UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

INFORMATION TECHNOLOGY

PRIVACY IMPACT STATEMENT FOR THE MICROSOFT O365 SYSTEM

11/21/2019

OFFICE OF THE MANAGING DIRECTOR

445 12TH STREET SW, WASHINGTON, DC 20554

Record of Approval

Document Approval		
Document POC		
Printed Name: Bahareh Moradi		**Attorney-Advisor** **Office of General Counsel**
Signature:	**Date** **11/18/2019**	
Approval Structure		
Printed Name: Michael Carlson		**Senior Agency Official for Privacy** **Deputy General Counsel** **Office of General Counsel**
Signature: Michael Carl	**Date** 11/21/19	
Printed Name:		
Signature:	**Date**	

Record of Approval

Date	Description	Author

Table of Contents

List of Tables

Micrsoft O365

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).

In accordance with FCC policy, system owners should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The IPA helps system owners determine whether their systems will collect the kind of information that would make them subject to the requirements of Section 208. The PIA should not be completed if the IPA has not yet been completed first since it determines if your system requires a PIA.

If you have any questions, please contact the Privacy Manager, Les Smith, at leslie.smith@fcc.gov or 202-418-0217.

[1] 44 U.S.C. § 3501 note.

[2] OMB Memorandum No. M-03-22 (Sep. 26, 2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.

1.2. System Overview

A. Avoiding technical terms and unexplained abbreviations, please provide a general description of this information system.

Office 365 (O365) is a Software as a Service (SaaS) that supports the FCC mission through offerings including Exchange Online, SharePoint Online, OneDrive online storage, and Office Professional Plus for local use on PCs. O365 is used for three system configurations, including physical and virtual desktop workstations accessed through Microsoft Office Online, VDI, and mobile devices. O365 applications serve as tools for communication, collaboration, and daily business operations across the enterprise.

This privacy impact assessment (PIA) evaluates privacy implications for FCC's use of the cloud-based O365 service products listed below:

- OneDrive
- Outlook
- SharePoint
- Word
- Excel
- PowerPoint
- OneNote
- Access

B. Is this a new information system or a significant revision of an existing system?

☒ New System

☐ Revision of Existing System: Please describe the revision that will be made to an existing system.

C. Why is the FCC developing, procuring, or revising this information system? What is the purpose of this system?

The FCC uses O365 to simplify administration of licenses and subscriptions to services at an enterprise level and facilitate system-wide user management, password administration, and oversight of security controls. O365 also allows the FCC to streamline and simplify virtual communications and collaborations that support daily business operations.

D. If this system is going to be provided through a cloud-based computing system,[3] please check the box that best describes the service the FCC receives from the cloud computing provider:

☒ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS)

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

☐ 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)

E. Under what legal authority is the FCC developing, procuring, or revising this information system?

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.

[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. Nature and Use of the Information that Will Be Collected

A. Specify in the table below what types of personally identifiable information (PII) may be collected, maintained, or processed in this information system. Check all that apply and add any types that are not listed below.

Table 1-1: PII Elements Table

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name ☒ Date of Birth ☒ Home Address ☒ Phone Number(s) ☒ Place of Birth ☒ Age ☒ Race/ethnicity ☒ Alias ☒ Sex ☒ Email Address ☒ Work Address ☒ Taxpayer ID ☒ Credit Card Number ☒ Facsimile Number ☒ Medical Information ☒ Education Records ☒ Social Security Number ☒ Mother's Maiden Name	☒ Biometric Identifiers (e.g. fingerprint, voiceprint) ☒ Audio Recordings ☒ Photographic Identifiers (e.g. image, x-ray, video) ☒ Certificates (e.g. birth, death, marriage, etc.) ☒ Legal Documents, Records, Notes (e.g divorce decree, criminal records, etc.) ☒ Vehicle Identifiers (e.g. license plates) ☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.) ☒ Geolocation Information ☒ Passport Number	☒ User ID ☒ Internet Cookie Containing PII ☒ Employment Status, History or Information ☒ Employee Identification Number (EIN) ☒ Salary ☒ Military Status/Records/ID Number ☒ IP/MAC address ☒ Driver's License/State ID Number (or foreign country equivalent) ☒ Other (Please Specify):

Other: The FCC does not use O365 to collect or maintain personally identifiable information (PII) directly from members of the public.

FCC houses a variety of information in O365 depending on the needs and purposes of the bureaus and offices across the enterprise that use this software. Documents that could be created or housed in O365 applications may include a variety of regulatory and law enforcement documents, internal staff memoranda, Congressional correspondence, and Federal Register notices of rulemakings. To the extent PII from the public is stored in applications supported by O365, the information collection is incidental.

O365 may also contain information pertaining to end-users at the FCC including employees and contractors.

B. Please explain why it is necessary to collect these PII data elements to carry out the purpose of this system.

Information in O365 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.

C. Will this PII be collected from individuals themselves, or from third parties?

Source of Data	Type of Data Provided and How it is Collected
FCC Staff and Contractors	FCC staff and contractors upload data that has been created or obtained in connection with the Commission's regulatory, licensing, enforcement, personnel and security management, and other activities. User-created content may also include information in the user's profile, emails, calendar, and other information voluntarily stored within O365.
Members of the Public	The FCC generally does not use O365 applications to collect PII directly from the public; however, information provided by and pertaining to members of the public may be stored in O365 applications. These individuals may include consumers, individuals commenting on agency rulemakings, etc. For the majority of the FCC's applications on O365, the information is incidentally stored.

