Version Number: 01-2019

U.S. Department of Commerce
International Trade Administration (ITA)

Privacy Threshold Analysis
for the
ITA Microsoft Office 365 Platform (ITA_O365PF)

U.S. Department of Commerce Privacy Threshold Analysis

ITA Microsoft Office 365 Platform (ITA_O365PF)

Unique Project Identifier: 2443

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system

The ITA Microsoft Office 365 (O365) platform is a general support system and major application.

b) System location

Microsoft Office 365 Multi-Tenant (O365 MT) is a multi-tenant cloud computing-based subscription service offering from Microsoft. Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Further, as defined within NIST SP 800-145 (The NIST Definition of Cloud Computing), the service model for O365 MT is Software-as-a-Service (SaaS). SaaS is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

O365 MT provides customers with cloud versions of Exchange Online (EXO), SharePoint Online (SPO) (including Office Online, and OneDrive for Business), Microsoft Teams, and Skype for Business Online (Skype). Exchange Online is an email service. SharePoint Online is a solution for sharing documents and information. Microsoft Teams and Skype for Business Online are communication/collaboration services that offer instant messaging, audio and video calling, online meetings, and web conferencing capabilities.
O365 MT has a number of supporting services in addition to this core, customer-facing services. Each core and supporting service is supported by a unique group of developers, testers, and administrators referred to throughout this document as a "service team". Each service is deployed onto service-specific servers, whether physical or virtual. While each service team follows O365 policy, their services may have unique implementations of some security controls.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The ITA O365 Platform connects with the ITA Active Directory (AD) authentication servers located in ITA's Amazon Web Services (AWS) US-EAST IaaS tenant and the ITA Microsoft Azure AD cloud service, as integrated into the ITA Network infrastructure for account management and authentication via Active Directory Federation Services (ADFS). There is no information sharing between the ITA O365 Platform and these cloud computing services. The ITA O365 Platform and component applications provide ITA personnel the platform to collaborate within the environment. These integrated applications share the same authentication process (ADFS) to provide the needed functionality for the operations of the cloud support system. Resources located in these applications are restricted by default and permissions are granted based on least-privileged access.

d) The purpose that the system is designed to serve

The ITA O365 platform provides collaborative cloud computing services within ITA. Microsoft O365 is a FedRAMP approved application using the Software as a Service delivery model. The applications contained in O365 include: Exchange Online (EXO), SharePoint Online (SPO) (including Office Online and OneDrive for Business), Skype for Business (SFB) and Microsoft Teams. Data Loss Prevention (DLP) is also enabled in O365 through the compliance suite, providing capability to identify, monitor, and protect sensitive information within the platform. This protects sensitive information and prevents its inadvertent disclosure.

The way the system operates to achieve the purpose

Detailed descriptions of application tools offered in the O365 Platform are provided below:

Exchange Online (EXO) provides emailing services and calendar capabilities for ITA personnel. Data collected, maintained and disseminated in the email service may include: employee name, job title, office telephone number, user ID, photographs, date/time of access and task information. This information is shared internally within ITA. The ITA Global Address List (GAL) collects a portion of this information (employee name, job title, office telephone number) and federates it with the DOC GAL. Users interact with the application via web browser and software applications (for desktop and mobile devices).

SharePoint Online (SPO) enabled ITA personnel to share and collaborate with colleagues within ITA. Office Online and OneDrive for Business are enabled through this platform. Office Online enables browser-based viewing and editing of Microsoft Office documents. OneDrive for Business enables online storage and synchronization of documents. Data collected, maintained and disseminated in the SharePoint Online suite include: employee name, job title, office telephone number, photographs, date/time of access, project titles, and tasks for execution assigned to personnel. SharePoint provides enhanced security (especially in dealing with extremely large quantities of documents). Without the appropriately assigned permissions (controlled and managed via Active Directory), users cannot access documents or even know those documents exist. All data is locked down and accessible only to those with the official need to know. Users interact with the application via web browser and software applications (for desktop and mobile devices).

Offices within ITA (including Technology, Services, and Innovation) are currently in the process of migrating to SharePoint Online from ITA's legacy on-premises SharePoint system.

