U.S. Nuclear Regulatory Commission

Privacy Impact Assessment
Microsoft 365 (M365)
Office of the Chief Information Officer (OCIO)

Version 1.0
06/06/2025

Template Version 2.5 (03/2025)

Document Revision History

Date	Version	PIA Name/Description	Author
06/06/2025	1.0	M365 Initial Release	NRC Privacy Office

Table of Contents

The agency 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 help determine any privacy risks related to the E-Government Act or later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

Name/System/Subsystem/Service Name: M365.

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform) Microsoft Cloud.

Date Submitted for review/approval: June 6, 2025.

Note: When completing this PIA do not include any information that would raise security concerns or prevent this document from being made publicly available.

1 Description

1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as "project"). Explain the reason the project is being created.

Microsoft 365 (M365) is a cloud-based Software-as-a-Service (SaaS) solution, used by the NRC to provide enterprise communication, productivity, and collaboration solutions to support the agency's business needs.

M365 is a subscription-based service, which provides access to numerous Microsoft services and software such as but not limited to:
Exchange Online/Outlook
Teams
One Drive for Business
OneNote
Office Products (Word, Excel, PowerPoint.)
SharePoint Online
External SharePoint Sharing
Power Platform

Microsoft Copilot Chat, a generative AI assistant for improving productivity and workflows through natural language conversations, was approved for use at the NRC June 2025. NRC's version of Copilot Chat also includes commercial data protection, ensuring that individual chat interactions are private, not saved by Microsoft, or used to train the underlying AI models. The information used in Copilot Chat remains safeguarded within our secure GCC tenant environment. As a result, employees are authorized to access and use internal NRC data with Microsoft Copilot Chat.

M365 and its applications are available and accessible on NRC provisioned laptops and mobile devices. As additional M365 applications and functionality are added, this PIA will be updated as appropriate.

Please mark appropriate response below if your project/system will involve the following:

☒ PowerApps	☒ Artificial Intelligence (AI)
☐ Dashboard	☐ Public Website
☒ SharePoint	☐ Internal Website
☒ Cloud Service Provider	☒ Other – *(numerous M365 apps)*
☐ Server/Database Design	

1.2 Does this privacy impact assessment (PIA) support a proposed new project, proposed modification to an existing project, or other situation? Select options that best apply in table below.

Mark appropriate response.

Status Options	
☒	New system/project
☐	Modification to an existing system/project. *If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.*
☐	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below.*
☐	Other (explain)

1.3 Points of Contact:

Role	Contact Information Name Office/Division/Branch Phone Number
Project Manager(s)	Bob Randall James Hardin
System Owner/Data Owner or Steward	Jonathan Feibus
ISSM	Branden Jarrell Zanira Khan
Executive Sponsor	Scott Flanders
Other	

2 Authorities and Other Requirements

2.1 What specific legal authorities and/or agreements permit the collection of information for the project?

Provide all statutory and regulatory authorities for operating the project, including the authority to collect the information; NRC internal policy is not a legal authority. Please mark appropriate response in table below.

Mark with an "X" on all that apply.	Authority	Citation/Reference
☐	**Statute**	
☐	**Executive Order**	
☐	**Federal Regulation**	
☐	**Memorandum of Understanding/Agreement**	
☒	**Other (summarize and provide a copy of relevant portion)**	The NRC 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.

2.2 Explain how the information will be used under the authority listed above (*i.e., enroll employees in a subsidies program to provide subsidy payment*)**.**

The authority to collect information within M365 lies within each program area's legal authorities defined within their various PIAs and SORNs.

If the project collects Social Security numbers, state why this is necessary and how it will be used.

M365 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.

3 Characterization of the Information

In the table below, mark the categories of individuals for whom information is collected.

Category of individual	
☒	Federal employees
☒	Contractors
☒	Members of the Public (any individual other than a federal employee, consultant, or contractor)
☒	Licensees
☐	Other

In the table below, is a list of the most common types of PII collected. Mark all PII that is collected and stored by the project/system. If there is additional PII not defined in the table below, a comprehensive listing of PII is provided for further reference in ADAMS at the following link: PII Reference Table.

Categories of Information			
☐	Name	☐	Resume or curriculum vitae
☐	Date of Birth	☐	Driver's License Number
☐	Country of Birth	☐	License Plate Number
☐	Citizenship	☐	Passport number
☐	Nationality	☐	Relatives Information
☐	Race	☐	Taxpayer Identification Number
☐	Home Address	☐	Credit/Debit Card Number
☐	Social Security number (Truncated or Partial)	☐	Medical/health information
☐	Sex (Male or Female)	☐	Alien Registration Number
☐	Ethnicity	☐	Professional/personal references
☐	Spouse Information	☐	Criminal History
☐	Personal e-mail address	☐	Biometric identifiers (facial images, fingerprints, iris scans)
☐	Personal Bank Account Number	☐	Emergency contact e.g., a third party to contact in case of an emergency
☐	Personal Mobile Number/Home Number	☐	Accommodation/disabilities information
☐	Marital Status	☒	Microsoft 365 (M365) may collect, maintain, transmit, or share PII in support of authorized business functions, in accordance with applicable laws, regulations, and Commission directives. Each program area is responsible for
☐	Children Information		
☐	Mother's Maiden Name		

Categories of Information			
			ensuring it has the legal authority to handle such information and must complete a PIA for any activities involving PII.

