U.S. Securities and Exchange Commission

Microsoft 365 (M365)

PRIVACY IMPACT ASSESSMENT (PIA)

February 28, 2025

Office of Information Technology

Publication History

Revision	Date	Changes Made
Initial	6/28/2023	Original Document
1	2/28/2025	Update for compliance with E.O. 14168

Section 1: Project or System Overview

1.1 Name of Project or System

Microsoft 365 (M365)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Office of Information Technology (OIT)

☒ Externally Hosted (Contractor or other agency/organization)

1.3 Reason for completing PIA

☒ New project or system

1.4 Does the system or program employ any of the following technologies?

☐ Electronic Data Warehouse (EDW)
☐ Social Media
☒ Mobile Application (or GPS)
☒ Cloud Computing Services
☐ www.sec.gov Web Portal
☐ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

Microsoft 365 (M365) is a cloud-based Software-as-a-Service (SaaS) solution, used by the SEC to provide enterprise communication, productivity, and collaboration solutions to support the agency's business needs. The objective of M365 cloud services implementation is to modernize the technology the SEC currently uses and to enhance the agency's operations by providing additional functions and features beyond the agency's current on-premise products. This implementation will allow the SEC to achieve efficient and effective information management; simplify administration of licenses and subscriptions to services at an enterprise level; and facilitate system-wide user management and oversight of security controls. Implementation of M365 also aligns with the Federal IT and Cybersecurity modernization component of the President's Management Agenda.

M365 is a subscription-based service, which provides access to numerous Microsoft services and software. Currently, the following M365 applications are available to the SEC workforce:

- Exchange Online – A cloud-based service that works in tandem with Microsoft Outlook to provide SEC users with email, calendaring, contacts and tasks, and supports mobile and web-based access to information, as well as mailbox data storage. 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. Active Directory serves as the SEC's identity, authentication, and access management service that provides an SEC-wide Global Address List (GAL) for authorized users.
- Teams – A cloud-based communication platform that enables real-time communication and collaboration; document sharing and storage; and meeting participation. Collaboration tools and content may be accessed, as needed (e.g., Chat and Calendar, online audio and video calling/conferencing; and screen and file sharing.) Teams connects with SharePoint, OneDrive, and Exchange to allow users to work seamlessly between these applications.

- OneDrive for Business – A file hosting service accessed via web browser. Serves as a personal cloud file storage area that allows users to 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 to create and store files directly in the cloud, using the standard suite of M365 applications such as Word, Excel, and PowerPoint. OneDrive may supplement, and eventually replace, employees' assigned network drives that contain documents and files that each employee has saved externally from their government-issued computers.
- SharePoint Online (SPO) – A web-based collaboration and document management and storage platform. SPO is a secure cloud data storage that allows document organization, sharing, and quick and efficient information access for greater collaboration and co-authoring of documents and related tasks.
- Microsoft Dataverse (MDV) – A cloud-based storage to securely store and manage data that is generated by M365 Power Apps.

Future implementation will include:

- Power Platform (Power Apps, Power Automate, Power Business Intelligence (BI), Virtual Agent) – A platform for building low code/no code applications, automating workflows and tasks, and performing business analysis and reporting.
- On-premises Data Gateway – A feature that provides secure data transfer between on-premises data (data not in the cloud) and cloud services and the Power Platform.

M365 and its applications are available and accessible on SEC provisioned laptops and some are available on SEC provisioned mobile devices (e.g., Outlook, Teams, OneDrive) to provide general environment tools, such as data storage; software maintenance tools, such as software security patches, application upgrades, and back up of data within the environment; and access management tools. M365 provides these services based upon the SEC's selection and approval of applications within the Microsoft Cloud infrastructure.

As additional M365 applications and functionality are added, they will be evaluated, and this PIA updated, as appropriate.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

The SEC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs. M365 may collect, maintain, transmit or share PII in support of authorized business functions pursuant to rules, regulations, and orders of Commission. The authority to collect information within M365 lies within each program area's legal authorities. 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.

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

M365 system applications do not collect the Social Security number (SSN). However, the SSN may be maintained within an application as part of deliverables stored therein, for example documents, spreadsheets, etc. The authority and purpose for the collection of the SSN is delineated in the applicable SORN for the respective program area.

2.4 Does the system or electronic collection require a Privacy Act System of Records Notice (SORN)? If yes, list the Privacy Act SORN Identifier(s).

M365 does not create a new system of records. Information covered by the Privacy Act. PII may be hosted within an application as part of deliverables stored therein, for example documents, spreadsheets, etc. The covering SORN varies by the mission of the respective program area. The information may be covered under a variety of existing SEC and government-wide SORNs. A full inventory of SEC's SORNs is available at: https://www.sec.gov.gov/privacy.

