g., via email. Please see the list of the [MSPB's Privacy Impact Assessments](#) for more information on how MSPB collects information from the public.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not receive notice that the information that they and others provide about them will be maintained and used within Office 365.

Mitigation: This risk is mitigated for MSPB users via the MSPB warning banner that is displayed on all user systems before logging on to the MSPB network and via the Rules of Behavior to which all users must agree. Other individuals receive notice via this PIA and any applicable SORN, as well as notice about the collection and use of their information, as appropriate, at the point of collection.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

MSPB maintains records in Office 365 in accordance with applicable MSPB records disposition schedules and GRS that NARA has approved. Due to the nature of Office 365, there may be multiple records schedules with different retention schedules, each with different retention requirements, applicable to the records created and maintained by Office 365 users. MSPB has approved plans and procedures to destroy records in conformance with applicable records schedules and NARA guidance.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that MSPB users will retain records in Office 365 longer than is necessary to meet the business needs for which they were collected.

Mitigation: This risk is mitigated by providing training and reminders to MSPB users regarding the applicable records retention schedules. Mitigation of this risk is dependent, in part, on end users following applicable retention schedules. Where possible, IRM, working with MSPB's Records Officer, will incorporate technical means to identify and apply applicable records schedules. To the extent that any records are present in the system that do not have a current records schedule, the appropriate program office will work with the Records Officer to develop one.

Section 6.0 Information Sharing

6.1 Is information shared outside of MSPB as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

No, MSPB does not share information from Office 365 outside of MSPB as part of normal agency operations.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

As noted in 6.1, MSPB does not share information from Office 365 outside of MSPB as part of normal agency operations.

6.3 Does the project place limitations on re-dissemination?

Yes, MSPB does not share information from Office 365 outside of MSPB, and IRM restricts access to the location of the information.

6.4 Describe how the project maintains a record of any disclosures outside of MSPB.

MSPB has dedicated software for tracking all requests for disclosures of information from Office 365 for records or information under the FOIA, the Privacy Act, or routine use requests under SORNs, or other applicable statutes and regulations. The tracking software is a web-based application that assists MSPB in tracking and recording requests received for the disclosure of information. This includes requests subject to the accounting provisions of the Privacy Act. The information retained as part of this accounting requirement includes the agency or individual requesting the information, a description of the requested information, the reason for the request, the date of the request, the date of the release, the authority for the release, and the limitations and obligations on the requesting agency or individual with regard to use and further dissemination.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the Office 365 cloud vendor may inappropriately access the information in the system or that the ownership of the data in the system will be unclear, resulting in inappropriate access and sharing.

Mitigation: This risk is mitigated via the contract between MSPB and the Office 365 reseller, which does not allow the service provider to access, review, audit, transmit, or store MSPB data, thereby minimizing the privacy risks from the vendor source.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

MSPB users have access to their information in the various Office 365 systems. Individuals seeking notification of and access to information about them in Office 365 may submit a request in writing to the Office of the Clerk of the Board, Merit Systems Protection Board, 1615 M Street, NW, Washington, DC 20419, or by email to privacy@mspb.gov. Individuals requesting access must comply with MSPB's Privacy Act regulations regarding verification of identity and access to records. See 5 C.F.R. Part 1205.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

MSPB users who need to correct inaccurate or erroneous information can submit an e-Support ticket.

Other individuals may request that records about them be amended by writing to the Office of the Clerk of the Board, Merit Systems Protection Board, 1615 M Street, NW, Washington, DC 20419. Individuals requesting amendment must follow MSPB's Privacy Act regulations regarding verification of identity and amendment to records. *See* 5 C.F.R. Part 1205. These provisions for amendment of the record are not intended to permit the alteration of evidence presented in the course of adjudication before MSPB either before or after MSPB has rendered a decision on the appeal.

7.3 How does the project notify individuals about the procedures for correcting their information?

MSPB Office 365 is not accessible to anyone outside of MSPB and, therefore, it does not provide notice directly to those individuals who are not MSPB users. MSPB users receive notice in the form of training, instructions, Rules of Behavior, and the MSPB warning banner before accessing Office 365. More generally, all users receive notice about accessing and amending their records via this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals whose information is contained within Office 365 will not have information regarding how to access and request amendment of their information.

Mitigation: This risk is mitigated for MSPB users via various business processes, including contacting IRM or FAM to amend their information. MSPB users will also receive notice in the form of training, instructions, Rules of Behavior, and the MSPB warning banner before

accessing Office 365. More generally, all users receive notice about accessing and amending their records via this PIA.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

MSPB ensures that its users follow the practices set forth in this PIA by implementing training, standard operating procedures, policies, Rules of Behavior, and role-based access. Only MSPB users with a valid need to know may access the information in Office 365. MSPB protects records in the system from unauthorized access and misuse through various administrative, technical, and security measures, such as access controls, mandatory security and privacy training, encryption, multi-factor authentication, security guards, and locked offices.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

MSPB requires privacy and security training to all MSPB users, including mandatory annual information security, privacy, records, and FOIA training, and they must sign the MSPB's Rules of Behavior when onboarding and annually thereafter.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

MSPB deploys role-based access controls and enforces a separation of duties throughout all MSPB operations to limit access to records. It also ensures that only MSPB users who have an official need to know will have access to the information. The need to know is determined by the respective responsibilities of the user and the needs of the office. MSPB users who do not have a need to know or a need to have certain access do not have access to the information in this system.

8.4 How does the project review and approve information sharing agreements, Memoranda of Understanding (MOU), new uses of the information, new access to the system by organizations within MSPB and outside?

MSPB's use of Office 365 does not utilize information-sharing agreements or MOUs. New uses of the information are not permissible without review and authorization by MSPB's Clerk of the Board, Chief Privacy Officer, CIO, and Senior Agency Official for Privacy. If MSPB approves any new uses of the information, it will utilize any such uses only after providing appropriate notice, such as an update to this PIA or MSPB's SORNs.

Responsible Official(s):

Gina K. Grippando
Clerk of the Board & Senior Agency Official for Privacy
Merit Systems Protection Board

Approval Signature:

GINA
GRIPPANDO



Digitally signed by GINA
GRIPPANDO
Date: 2026.09.30 14:52:48
-04'00'

Gina K. Grippando
Clerk of the Board & Senior Agency Official for Privacy
Merit Systems Protection Board