Privacy Impact Assessment for

OPM - Microsoft Office 365

December 30, 2020

Contact Point

Mary C. Price

Associate CIO, Enterprise Infrastructure Solutions

Office of the Chief Information Officer

Reviewing Official

Kellie Cosgrove Riley

Chief Privacy Officer

Abstract

Microsoft Office 365 is a cloud-based Software as a Service (SaaS) solution that provides OPM services and software, such as Exchange Online. The solution provides users access to email, calendar, contacts, and tasks from PCs, the web, and mobile devices. Office 365 also includes licensing of the desktop version of the latest Office applications such as: Email (Outlook), Word, Excel, and PowerPoint. This Privacy Impact Assessment (PIA) is conducted because Microsoft Office 365 in part collects, maintains, and disseminates personally identifiable information.

Overview

The Office 365 Project and system is an endeavor undertaken by the Enterprise Information Solutions (EIS), in the Office of the Chief Information Officer (OCIO), to stand up and deploy a communications and collaboration suite of applications for the U.S. Office of Personnel Management (OPM) in the cloud. The system will help manage access, protect business information and provide scalability. Office 365 will provide services to allow for better productivity by providing flexible and familiar tools for many OPM devices agency wide.

OPM requires a robust and standardized suite of collaboration, communication, and office productivity tools for employees and contractors. Office 365 integrates fully with Active Directory, enabling administrators to use group policies, and other administrative tools, to manage Exchange Online features across the OPM environment. The intended configuration as part of the OPM LAN/WAN is a hybrid exchange environment. These services run more efficiently and are more cost effective in a cloud-based Software as a Service (SaaS) platform.

Microsoft Office 365 is a subscription-based service which provides access to numerous Microsoft services and software. Office 365 is offered in a tiered structure, with services and functions, and escalating subscription prices. It

provides a reliable, security-enhanced messaging environment with the flexibility to meet changing Federal business needs. From this interface users can access, create, store, share and collaborate using the various Office 365 applications. OPM employees with a user account and appropriate access privileges may search, view, share, and edit documents.

The deployment of Office 365 will modernize the collaboration, communication and office productivity tools enabling OPM and its administrators and user community to be more productive. Driving the adoption to Office 365 will create a transformation of how the user community can leverage IT products and services.

Office 365 provides multiple components within the suite that will deliver the following business outcomes:

Office 365 Infrastructure (Hybrid Cloud)

A Hybrid cloud architecture will be the path taken to migrate the agency to Office 365 and integrate cloud technologies and services into the existing on-premises infrastructure as part of the overall IT strategy. The required infrastructure elements to be accounted for to implement Office 365 are networking, identity, and security.

Exchange Online

Microsoft 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. Microsoft 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. The intended configuration as part of the OPM General Support Systems (GSS) is a hybrid exchange environment.

Office 365

Microsoft Office 365 is a subscription service that provides the latest version of the Office desktop applications that the OPM user community is familiar with, such as Word, Excel, and PowerPoint. Even though Office 365 is a cloud-based service, Office applications don't run in the cloud. Instead, the Office applications are downloaded from the Office 365 portal and installed on local computers. Microsoft uses Click-to-Run technology to make the download and installation of Office applications fast and simple. Click-to-Run uses virtualization technology to run Office applications in a self-contained environment on a local computer, which allows users to run Office applications side-by-side with earlier versions of Office. The delivery of Office 365 to OPM users will allow installs on up to 5 laptops/desktops, 5 tablets and 5 phones per user license.

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, forms, presentations 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 may have system user accounts. Active Directory, which serves as the 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 (email messages) that is maintained in Office 365.

The type of information collected, maintained, used, or disseminated by the system includes: 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.

Users access Office 365 via a Uniform Resource Locator (URL), or web address. In accordance with recommended best practices the OPM Office 365 instance 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 Single Sign On (SSO) capability for the OPM user community. These capabilities are to simplify agency processes and quickly identify relevant data while decreasing cost and risk. OPM will be better able to store, archive, retain, and discover 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, contain and respond to threats, and protect valuable intellectual property.

Currently, under the auspices of the CARES Act, OPM has received funding to expand the offering of collaboration tools for use by OPM employees to increase productivity. At this writing, expansion of the tools under the Office 365 banner is an agency priority. We anticipate that there will be additional research and security and privacy assessments of these tools in the near future. Once completed, this Privacy Impact Assessment will be amended to address additional Office 365 functionality and assess any associated risk and mitigation.

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 and its components 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?

Various 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. In addition, OCIO will work with the Office of Privacy and Information Management to determine the need for and development of a SORN or SORNs applicable to employee account and audit log information.

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). It is updated at least annually and signed by the system owner to acknowledge the updates.

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.

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.

Email messages and attachments that are collected, maintained, and disseminated within collaboration portals/repositories contain varied information, including information about individuals. In addition, the system contains user account information, to include username, work email address, work phone number, work address, title of OPM employees and contractors, and related organizational information required for system administration.

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

Information about the systems 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.

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.

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 is mitigated, with respect to user information, via controls behind the program 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 services such as Exchange Online will allow users to view contact information to interact and work with each other within the collaborative environment. Outlook 365 is used to 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 Forcepoint Data Loss Prevention (DLP) application to monitor endpoint web activities and Microsoft Outlook email. OPM deploys a remote Forcepoint agent with preconfigured rules and Internet access polices that prevent the inappropriate release of PII.

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

All OPM employee and contractors use Office 365. OPM OCIO assigned System Administrators/Engineers maintain, monitor and support 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.

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. 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 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.

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. OPM users receive 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 and Office 365 will incorporate, where possible and working with OPM's Records Officer, technical means to identify and apply those 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.

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 is in the system can 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 changes and removal are managed by 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 myTheo or contact the OPM Helpdesk to have this information corrected on the GAL. In order 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. Cyber Solutions 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.

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 other 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.

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

Mary C. Price

Associate CIO, Enterprise Infrastructure Solutions

Office of the Chief Information Officer

Approval Signature

Signed Copy on file with Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer