UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR MICROSOFT 365 (M365) PART OF THE ESI SAAS - 1 BOUNDARY

December 2022

Next Review Cycle: December 2023

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Record of Approval

Document Approval		
Drafter Name: Kenneth Wisneski		**Bureau/Office:** OMD/IR
SAOP Approval		
Printed Name: Elliot S. Tarloff		**Senior Agency Official for Privacy**
Signature: Elliot S. Tarloff Digitally signed by Elliot S. Tarloff Date: 2022.12.19 14:28:15 -05'00'	**Date**	

Record of Approval

Date	Description	Author
12/15/2022	Validation of information – System Owner Designated Representative	Steve Kanen
12/15/2022	Validation of completeness – IT Compliance Lead	Liem Nguyen

Revision History

Date	Description	Name
11/03/2022	Original Document Created	ISSO - Kenneth Wisneski
12/08/2022	Privacy edits to Sections 1.2, 1.3B-D, 1.4A-B, 1.5C, 1.6A-B.	Privacy Legal Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff
12/15/2022	Formatting edits	SAOP

MICROSOFT 365 PART OF THE ESI SAAS- 1 BOUNDARY

1.1. Introduction

Section 208 of the E-Government Act of 2002[1] requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and, unless it contains classified or sensitive information, it must be made available to the public. The PIA was intended to be a tool for agencies to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: "*In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks.*"[2]

The FCC is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

System owners, in collaboration with the Information System Security Officers (ISSOs) should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The FCC Senior Agency Official for Privacy (SAOP) uses the IPA to determine whether a system will collect the kind of information that would make it subject to the requirements of Section 208, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination.

If you have any questions, please contact the Privacy Team at privacy@fcc.gov.

[1] 44 U.S.C. § 3501 note.

[2] OMB Memorandum No. M-03-22 (Sep. 26, 2003), https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/.

1.2. Authority To Operate (ATO) Boundary Overview

For each IT system that resides within the ATO Boundary, please use the table below to provide the system name, a brief description of the what the system does, whether it contains Personally Identifiable Information (PII) and a brief description of the PII (if applicable), the applicable System of Records Notice, the legal authorities to collect and maintain the PII, and whether the PII is shared with other systems (internal or external).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM ESI SaaS-1 (M365)
NAME OF BUREAU Office of Managing Director (OMD)
DOES THE SYSTEM CONTAIN PII? Yes, M365 contains PII, but the FCC does not use M365 to collect PII directly from the public, and the FCC generally does not retrieve records from M365 using unique identifiers of individuals.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The FCC houses a variety of information in M365 depending on the needs and purposes of the Bureaus and Offices that use this software. To the extent PII from the public is stored in M365 applications, the information collection is incidental. M365 may also contain information pertaining to FCC employees and contractors.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? N/A. The FCC is not required to publish a System of Record Notice (SORN) for M365 as it is not considered a “system of records” as defined by the Privacy Act, 5 U.S.C. 552a(a)(5).
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The information in this system is collected, maintained, and disseminated pursuant to the Communications Act of 1934, as amended, and other rules and regulations the FCC enforces.

DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (C) OF THE PRIVACY ACT? N/A.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

A. Is this a new ATO Boundary or an existing ATO Boundary?

☐ New Boundary
☒ Existing Boundary

B. If the ATO Boundary is/will consist of cloud-based computing system(s),[3] please check the box that best describes the service the FCC receives/will receive from the cloud computing provider:

☒ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS). A non-exhaustive list of applications is Microsoft Word, Microsoft Excel, Microsoft PowerPoint, OneNote, OneDrive, Microsoft Teams, Exchange Online, SharePoint Online, Microsoft Outlook, Microsoft Access (PC Only) and Microsoft Publisher (PC Only).

☐ The FCC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS) [list applicable system(s)]

☐ The FCC has deployed its own application/s on the cloud network and controls how these application/s are configured and operate (Infrastructure as a Service or IaaS) [list applicable system(s)]

C. If the IT systems in the ATO Boundary are in the cloud, are they FedRAMP certified?

☒ Yes, all the IT systems are FedRAMP certified
☐ No, none, or only some, of the IT systems are FedRAMP certified

[3] *See* NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

1.3 Collection of Data

A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

Information in M365 applications is collected, used, disseminated, and maintained for the FCC to perform its regulatory, licensing, enforcement, policy, personnel management, and other activities. Due to the range of supported services, personal information may be present for a variety of reasons in the course of conducting internal and external communication and collaboration, creation and management of records, information security, and daily business operations.

B. For each system within this Boundary, will this PII be collected from individuals themselves, or from third parties? If collected from individuals themselves, link to the Privacy Act Statement[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

The FCC generally does not use M365 applications to collect PII directly from the public; however, information provided by and pertaining to individuals may be stored in M365 applications. Such individuals may include consumers, representatives from regulated entities, and representatives from other federal, state, and local government entities. Because M365 is not a Privacy Act "system of records," no Privacy Act Statement is required.

C. What steps is the FCC taking to limit the collection of PII to only that which is necessary?

Direct Enterprise Controls:

M365 applications (e.g., Word, Excel, Outlook, PowerPoint, Teams, SharePoint Online, OneDrive Online) provide read, write, manipulation, correspondence, collaboration, and storage capabilities for FCC personnel throughout the enterprise. The FCC stores a variety of information in M365 applications depending on the needs and purposes of the Bureaus and Offices that use this software. Thus, it is the responsibility of FCC staff and contractors to limit the PII maintained on M365 to that which is necessary.