Skype for Business (SFB) and Microsoft Teams offers ITA personnel instant messaging, audio/video calling, and online/broadcast meeting capabilities. Data collected, maintained and disseminated through SFB include employee name, job title, meeting information, photograph, date/time of chats and contact information such as office address, location, and telephone number. Meeting "free/busy" calendar information is federated with DOC for scheduling purposes. Users interact with the application via web browser and software applications (for desktop and mobile devices). This service is slated for replacement in the coming two years with Microsoft Office 365 Teams.

The ITA O365 platform has a number of supporting services in addition to this core, customer-facing services. Each core and supporting service is supported by a unique group of developers, testers, and administrators referred to throughout this document as a "service team". Each service is deployed onto service-specific, Microsoft-managed cloud SaaS infrastructure. The services themselves may be configured by their respective service team, but the operation and maintenance of the cloud servers themselves is managed entirely by Microsoft. While each service team follows O365 policy, their services may have unique implementations of some security controls.

e) A general description of the type of information collected, maintained, use, or disseminated by the system

This document is intended to cover internal uses of cloud-based services as employee collaboration tools. ITA employees using these collaboration tools provide the following information via Active Directory: first name, last name, work email address, username, work phone number, and office location. Generally, employees should not provide information beyond business contact information. Some tools (like Skype for Business) rely on Active Directory to pre-populate the user's account. In other cases, ITA personnel may send basic business contact information, such as first name, last name, and email address, to create an account.

Any programs or systems using collaboration tools that require information beyond basic business contact information will require their own privacy compliance documentation. Information maintained in DOC content management sites, such as SharePoint, will depend on the particular business processes for which the systems are established. Content management sites may be used to support DOC programs such as: human resources, financial management, acquisition services, etc. Therefore, systems may include a variety of information from or about the public. Program site managers are responsible for managing the content of their sites. Content management sites that contain PII, beyond business contact information, are governed by the SORN specific to the record types stored within the IT system and must be used in accordance with the purpose(s) enumerated in the SORN.

f) Identify individuals who have access to information on the system

Only authorized ITA TSI personnel with privileged account credentials will have access to administrate the ITA O365 platform. Non-administrative information (e.g., ITA email) may be accessed only by users with valid, active ITA user accounts with the appropriate permissions to access it, controlled via ITA's Active Directory.

g) How information in the system is retrieved by the user

Users access non-privileged information on the ITA O365 platform via HTTPS-encrypted internet traffic routed through Microsoft's Cloud servers. Privileged access to O365 resources (including the Microsoft Exchange Control Panel and other administrative features) is only accessible to users with privileged credentialed accounts controlled via ITA's Active Directory. Users interact with the EXO, SPO, and SFB cloud service applications via web browser and software applications (for desktop and mobile devices).

h) How information is transmitted to and from the system

Users access non-privileged information on the O365 platform via HTTPS-encrypted internet traffic routed through Microsoft's Cloud servers.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

__x_ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015). *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

_x___No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

__x No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__x_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__x DOC employees
____ National Institute of Standards and Technology Associates
_x___Contractors working on behalf of DOC
____ Other Federal Government personnel
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

_x___ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__x Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

___x_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the ITA Microsoft Office 365 Platform and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the ITA Microsoft Office 365 Platform and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Larry Rubendall

Signature of SO: LARRY RUBENDALL Digitally signed by LARRY RUBENDALL Date: 2020.03.20 09:42:41-04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Joe Ramsey

Signature of ITSO: JOSEPH RAMSEY Digitally signed by JOSEPH RAMSEY Date: 2020.04.28 15:30:00 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Angenette Cash

Signature of PAO: ANGENETTE CASH Digitally signed by ANGENETTE CASH Date: 2020.03.26 07:55:42 -04'00' Date: _____

Name of Authorizing Official (AO): Rona Bunn

Signature of AO: RONA BUNN Digitally signed by RONA BUNN Date: 2020.05.03 12:48:52 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Angenette Cash

Signature of BCPO: ANGENETTE CASH Digitally signed by ANGENETTE CASH Date: 2020.03.26 07:56:15 -04'00' Date: _____