3.1 Describe how the data is collected for the project. (i.e., NRC Form, survey, questionnaire, existing NRC files/ databases, response to a background check).

Microsoft 365 (M365) is not intended to collect Personally Identifiable Information (PII) directly from individuals. However, it may maintain or process PII obtained through other NRC systems or programs (e.g., forms, surveys, or questionnaires). When PII is collected by other NRC systems, the NRC ensures that all forms—whether paper-based or electronic—include an appropriate Privacy Act Statement, as required by the Privacy Act of 1974.

3.2 If using a form (paper or web) to collect the information, provide the form number, title and/or a link to the form.

See response under 3.1.

3.3 Who provides the information? Is it provided directly from the individual or a third party.

See response under 3.1.

3.4 Explain how the accuracy of the data collection is validated. If the project does not check for accuracy, please explain why.

M365 does not validate the accuracy of the data it processes, as it is not a Privacy Act system of records. However, when M365 is used to transport, exchange, or share information related to NRC Privacy Act systems of records, individuals are provided access to their PII through the respective source systems. This allows them to review and request corrections to their information, ensuring data accuracy is maintained at the source level.

3.5 Will PII data be used in a test environment? If so, explain the rationale for this and how the PII information is protected.

N/A.

3.6 What procedures are in place to allow the subject individual to correct inaccurate or erroneous privacy information?

Procedures for correcting inaccurate or erroneous privacy information are handled at the source system level, not within Microsoft 365 (M365). M365 users are responsible for ensuring the accuracy of the data they create, transmit, or share. NRC offices that manage systems storing or processing PII are responsible for implementing appropriate measures to review, verify, and correct any inaccurate or outdated information within those systems.

4 Data Security

4.1 Describe who has access to the data in the project (i.e., internal NRC, system administrators, external agencies, contractors, public).

Access to data within the Microsoft 365 (M365) environment is limited to authorized internal NRC users, including system administrators and contractors, as necessary to perform official duties. M365 itself does not provide individual access procedures, as it is not a Privacy Act system of records and is not subject to individual access requirements under the Privacy Act. However, when M365 is used to facilitate the transport, exchange, or sharing of information from NRC Privacy Act systems of records, individuals may access their PII through the respective source systems, in accordance with the Privacy Act. NRC users must comply with agency Rules of Behavior and are required to complete annual Privacy and Information Security Awareness Training, which addresses the appropriate handling and sharing of PII.

4.2 If the project/system shares information with any other NRC systems, identify the system, what information is being shared and the method of sharing.

M365 may facilitate the sharing of information with other NRC systems; however, it does not directly integrate or automatically share data with specific systems. M365 users—including site owners—are responsible for setting appropriate access permissions to ensure that only individuals with a need to know can access the shared information. The risk of unauthorized access is mitigated by user adherence to applicable Privacy Act systems of records and NRC policies governing data handling, access control, and privacy protection.

4.3 If the project/system connects, receives, or shares information with any external non-NRC partners or systems, identify what is being shared.

N/A.

If so, identify what agreements are in place with the external non-NRC partner or system in the table below.

Agreement Type	
☐	Contract Provide Contract Number:
☐	License Provide License Information:
☐	Memorandum of Understanding Provide ADAMS ML number for MOU:
☐	Other
☐	None

4.4 Describe how the data is accessed and describe the access control mechanisms that prevent misuse.

Data within Microsoft 365 (M365) is accessed by authorized NRC users across all divisions and offices. Users interact with M365 tools—such as SharePoint, OneDrive, and Teams—to produce, store, and collaborate on deliverables, including Office files, dashboards, and other digital products. Access to this content is governed by role-based access control (RBAC), with permissions assigned through role-based security groups. Each NRC division or office is responsible for managing and periodically reviewing access to its respective M365 collaborative workspaces and stored content to ensure that only individuals with a valid need to know are granted access. This layered approach helps prevent unauthorized access and misuse of sensitive information**.**

4.5 Explain how the data is transmitted and how confidentiality is protected (i.e., encrypting the communication or by encrypting the information before it is transmitted).