D. Will individuals be able to consent to the collection or particular uses of the information? What will the form of the consent be? What happens if individuals do not consent to the collection or particular uses?

The opportunity or right depends on how the information is collected. The FCC generally does not use O365 to collect information, including PII, directly from the public. However, FCC staff and contractors use O365 for business operations in furtherance of the FCC's enforcement or policy mission. To the extent information maintained in O365 applications incidentally includes PII, individuals will not have an opportunity to consent. To the extent that consent is required for the underlying collection, however, the FCC will obtain any consent necessary.

Information in O365 pertaining to FCC employees and contractors is collected to authenticate end-users and manage administrative business functions including personnel security, human resources, emergency notifications, etc.

E. Please explain how these PII data elements will be processed or used in the course of operating this information system.

O365 applications used by the FCC generally do not collect or maintain PII directly from the public. Any information provided by and pertaining to members of the public is incidentally stored. To the extent the incidental information is used, the use is ancillary to the FCC's enforcement, regulatory, licensing and other activities.

PII from FCC employees and contractors is processed and used for internal operational, personnel, and security management at the agency.

F. 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 O365 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 it is 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).

G. Are there procedures in place to allow individuals access to their PII or to correct inaccurate information?

To the extent any information in these FCC applications on O365 are "records" under the Privacy Act of 1974, an individual may make a request for access to information the FCC maintains about her or him. The FCC's Privacy Act Information page provides links to the FCC's System of Records Notices (SORNs), as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals seeking access must follow the FCC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 47 C.F.R. § 0.551, et seq. Access to information under the Privacy Act is subject to certain exemptions.

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

Information in the O365 cloud instance is retained and destroyed in accordance with applicable FCC policies and procedures, as well as with the FCC records disposition schedule and General Records Schedules approved by the National Archives and Records Administration (NARA). FCC staff receive training and reminders about their records and destruction obligations. All information will be securely and irreversibly disposed of/destroyed in accordance with applicable FCC policies and procedures, OMB, NARA, and NIST regulations and guidelines.

1.4. Data Security

A. Are there administrative procedures and technicial safeguards in place to protect the data in the system? What controls are in place to ensure proper use of the data?

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 4), https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

Additionally, the FCC purchases cloud computing services, including O365, from providers that have been authorized under the Federal Risk and Authorization Management Program (FedRAMP). Cloud service providers that have received this authorization have demonstrated that they apply security controls to their computing resources in a manner that is consistent with the federal risk-based information security requirements the FCC follows.

B. Has the system undergone the appropriate security risk assessment and received authority to operate?

The system has a System Security Plan from June 2015 that was updated in January 2016. Additionally, the FCC purchases cloud computing services from providers that have been authorized under the Federal Risk and Authorization Management Program (FedRAMP). Cloud service providers that have received this authorization have demonstrated that they apply security controls to their computing resources in a manner that is consistent with the federal risk-based information security requirements the FCC follows. O365's FedRAMP authorization was granted on November 20, 2014.

O365 first received Authority to Operate at the FCC on June 23, 2016, and was renewed on August 22, 2019.

1.5. Access and Sharing of 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 O365 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 O365 is appropriately limted. Access to the information stored within O365 is dependent on the particular business purpose and the access permissions granted to a specific user. For example, system administrators may have access to system data and system audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions.
Contractors	FCC may have contractor support within program areas, and these contractors will have access to the information in O365 as required to perform their duties.
Office of Inspector General (OIG)	Under appropriate circumstances, data showed within O365 or O365 log data may be provided to the OIG for auditing or law enforcement purposes.

B. Will the information be shared with 3rd parties as part of the operations of the information system (e.g., through an application programming interface or "API")?

Software as a service requires the service provider to have access to information collected and stored on its applications. Authorized FCC contractors have access to information in O365, when necessary. Some authorized FCC contractors have access to O365 simply as users, and one or more authorized FCC contractors have access to certain administrative functions. All FCC contractors are required to complete security and privacy training prior to obtaining access to any FCC systems, and complete annual security and privacy training to maintain network access and access to those systems.

Contractors who access O365 are subject to the same rules and policies as FCC staff. Contractors must also follow the reporting and other procedures in the FCC's Breach Notification Policy.

Additionally, the system is connected directly to FCC Active Directory for user account information and access across numerous FCC applications and systems.

1.6. Privacy Act System of Records Notice

A. Is the FCC planning to publish or has it already published a Privacy Act System of Records Notice (SORN) for this information system? If the FCC has already published a SORN, please provide a citation to the Federal Register.

The FCC is not required to publish a SORN for O365 because it is not a system of records, as that term is defined the Privacy Act, 5 U.S.C. § 552a(a)(5).

Appendix A - Acronyms and Abbreviations

Table A-1: Acronyms and Abbreviations

Acronym	Definition
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Modernization Act
FOIA	Freedom of Information Act
IaaS	Infrastructure as a Service
IPA	Initial Privacy Assessment
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PaaS	Platform as a Service
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SaaS	Software as a Service
SORN	System of Records Notice