2.5 Does the system or electronic collection require an OMB Control Number? If yes, describe.

No

2.6 What privacy risks were identified related to authority and purpose of collection and how were those risks mitigated?

There is a risk that sensitive information, including PII, stored in M365 could potentially be used or shared for a purpose not compatible with the original purpose for which the information was collected. This risk is mitigated by users being appropriately trained on usage and applicable policies and procedures. The risk is further mitigated by a combination of technical and operational controls to reduce the risk associated with the environment, such as monitoring, reporting, encryption, passwords, audit logs, firewalls, malware identification and data loss prevention program.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

Identifying Numbers					
☒	Social Security Number	☒	Alien Registration	☒	Financial Accounts
☒	Taxpayer ID	☒	Driver's License Number	☒	Financial Transactions
☒	Employee ID	☒	Passport Information	☒	Vehicle Identifiers
☒	File/Case ID	☒	Credit Card Number	☒	Employer ID
☒	**General Personal Data**				
☒	Name	☒	Date of Birth	☒	Marriage Records
☒	Maiden Name	☒	Place of Birth	☒	Financial Information
☒	Alias	☒	Home Address	☒	Medical Information
☒	Sex	☒	Telephone Number	☒	Military Service

☒	Age	☒	Email Address	☒	Mother's Maiden Name
☒	Race/Ethnicity	☒	Education Records	☒	Health Plan Numbers
☒	Civil or Criminal History	☒	Zip Code		
Work-Related Data					
☒	Occupation	☒	Telephone Number	☒	Salary
☒	Job Title	☒	Email Address	☒	Work History
☒	Work Address	☒	Certificate/License Number	☒	Business Associates
☒	PIV Card Information	☒	Fax Number		
Distinguishing Features/Biometrics					
☒	Fingerprints	☒	Photographs	☒	Genetic Information
☒	Voice Recording	☒	Video Recordings	☒	Voice Signature
System Administration/Audit Data					
☒	User ID	☒	Date/Time of Access	☒	ID Files Accessed
☒	IP Address	☒	Queries Ran	☒	Contents of Files

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

Information in M365 applications is collected, used, disseminated, and maintained for the SEC to perform its regulatory, enforcement, policy, personnel management, and other mission and business activities.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees
Email, Teams chats, Microsoft Office and other M365 application files, other files and deliverables

☒ SEC Federal Contractors
Purpose: Email, Teams chats, Microsoft Office and other M365 application files, other files and deliverables

☒ Interns
Purpose: Email, Teams chats, Microsoft Office and other M365 application files, other files and deliverables

☒ Members of the Public
Purpose: Email, Microsoft Office files and other files and deliverables

☐ Employee Family Members
Purpose:

☒ Former Employees
Purpose: Email, Teams chats, Microsoft Office and other M365 application files, other files and deliverables

☒ Job Applicants
Purpose: Email, Microsoft Office and other files and deliverables

☒ Vendors
Purpose: Email, Microsoft Office and other files and deliverables

☒ Other: Federal Detailees (Government employees temporarily assigned to another position.)
Purpose: SEC Employees

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

PII from M365 is not used for testing, training, or/or research.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

SEC records are retained in accordance with SEC Regulation, *Records and Information Management Program*, which is informed by the Federal Records Act and NARA regulations. Due to the nature of M365, there may be numerous records schedules with different retention requirements applicable to the records created and maintained by M365 users. It is the responsibility of the respective M365 users to maintain and dispose of the records they create in accordance with the appropriate records retention schedules applicable to their program area.

3.6 What are the procedures for identification and disposition at the end of the retention period?

Due to the nature of M365, there may be numerous records schedules with different retention requirements applicable to the records created and maintained by M365 users. It is the responsibility of the respective M365 users to maintain and dispose of the records they create in accordance with the appropriate procedures and records retention schedules, applicable to their program area.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☒ N/A

3.8 What privacy risks were identified related to data collection, minimization, and retention and how were those risks mitigated?

There is a risk that the PII maintained by M365 may be unnecessary or excessive or may be kept longer than is necessary to meet the business need for which it was collected. This risk is mitigated by M365 users being appropriately trained on and following requirements, policies and procedures. SEC users are required to complete Annual Records Management Training, which explains records and information management (RIM) and responsibilities for managing SEC records. Additionally, SEC users are responsible for complying with applicable Records and Information Management Program SEC Regulation(s) (SECR) regarding the creation, organization, maintenance, use and disposition of all SEC records, which is informed by the Federal Records Act and National Archives and Records Administration (NARA) regulations.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☒ N/A
☐ Privacy Act Statement
☐ System of Records Notice
☐ Privacy Impact Assessment (*Date of Last Update)*
☐ Web Privacy Policy

4.2 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this information system or project operate? Provide number and name.

M365 does not operate as a Privacy Act system of records. However, M365 may be used to process, store, maintain, disseminate, or disclose information about individuals that is collected from other SEC systems that do operate as Privacy Act systems of records. A full inventory of SEC's SORNs is available at: https://www.sec.gov.gov/privacy.

4.3 What privacy risks were identified regarding openness and transparency and how were those risks mitigated?

There is a risk that individuals are not aware that their data is maintained and used within M365. M365 does not

operate as a Privacy Act system of records. Therefore, notice, in the form of a Privacy Act Statement or SORN, is not required. However, in instances where PII is obtained from other SEC systems that operate as Privacy Act systems of records, notice is provided through the publication of SEC's SORNs for those systems, which are available at: https://www.sec.gov/privacy, as well as notice about the collection and use of their information, as appropriate, at the point at which it is collected. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

M365 does not aggregate or consolidate data in order to make determinations or derive new data about individuals.

5.2 Will internal organizations have access to the data?

Access to the data within M365 is limited based on business need and applicable SEC regulations, policies, and procedures. Users may use M365 applications to share data with those who have a need to know. Access to information is granted by the pertinent data owner and controlled using role-based permissions that are dependent upon a person's need to know and the principle of least privilege. 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. Further, all SEC information and information system users must annually complete the SEC's Privacy and Information Security Awareness Training, which includes the Rules of the Road.

5.3 Will external organizations have access to the data?

Authorized SEC users may use M365 to share data external to SEC, e.g., Outlook, that was obtained from other SEC systems that operate as Privacy Act systems of records. M365 users are responsible for ensuring that any sharing of information external to SEC is in accordance with the routine uses stipulated in SEC's SORNs, which are available at: https://www.sec.gov/privacy.

5.4 What information will be shared and with whom?

Any sharing of information in M365 applications varies by the mission of the program offices and is within the scope of the SEC's governing statues and regulations.

5.5 What privacy risks were identified regarding use limitation and sharing of information and how were those risks mitigated?

There is a risk that information in M365 will be used by or shared with unauthorized user as follows:

- Individuals may be able to view files, or folders when collaborative file system access is mistakenly or unknowingly shared by the owner. M365 users, including site owners, must take proper precautions when setting collaborative file system access permissions to ensure only those with a need to know are granted access. Mitigation of this risk is dependent, in part, on the users, who are the subject matter experts concerning the information they place into M365, adhering to Privacy Act systems of records and any applicable information or data handling policies and procedures pertinent to their program information.

- Individuals may take screenshots using phone cameras and other video or photo devices or screen capture or recording tools during a meeting conducted with cloud-based collaborative audio-video tools without notifying participants or the individual sharing the content. Meeting participants are responsible for sharing only that content which is applicable to the meeting and for ensuring that those attending the

meeting have a business need to participate and view any information discussed and presented during the meeting.

- Individuals participating in a meeting conducted using cloud-based collaborative audio-video tools may unknowingly be recorded without their consent. SEC's cloud-based collaborative audio-video tools display a banner that notifies meeting participants when a session is being recorded. Participants have the option of exiting, or may consent to the recording by participating in the meeting. Further, meeting participants can disable their cameras and microphones during calls and meetings.

- Individuals may inadvertently gain access to cloud-based collaborative audio-video meetings. Meeting organizers are responsible for ensuring that meeting participants are restricted to those having an authorized purpose.

In addition to the noted mitigation actions, SEC users are responsible for compliance with the Rules of the Road and are required to complete annual Privacy and Information Security Awareness Training, which includes information on rules and regulations regarding the sharing of PII.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

M365 is not intended to collect PII directly from individuals. However, M365 may maintain or process PII that was obtained from other SEC systems or programs. In those instances where PII is collected by other SEC systems, the SEC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974.

6.2 What methods will be used to collect the data?

The sources of the PII in M365 include the following:

Data Source	Description of Information Provided by Source
Active Directory/Global Address List Information	The information in the GAL includes business contact information about SEC employees and contractors with active SEC authorized email addresses. This contact information typically includes the individual's name, title, SEC email address, office location, work telephone number, and physical business mailing address. The information is obtained from SEC employees and contractors during the SEC onboarding process.
Email/Mailbox/Archive	Email messages could potentially include any type of PII that is pertinent and necessary for fulfilling a legitimate SEC business function (e.g., personnel data, examination and enforcement data, legal documents, etc.). The source of an email message is the sender of the message, who could be an SEC employee/ contractor or a member of the public.
Collaborative Audio-Video Tools	The use of cloud-based collaborative audio-video tools facilitates the sharing of information, including PII, that is necessary for fulfilling a legitimate SEC business function (e.g., personnel data, examination and enforcement data, legal documents, etc.). The source of information shared via these tools could be an SEC employee/ contractor or a member of the public.
Collaborative File Systems	The use of cloud-based collaborative file systems facilitates the sharing of information, including PII, that is necessary for

	fulfilling a legitimate SEC business function (e.g., personnel data, examination and enforcement data, legal documents, etc.). The source of information maintained within the collaborative file systems could be an SEC employee/contractor, or a member of the public.

6.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.

User generated content that is stored in M365 is not checked for accuracy. It is the responsibility of M365 users to ensure the data that they create, transmit or share using M365 is not inaccurate or outdated. The SEC reviews privacy artifacts to ensure adequate measures are taken to check for and correct any inaccurate or outdated PII in its holdings.

6.4 Does the project or system process, or access, PII in any other SEC system?

Multiple SEC applications interface with M365 to retrieve business contact information (e.g., network user names, network IDs, and email addresses) from AD to support the administration of access controls and SEC's single sign-on functionality, and from the GAL to send and receive electronic business communications for authorized purposes.

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

There is a risk that the information maintained and processed by M365 may not be accurate. This risk cannot be fully mitigated by M365 and is primarily dependent on users who generate content and end users who have responsibility for the content they maintain and process using M365. The collaborative nature of some M365 components provide a platform where those involved in the collaboration may address inaccuracies identified. Information maintained and processed by M365 that is used by the SEC as part of its enforcement, examination, compliance, legal, administrative, and other legally authorized functions will be reviewed for accuracy and timeliness as required by the particular function, laws, and authorities, if any, applicable at the time the agency compiles the information.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

M365 does not operate as a Privacy Act system of records and is not intended to collect PII directly from individuals. However, M365 may maintain or process PII that was obtained from other SEC systems or programs. In those instances where PII is collected by other SEC systems or programs, the SEC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974. The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.

7.2 What procedures are in place to allow individuals to access their information?

M365 does not have procedures for individual access since it does not operate as a Privacy Act system of records and, therefore, is not subject to the Privacy Act individual access requirement. However, in cases where M365 facilitates the transport, exchange, or sharing of information related to SEC Privacy Act systems of records, the SEC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act. The SEC publishes its SORNs on the SEC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act. The SEC publishes access procedures in its SORNs, which are

available on the SEC public facing website. The SEC adheres to Privacy Act requirements and Office of Management and Budget (OMB) policies and guidance for the proper processing of Privacy Act requests.

7.3 Can individuals amend information about themselves in the system? If so, how?

M365 does not have procedures to allow individuals to correct inaccurate or erroneous information since it does not operate as a Privacy Act system of records, and therefore, is not subject to the Privacy Act redress requirement. However, in cases where M365 facilitates the transport, exchange, or sharing of information related to SEC Privacy Act systems of records, the SEC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act. The SEC publishes its SORNs on the SEC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act. The SEC publishes access procedures in its SORNs, which are available on the SEC public facing website. The SEC adheres to Privacy Act requirements and Office of Management and Budget (OMB) policies and guidance for the proper processing of Privacy Act requests.

7.4 Discuss the privacy risks related to individual participation and redress? How were these risks mitigated?

There is a risk that individuals do not have the opportunity to access their information or amend inaccurate information contained within M365. While M365 does not operate as a Privacy Act systems of records, and is not subject to the Privacy Act redress requirement, in instances where PII is obtained from other SEC systems that operate as Privacy Act systems of records, information regarding how individuals may access and amend their information in those systems is provided through the publication of SEC's SORNs for those systems, which are available at: https://www.sec.gov/privacy.

Section 8: Security

8.1 Can the system be accessed outside of a connected SEC network?

No

8.2 Does the project or system involve an online collection of personal data?

No

8.3 Does the site have a posted privacy notice?

N/A

Section 9: Accountability and Auditing

9.1 Describe what privacy-related training is provided to users, either general or specific to the system or project.

All SEC users receive initial and annual privacy and information security awareness training, and sign SEC's Rules of the Road, which outline roles and responsibilities for proper handling and protection of PII. In addition, training and guidance concerning the use of various applications within M365 is offered to end users.

9.2 Does the system generate reports that contain information on individuals?

M365 produces audit logs which may contain information on user actions related to applications accessed and which features/modules are used, as well as capacity/usage data.

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

Yes, privacy requirements for contractors and service providers are mandated and are documented in relevant contracts.

9.4 Does the system employ audit logging or event logging?

Yes

9.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

M365 is used by all SEC divisions and offices. Within their respective workspaces, SEC users can use the tools of M365 to produce and/or store deliverables, which may include Office files, dashboards, and other products. Content access is controlled by role-based security groups. SEC divisions and 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. To mitigate this risk, user accounts are synched with Active Directory and system privileges are granted through role-based access control.