Privacy Impact Assessment for

OPM - Microsoft Office 365

May 13, 2021 (update)

Contact Point

Russell Miller

Acting Associate CIO, Enterprise Infrastructure Solutions

Office of the Chief Information Officer

Reviewing Official

Kellie Cosgrove Riley

Chief Privacy Officer

Abstract

Office 365 is a Microsoft cloud-based Software as a Service (SaaS) solution, through which OPM will stand up and deploy a full suite of office communications and collaboration applications for OPM in the cloud. Office 365 will provide the OPM enterprise with a robust and standardized suite of collaboration, communication, and office productivity tools for OPM employees and contractors. Office 365 includes licensing of the desktop version of the latest Office applications such as: Email (Outlook), Word, Excel, and PowerPoint, as well as collaboration and communication tools including Teams, OneDrive and Power BI. This Privacy Impact Assessment (PIA) is being conducted because Microsoft Office 365 in part collects, maintains, and disseminates personally identifiable information.

Overview

The Office of Personnel Management (OPM), Office of the Chief Information Officer (OCIO) is deploying Microsoft Office 365, a cloud-based Software as a Service (SaaS) solution, in order to stand up and deploy a communications and collaboration suite of applications for OPM in the cloud. Office 365 will provide a robust and standardized enterprise-wide suite of collaboration, communication, and office productivity tools for OPM employees and contractors that will also allow OPM to manage, access, and protect information, and provide scalability.

Office 365 will be used by all OPM program offices for collaboration. Within their collaborative workspaces, OPM employees can use the tools of Office 365 to produce deliverables, which may include Word documents, spreadsheets, presentations dashboards, and other products. Content access is controlled by role-based security groups. Program offices are responsible for establishing and periodically reviewing access to their collaborative workspaces and stored objects to ensure that only those with a need to know have access. Only OPM employees and authorized

contractors/guests may have system user accounts. Active Directory, which serves as OPM's centralized domain management tool, will be used for identification and authentication of users. Other individuals may have access to information in the system only in the sense that they may receive email messages from OPM users containing information that is maintained in Office 365.

Users access Office 365 via a Uniform Resource Locator (URL), or web address. In accordance with recommended best practices, OPM's Office 365 uses Active Directory Federation Services (ADFS) to connect users. The site interfaces with OPM's Active Directory to ensure that only personal identity verification (PIV) authenticated users can access the applications. This also provides a Single Sign On (SSO) capability for the OPM user community. This suite of tools will enhance OPM's ability to store, archive, and retain discoverable data in place across the Office 365 platform. Additionally, OCIO staff and other appropriate offices, to include the Office of Privacy and Information Management (OPIM), will be able to monitor and investigate actions taken on data, identify risks, and contain and respond to threats.

Office 365 is a subscription-based service which provides access to numerous Microsoft services and software. Currently, the following applications within Office 365 are available to the OPM workforce:

Exchange Online

Exchange Online is a hosted messaging solution that delivers the capabilities of Microsoft Exchange Server as a cloud-based service. The solution provides users access to email, calendar, contacts, and tasks from PCs, the web, and mobile devices. Exchange Online integrates fully with Active Directory, enabling administrators to use group policies, as well as other administrative tools, to manage Exchange Online features across the environment.

Office Desktop Applications

Office 365 provides the latest version of the Office desktop applications that OPM personnel are familiar with, such as Word, Excel, and PowerPoint. The Office desktop applications are installed on local computers.

OneDrive

OneDrive is a document, file and synchronization service, and serves as OPM's integrated storage, backup, and collaboration tool. With OneDrive, OPM personnel can control how they store, share and update their files, choosing between the following options as needed:

- Storing and accessing some files only on their computer.
- Maintaining some files only on the cloud in order to share files for real-time collaboration with colleagues.
- Backing up files, stored on one's local computer, to the cloud and synchronizing them, so that changes can be retained in both places and allowing for download for personnel to work offline should they not have internet access available.

OneDrive also provides the capability for OPM personnel to create files directly in the cloud, using the standard suite of Office applications such as Word, Excel, and PowerPoint. Eventually, OneDrive will replace employees' assigned network drives that contain documents and files that each employee has saved externally from their government-issued computers.

Microsoft Teams

Microsoft Teams is a persistent chat-based collaboration platform that enables document sharing, revision tracking, online meetings, and other useful features for business communications. Business communications include: instant messaging, document storage in SharePoint, online audio and video calling/conferencing and screen and file sharing. Teams enables OPM personnel to communicate and collaborate in real time with colleagues

and 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.

Microsoft Power BI

Microsoft Power BI is a business analytics service. Power BI provides interactive visualizations and business intelligence dashboards with an interface where end users can easily structure, condense, and consolidate data to create their own easily interpreted and understandable reports and dashboards.

Power BI is used to run reports, structure data, and identify possible conclusions using data contained in various OPM systems as well as other data sources like spreadsheets and SharePoint lists. Power BI will have access to a wide range of data sets across OPM and the capability to illustrate the data in various ways to make it clear and concise to a wide range of users. This will assist OPM decision makers in making well informed strategic and operational decisions by gathering data and presenting it in easily interpreted illustrations, graphs, and charts. Power BI reports must be explicitly shared with authorized users in order for them to have access.

As additional Office 365 applications and functionality are added, they will be evaluated, and this PIA updated as appropriate.

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 information contained in Office 365 is collected pursuant to a variety of authorities that govern OPM program areas. In addition to program-specific authorities, there are numerous laws, regulations, Executive Orders, and

OMB Circulars and Memoranda that require and authorize Federal agencies to manage and modernize their IT systems. Federal IT modernization is a component of the President Management Agenda and the successful move of agencies to cloud email and collaboration tools is also a cross-Agency priority goal.

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

Records contained in the email content and attachments and within collaboration portals/repositories are subject to various OPM systems of records notices, available at opm.gov/privacy.

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

Yes. A System Security Plan was completed on June 3, 2020 in connection with the Office 365 Authority to Operate (ATO). The current ATO expires March 12, 2023.

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

Depending on the nature and type of record within the components of Office 365, various NARA-approved records schedules will apply. In particular, email records and the persistent chat records are governed by GRS 6.1 Capstone E-mail Retention.

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.

Office 365 collects, maintains, uses, or disseminates: names and contact information of OPM users and other individuals who communicate with OPM users via Office 365; email messages (including any attachments) which may contain a variety of information, to include PII about OPM employees, other Federal employees, and members of the public; message log information (including IP address of sender, date, and time); instant messages, which may contain a variety of information, to include PII about OPM employees, other Federal employees, and members of the public; and information stored in collaboration portals/repositories (such as spreadsheets, word processing, and PowerPoint documents), which may contain a variety of information, to include PII about OPM employees, other Federal employees, and members of the public. The system also maintains logs of OPM user activity.

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

Information about the system users comes from the individuals or from internal OPM systems. The information in the content of the email or in documents and records contained within the collaboration portals/repositories may come from a variety of sources, including individuals or entities outside of OPM who correspond using email or provide information to any of the OPM program offices in the normal course of business.

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 use information from commercial sources or publicly available data except to the extent that users include such information in the content they develop and share within the O365 suite.

2.4. Discuss how accuracy of the data is ensured.

OPM has a high degree of confidence in the accuracy of the user information because OPM receives the information directly from the employees or contractors. In most cases, employees have direct control over their information and may edit it to maintain its accuracy at any time. Other information contained in the various components of Office 365 may be checked for accuracy outside of the system or presumed accurate based on its source. 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.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

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

Mitigation: This risk cannot be fully mitigated by Office 365 and is primarily dependent on end users in the program offices who have responsibility for their content. The collaborative nature of the system and its applications naturally provides a platform where those collaborating on a project can address any inaccuracies. With respect to user information, the risk of inaccuracy is mitigated primarily via controls that may limit or guide how the user technically enters the information. In addition, employees are routinely reminded to update information about themselves in the Global Address Book within the Outlook program.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

Office 365 is used to communicate and collaborate on various OPM program office projects and activities. The information that end users include within

Office 365 is used to further their program area missions in an effective and efficient manner that appropriately controls access, provides the ability to track changes and reduce version control issues, and enables appropriate use and sharing of OPM information. Office 365 services such as Exchange Online allow users to view contact information to interact and work with each other within the collaborative environment and communicate through email and scheduling meetings with internal users and individuals outside OPM.