Indirect Enterprise Controls:

FCC staff and contractors are required to complete annual privacy training that includes instruction on limiting the collection of PII.

The FCC does not use M365 to collect PII directly from members of the public. To the extent PII is stored in applications supported by M365, the information collection is incidental, and the

[4] A Privacy Act Statement must inform individuals about (1) the authority to solicit information, (2) the principal purpose(s) for collecting the information, (3) the routine uses for disclosing the information, and (4) whether providing the information is mandatory or voluntary.

data may be subject to additional limitations insofar as they are included in any FCC systems that are Privacy Act "systems of records."

D. What steps will the FCC take to make sure this PII is accurate, complete, and up to date?

Due to the nature of the system and the anticipated broad use of these services across the enterprise, information that is stored in M365 generally will not be checked for accuracy, completeness, or currency. It is the responsibility of the parties providing the data to ensure the completeness, accuracy, and currency of data at the time those data are created. Information that is used by the FCC as part of its regulatory, enforcement, and other activities will be reviewed for accuracy and timeliness as required by the particular activity and the laws and authorities, if any, applicable at the time the agency compiles the records (e.g., Communications Act, personnel laws, administrative or court evidentiary rules and procedures).

1.4 Use of the Data

A. Please explain the data flow, including whether the PII will be ingested from, or shared with, another system. Are internal connections reflected in the Cyber Security Asset Management tool (CSAM)? Are Information Sharing Agreements (ISAs) in CSAM for external connections?

A user acquires access to M365 applications when he or she onboards. The M365 applications are assigned to users by administrators. An administrator assigns each user to a pre-defined Organizational Unit (OU) in Active Directory (AD) that stores the M365 application baseline. If the user requires other M365 applications, he/she will be given permissions based on his/her role and responsibilities. The user's credentials are set up in an Active Directory Federation Services (ADFS) profile that is synced with the M365 AD to provide the user access to the M365 assigned products. Any other products needed from the M365 offering will need to be approved by the group's Contracting Official Representative (COR) and M365 Change Advisory Board (CAB). Once the user has access to the suite of M365 applications, he or she can execute tasks, and finished products will be stored in the associative drives and/or cloud provided services (i.e, Onedrive for Business, Sharepoint Online, Exchange Online) directories. Any PII will be stored within these final products and storage containers for each application or service.

There are no Information Sharing Agreements (ISAs) in CSAM, nor do any M365 applications share PII with any other systems. The M365 applications are not Privacy Act "systems of records."

B. Will the information be shared with third parties as part of the operations of the information system (e.g., through an application programming interface or "API")?

No, information is not shared with third parties via API.

C. How long will the PII be retained and how will it be disposed of?

Information in the systems within this boundary is retained and destroyed in accordance with applicable FCC policies and procedures, as well as with the FCC records disposition schedule or General Records Schedules approved by the National Archives and Records Administration (NARA).

1.5 Data Security and Privacy

A. What are the system's ratings for confidentiality, integrity, and availability?

Confidentiality	__High	_X__Moderate	___Low
Integrity	__High	_X__Moderate	___Low
Availability	__High	_X__Moderate	___Low

B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.

The FCC protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire FCC enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems. Following the risk-based policy established in the Federal Information Modernization Act (FISMA), the FCC applies more security measures (also known as security "controls") to information systems that present higher operational risks. Consistent with this policy, the FCC applies specific security controls to systems that collect and process PII. A comprehensive list of the security and privacy controls the FCC may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53, Revision 5 [NIST].

C. Does the system inherit privacy controls from an external provider? If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy applicable portions of the document.

Yes, privacy controls are included in the FedRAMP package. There are no ISAs, MOUs, or similar documents in place.

1.6 Access to the Information

A. Which FCC employees and contractors will have access to the PII in this information system?

Will Have Access	How and Why the Data Will Be Accessed
FCC Staff	Access to M365 is restricted to authorized FCC end users. All end users must adhere to the FCC Rules of Behavior and take steps to ensure that access to any PII stored in M365 is appropriately limited. Access to the information stored within M365 is dependent on the particular business purpose and the access permissions granted to a specific user.
Contractors	FCC may have contractor support within program areas, and these contractors will have access to the information in M365 as required to perform their duties.
Office of Inspector General (OIG)	Under appropriate circumstances, data showed within M365 or M365 log data may be provided to the OIG for auditing or law enforcement purposes.

B. Does this system leverage Enterprise Access Controls?

Yes, the Microsoft 365 SaaS allows users (privileged and non-privileged) to access the production environment through either Active Directory Federation Services (ADFS) servers or OKTA, an enterprise-grade, identity management service, built for the cloud. Either M365 user access path can solicit FCC Active Directory (AD) servers to provide user profiles and security policies to use as input for user authentication and authorization.

To access M365 for the web through the Internet via https://login.microsoftonline.com, OKTA uses Active Directory to provide an identity management service for M365 users to login into M365. FCC NetOps M365 Global administrators ensure only M365 privileged and non-privileged users are allowed to access the M365 SaaS solution. This is accomplished by submitting a Change Request to acquire certain M365 roles related to unique M365 permissions.

All M365 security access policies follow strict FCC guidelines and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 access, identification and authentication and configuration management controls.