Data transmitted within M365 is protected through multiple layers of security to ensure confidentiality and integrity. All data in transit is encrypted using federal-standard protocols such as TLS (Transport Layer Security), and data at rest is also encrypted using strong encryption algorithms. These measures help prevent unauthorized access during transmission and storage. While there is a risk that PII stored in M365 could be used or shared for purposes not aligned with its original collection intent, this risk is mitigated through a combination of user training and strict adherence to NRC policies and procedures.

Additional technical and operational safeguards include:

- Multi-Factor Authentication (MFA) to ensure only authorized users can access the system
- Audit logging and monitoring to track access and detect suspicious activity
- Firewalls and malware protection to guard against external threats
- NRC's Data Loss Prevention (DLP) program to identify and restrict the sharing of sensitive information
- Role-based access controls to limit access to only those with a legitimate need to know

Together, these measures help maintain the confidentiality, integrity, and appropriate use of sensitive data transmitted or stored within the M365 environment.

4.6 Describe where the data is being stored (i.e., NRC, Cloud, Contractor Site).

Microsoft cloud.

4.7 Explain if the project can be accessed or operated at more than one location.

M365 is productivity software used for collaborating with NRC users in many locations.

4.8 Can the project be accessed by a contractor? Have the contractors completed an IT-II investigation? Do they possess an NRC badge?

Yes- M365 can be accessed by a contractor who has been vetted by the NRC.

4.9 Explain the auditing measures and technical safeguards in place to prevent misuse of data.

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.

4.10 Describe if the project has the capability to identify, locate, and monitor (i.e., trace/track/observe) individuals.

N/A.

4.11 Define which FISMA boundary this project is part of.

Information Technology Infrastructure.

4.12 Is there an Authority to Operate (ATO) associated with this project/system?

Authorization Status	
☐	Unknown
☐	No *If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track*.
☐	In Progress provide the estimated date to receive an ATO. Estimated date:
☒	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality-Moderate Integrity- Moderate Availability- Moderate

4.13 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact EA Service Desk to get the EA/Inventory number.

EA # 20090005.

5 Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

Response	
☐	**Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, or other unique number, etc.)** **List the identifiers that will be used to retrieve the information on the individual.**
☒	**No, the PII is not retrieved by a personal identifier.** **If no, explain how the data is retrieved from the project.** PII within M365 is not retrieved by a personal identifier. If any information is retrievable, it would be accessed and managed through the originating source system or by the designated system owner. M365 serves only as a platform for collaboration and data handling—not as a system of records for retrieving PII by individual identifiers.

5.2 For all collections where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a System of Record Notice (SORN) in the Federal Register. *As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personal identifier assigned to the individual.*

Mark the appropriate response in the table below.

Response	
☐	***Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html)*** ***Provide the SORN name, number, (List all SORNs that apply):***
☐	**SORN is in progress**
☐	**SORN needs to be created**
☐	**Unaware of an existing SORN**
☒	**No, this system is not a system of records and a SORN is not applicable.**

5.3 When an individual is asked to provide personal data (i.e., form, webpage, survey), is a Privacy Act Statement (PAS) provided?

A Privacy Act Statement is a disclosure statement required to appear on documents used by agencies when an individual is asked to provide personal data. It is required for any forms, surveys, or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records.

Mark the appropriate response.

Options	
☐	**Privacy Act Statement**
☒	**Not Applicable**
☐	**Unknown**

5.4 Is providing the PII mandatory or voluntary? What is the effect on the individual by not providing the information?

Not Applicable. Refer to the source system collecting the PII.

6 Records and Information Management-Retention and Disposal

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are **Temporary** (eligible at some point for destruction/deletion because they no longer have business value) or **Permanent** (eligible at some point to be transferred to the National Archives because of historical or evidential significance). Records/data and information with historical value, identified as having a "permanent" disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a "temporary" disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR, agencies are required to establish procedures for addressing Records and Information Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for NARA's Universal Electronic Records Management (ERM) requirements, and if a mitigation strategy is needed to ensure compliance.

If the project/system:

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,
- Involves a cloud solution,
- And/or if there are additional questions regarding Records and Information Management - Retention and Disposal, please contact the NRC Records staff at **ITIMPolicy.Resource@nrc.gov** for further guidance.

If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.

6.1 Does this project map to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules?

☒	NUREG-0910, "NRC Comprehensive Records Disposition Schedule
☒	NARA's General Records Schedules
☒	Unscheduled

6.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.

System Name (include sub-systems, platforms, or other locations where the same data resides)	Microsoft 365
Records Retention Schedule Number(s)	NUREG-0910, "NRC Comprehensive Records Disposition Schedule GRS 3.2 010: Information Systems Security Records GRS 6.3 010: Information Technology Records Unscheduled
Approved Disposition Instructions	NUREG-0910, "NRC Comprehensive Records Disposition Schedule GRS 3.2 010: Information Systems Security Records: Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

	GRS 6.3 010: Information Technology Records: Temporary. Destroy when 7 years old, but longer retention is authorized if required for business use. Unscheduled: Additional information/data/records kept in this system may need to be scheduled; therefore, NRC records personnel will need to work with staff to develop a records retention and disposition schedule for records created or maintained. Until the approval of such schedule, these records and information are Permanent. Their willful disposal or concealment (and related offenses) is punishable by fine or imprisonment, according to 18 U.S.C., Chapter 101, and Section 2071. Implementation of retention schedules is mandatory under 44 U.S. 3303a (d), and although this does not prevent further development of the project, retention functionality or a manual process must be incorporated to meet this requirement
Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records accessibility, reliability, integrity, and disposition.	Microsoft 365 will be assessed using the Records and Information (RIM) Certification process. The structured process will provide criteria aligned with the Suggested Rating to accurately reflect the system's ability to support records management requirements.
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	Microsoft 365 will be assessed using the Records and Information (RIM) Certification process. The structured process will provide criteria aligned with the Suggested Rating to accurately reflect the system's ability to support records management requirements.
Disposition of Permanent Records Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions? If so, what formats will be used? **NRC Transfer Guidance (Information and Records Management Guideline - IRMG)**	N/A.

Note: Information in *Section 6, Records and Information Management-Retention and Disposal* does not need to be fully resolved for final approval of the privacy impact assessment.

7 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an Office of Management and Budget (OMB) approval in the form of a "control number"—before promulgating a paper form, website, surveys, questionnaires, or electronic submission from 10 or more members of the public. If the data collection is from federal employees regarding work-related duties, then a PRA clearance is not necessary.

7.1 Will the project be collecting any information from 10 or more persons who are not Federal employees?

M365 is not designed for direct data collection from individuals. If any information is collected, it would be the source system's responsibility to provide a response.

7.2 Is there any collection of information addressed to all or a substantial majority of an industry (i.e., Fuel Fabrication Facilities or Fuel Cycle Facilities)?

M365 is not designed for direct data collection from individuals. See response for 7.1.

7.3 Is the collection of information required by a rule of general applicability?

M365 is not designed for direct data collection from individuals. See response for 7.1.

Note: For information collection (OMB clearances) questions: contact the NRC's Clearance Officer. Additional guidance can be found on the NRC's internal Information Collections Web page at: https://intranet.nrc.gov/ocio/33456.

STOP HERE - The remaining pages will be completed by the Privacy Officer, Records Management, and Information Collections Team.

8 Privacy Act Determination

Project/System Name: M365

Submitting Office: Office of the Chief Financial Officer

Privacy Officer Review

Review Results		Action Items
☐	This project/system **does not contain PII.**	**No further action** is necessary for Privacy.
☐	This project/system **does contain PII**; the Privacy Act does **NOT** apply, since information is NOT retrieved by a personal identifier.	**Must be protected with restricted access** to those with a valid need-to-know.
☒	This project/system **does contain PII**; the **Privacy Act does apply**.	**SORN is required-** Information is **retrieved** by a personal identifier**.**

Comments:

M365 is not designed for direct data collection from individuals, it is a platform for storing and managing data. If any information is collected, it would be the source system's responsibility to submit a PIA for any data collection in order to determine if a SORN is required.

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 07/10/25	Privacy Officer

9 OMB Clearance Determination

NRC Clearance Officer Review

Review Results	
☒	No OMB clearance is needed.
☐	OMB clearance is needed.
☐	Currently has OMB Clearance. Clearance No._____

Comments:

Reviewer's Name	Title
Signed by Benney, Kristen on 06/16/25	Acting Agency Clearance Officer

10 Records Retention and Disposal Schedule Determination

Records Information Management Review

Review Results	
☐	No record schedule required.
☐	Additional information is needed to complete assessment.
☒	Needs to be scheduled.
☐	Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
Signed by Dove, Marna on 07/09/25	Sr. Program Analyst, Electronic Records Manager
Signed by Williams, Lisa on 06/26/25	Records and Information Management Specialist

11 Review and Concurrence

Review Results	
☒	This project/system **does not** collect, maintain, or disseminate information in identifiable form.
☐	This project/system **does** collect, maintain, or disseminate information in identifiable form.

I concur with the Privacy Act, Information Collections, and Records Management reviews.

Signed by Nalabandian, Garo
on 07/10/25

Director
Chief Information Security Officer
Cyber Information Security Division
Office of the Chief Information Officer

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: Microsoft 365 (M365)	
Date CISD received PIA for review: June 6, 2025	**Date CISD completed PIA review:** July 10, 2025
Action Items/Concerns: M365 is not designed for direct data collection from individuals, it is a platform for storing and managing data. If any information is collected, it would be the source system's responsibility to submit a PIA for any data collection in order to determine if a SORN is required.	