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 OPM plans to use such results.

OPM has implemented a data loss prevention tool in order to monitor endpoint web activities and email in an effort to prevent the inappropriate release of PII.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

All OPM employees and contractors use Office 365. Within the Office 365 applications, users are provided instruction and training to provide access to their content within the applications only with those who have a need-to-know. The OPM OCIO assigned System Administrators and Engineers maintain, monitor, and support the OPM Office 365 SaaS tenant.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the information in Office 365 may be accessed by unauthorized users or by authorized users for an unauthorized purpose.

Mitigation: This risk is mitigated by requiring all users to have an OPM system account and PIV card. Prior to receiving access to OPM's network, all users must agree to the OPM Rules of Behavior, which includes the consent to monitoring and restrictions on data usage. The systems are monitored

for misuse and unauthorized activity and access can be removed at any time by the system administrator. This risk is also mitigated by providing training and guidance to end users who are the subject matter experts regarding, e.g., access controls within their purview to provide information and invitations to collaborative meetings only to those who have a need-to-know.

In addition, OPM uses a combination of technical and operational controls to reduce risk in the Office 365 environment, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention policies. As a FedRAMP-approved cloud service provider, Office 365 undergoes regular reviews of its security controls

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.

OPM users are provided training and must sign Rules of Behavior before accessing the system. In addition, they are presented with an OPM Warning Banner prior to logging on to any OPM system, which stipulates users do not have the right to privacy while using the system, which includes internet and email services. Certain applications within Office 365 may provide appropriate notice to individuals whose information may be used or collected within the system. For example, individuals who participate in Teams meetings are provided notice if a meeting is going to be recorded. Individuals who provide information to OPM that OPM users may then include in the collaboration components of Office 365 may receive notice at the point of collection regarding the purpose for which that information may be used, but not notice of its inclusion in Office 365. This PIA and any relevant SORN also provide notice to individuals.

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

OPM users and others whose information may be contained in Office 365 generally do not have an opportunity to consent to the inclusion of their information in the system. OPM users cannot decline to provide their information to access Office 365. Individuals who are not OPM users but whose information is contained in the system may have opportunities at the point their information is collected to decline to provide it but once provided cannot decline for it to be included in Office 365. For example, those who participate in Teams meetings receive notice if a meeting is going to be recorded and can opt to leave the meeting or turn off their camera and microphone.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not have 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 OPM users via the OPM Warning Banner that is displayed on all user systems prior to logging on to the OPM 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 at which it is collected.

Section 5.0. Data Retention by the Project

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

Depending on the nature and type of record within the components of Office 365, various NARA-approved records schedules will apply. For example, email and persistent chat records are retained pursuant to GRS 6.1 Capstone E-mail Retention, which establishes retention at 7 years for most users and

15 years, followed by permanent retention with NARA, for Capstone officials. OPM users receive regular training and reminders about their records and destruction obligations.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that records in Office 365 will be retained for 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 OPM users regarding the applicable retention schedules. Mitigation of this risk is dependent, in part, on end users following applicable retention schedules; where possible, OCIO, working with OPM's Records Officer, will incorporate technical means to identify and apply applicable records schedules. To the extent any records are present in the system that do not have a current records schedule, the appropriate program office will work with the Records Office to schedule the records.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM 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.

Information contained in Office 365 may be shared outside of OPM, depending on the nature and type of records and consistent with applicable laws and policy.

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

To the extent that information about individuals contained in Office 365 are Privacy Act records, they will be shared outside of OPM only as consistent with applicable routine uses or other applicable provisions of the Privacy Act.

6.3. Does the project place limitations on re-dissemination?

To the extent that information about individuals contained in Office 365 are Privacy Act records, they will be shared outside of OPM only as consistent with applicable routine uses or other applicable provisions of the Privacy Act. Where appropriate, limitations on re-dissemination will be included in any applicable information sharing agreement or contract.

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

All actions in Office 365 taken by a user are logged and are monitored and accessed by those with a need to know.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information in Office 365 will be share outside of OPM with those who do not have a need to know.

Mitigation: This risk is mitigated through training, required adherence to Rules of Behavior, and through the use of data loss prevention tools and system activity logs. Mitigation of this risk is dependent, in part, on the end users, who are the subject matter experts concerning the information they place into Office 365, adhering to Privacy Act systems of records and any applicable handling policies and procedures pertinent to their program information.

Privacy Risk: There is a risk that the 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 OPM and the Office 365 Microsoft reseller partner, which does not allow the service provider to access, review, audit, transmit, or store OPM data, which minimizes privacy risks from the vendor source.

Section 7.0. Redress

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

OPM users have access in the various Office 365 systems to their information. For example, Exchange Online user data can be accessed via Outlook. Others whose information may be contained in an Office 365 application may access their information as appropriate by following the instructions in any applicable system of records notice.

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

Active Directory is an enterprise administrative tool; certain OPM user information hosted in Active Directory is read-only to the individual; a user has access to view the data but can only request appropriate changes and removal by contacting system owners and operators.

The Global Address Book is an aspect of Microsoft Outlook; an individual OPM 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 OPM's Intranet site or by contacting the OPM Helpdesk to have this information corrected on the GAL. To remove an employee from the GAL, requests must be submitted through the Help Desk.

Others whose information is in the system can access and request amendment to their information as appropriate by following the instructions in any applicable system of records notice.

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

OPM's Office 365 implementation is not accessible to anyone outside of OPM and, therefore, does not provide notice directly to those individuals who are not OPM users whose information it contains. OPM users receive notice in the form of training, instructions, Rules of Behavior, and the OPM Warning Banner prior to accessing. More generally, all individuals receive notice

about accessing and amending their records via this PIA and any applicable SORNs.

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 OPM users via various business processes and for those individuals who are not OPM users via this PIA and any applicable SORNs.

Section 8.0. Auditing and Accountability

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

Office 365 audit logs are captured by OPM's auditing tools and retained in the tools archive. The Office of the Chief Information Security Officer reviews for suspicious or unusual activity and suspected violations, and as necessary appropriate action is taken.

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

All OPM employees and contractors are required to take IT Security and Privacy Awareness training on an annual basis, and sign OPM's Rules of Behavior. In addition, training and guidance concerning the use of the various applications within Office 365 is offered to end users and available via an OCIO Resource Center on the OPM Intranet.

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

All OPM employees and contractors have access to Office 365. User access to individual services are managed by the OCIO Helpdesk. Only approved

OPM users are allowed to use Office 365. In addition to OPM employees, any contract employees or other users within the system need to first be approved, an OPM temporary account must be created, and an OPM device is issued to them by the Help Desk. The principle of least privilege is used to grant access to OPM federal employees and contractors, and user actions are tracked in the Office 365 audit logs.

When individuals are included in a Teams meeting, it is the responsibility of the OPM user who initiates the meeting to determine that both OPM and non-OPM individuals who are invited to attend have a need-to-know and that it is otherwise permissible to provide access to all meeting content, to include the discussion as well as any shared documents that may contain PII and other sensitive information.

In OneDrive, Teams, and SharePoint, OPM users cannot provide access to non-OPM users to collaborate on documents. If a requirement for non-OPM users to have review/edit capabilities during an OPM sponsored meeting or conferences, an administrator needs to add a guest user to the specific Team. The guest user needs to then acknowledge the request, register, and log in with Microsoft credentials. Guests may view, review, and edit documents within the OPM environment. However, guests are not authorized to copy from, download, save (externally) or print (even to PDF) any documents used during the event. Guest users accounts are removed from the OPM Active Directory after the collaboration event.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

Any changes in system access, sharing agreements, or Memorandum of Understandings (MOUs) would need to be reviewed and approved by all appropriate OPM stakeholders, including the Chief Information Security Officer and the Chief Privacy Officer.

Responsible Officials

Russell Miller

Acting Associate CIO, Enterprise Infrastructure Solutions

Office of the Chief Information Officer

Approval Signature

Signed Copy on file with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer