U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our Privacy Office Support Request Page. For further guidance, consult the DOI PIA Guide.

System Information

System or Project Name:	Microsoft Office 365 Cloud
System or Project Acronym:	O365
Date submitted for review:	April 20, 2026
System Operational Status:	Operational

Point of Contact

Name:	Dianna Taylor
Title:	Privacy Officer
Office:	OCIO
Phone:	703-878-1763
E-mail:	DOI_Privacy@ios.doi.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

☐ New System
☐ New Electronic Collection
☒ Significant Modification
☐ Other: Describe below

Microsoft Office 365 Cloud remains an operational Department-wide enterprise cloud environment. This PIA is being updated to reflect significant modification through the implementation and Department-wide availability of additional Microsoft generative AI capabilities, including Microsoft Copilot and Microsoft Copilot Studio, and to align the privacy analysis to the current DOI PIA format.

2. What is the purpose of the system or project?

Microsoft Office 365 Cloud is a Department-wide enterprise cloud service environment that supports official communication, collaboration, productivity, storage, identity-linked access, and related business operations across DOI. The environment provides enterprise email, calendar, document storage, collaboration sites, chat, meetings, forms, browser-based Office functions, and other Microsoft 365 capabilities used by authorized DOI

personnel to perform official duties.

Microsoft Copilot and Microsoft Copilot Studio operate within this broader Microsoft 365 environment as approved generative AI capabilities. Copilot in Word, Excel, PowerPoint, Teams, Outlook, and other Microsoft 365 applications uses the same Microsoft 365 Copilot service foundation, but each in-app experience operates in the context of the specific Microsoft application and its native functions rather than acting only as a pass-through to a standalone chat interface. In this way, the approved Copilot capabilities operate as service capabilities within the Microsoft Office 365 Cloud environment and are addressed through this PIA at the platform and service boundary level.

3. Is the system registered in BisonGRC?

☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

Microsoft Office 365 Cloud is registered in BisonGRC as DOI's enterprise Microsoft cloud environment. Enter the current UII code and system name exactly as listed in BisonGRC for the authoritative system record.

4. What legal authorities authorize the collection and use of data in this system or project?

The following authorities support the collection and use of data in Microsoft Office 365 Cloud:

- **5 U.S.C. § 301, Departmental Regulations.** Supports DOI's general authority to manage internal operations and records in carrying out official business. The 2020 PIA cited this authority for the enterprise Microsoft cloud environment.
- **44 U.S.C. Chapter 35, Paperwork Reduction Act.** Applies where O365 capabilities, such as Forms and related services, are used to support information collection activities subject to OMB review. The 2020 PIA cited the PRA as part of the legal authority set for O365.
- **40 U.S.C. § 11312 and related Clinger-Cohen Act authorities.** Support DOI's management of information technology and enterprise systems. The 2020 PIA cited the Clinger-Cohen Act as a basis for O365 operations.
- **44 U.S.C. §§ 3551–3558, Federal Information Security Modernization Act (FISMA).** Requires risk-based security protections for Federal information and systems, including enterprise cloud services and associated user data. The 2020 PIA expressly relied on FISMA for O365.
- **OMB Circular A-130, Managing Information as a Strategic Resource.** Requires lifecycle management of information resources, including privacy and security risk management for identifiable information and cloud services. The 2020 PIA cited A-130 for O365.
- **Privacy Act of 1974, 5 U.S.C. § 552a.** Applies where records about individuals are maintained and retrieved by personal identifier under applicable DOI systems of records or where platform-level records are covered by an existing SORN.
- **E-Government Act of 2002, Section 208, 44 U.S.C. § 3501 note.** Requires agencies to assess privacy risks when developing or procuring IT that collects, maintains, or disseminates information in identifiable form.
- **Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service"; Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011; and Presidential Memorandum, "Building a 21st Century Digital Government,"**

May 23, 2012. These authorities were cited in the 2020 PIA and continue to support DOI's enterprise cloud computing posture.

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: If yes, list the applicable citations below.
☐ No

For the platform access and logical-account portion of Microsoft Office 365 Cloud, INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) is the relevant existing SORN because it covers individuals who require access to DOI networks, information systems, and email services, and includes records such as login names, work email addresses, access and permission rights, and authentication-related data. INTERIOR/DOI-45, Personnel Security Program Files may also be relevant to the personnel security and vetting basis for granting ongoing access, but it is not the primary SORN for logical-access records.

This platform-level determination applies to Microsoft Office 365 Cloud and the approved Microsoft generative AI capabilities operating within that shared enterprise service boundary, including the associated account, access, logging, retention, and administrative service structure. It does not resolve SORN coverage for downstream business uses, separate AI-enabled activities, or higher-risk use cases. Each approved downstream use case remains subject to separate review before operational use to determine whether an existing SORN is sufficient or whether a new or modified SORN or other required public notice is needed.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

☐ Yes
☒ No

Microsoft Office 365 Cloud is an enterprise productivity and collaboration environment and is not, at the platform level, a standardized collection of information from ten or more members of the public in a 12-month period. Specific uses of Microsoft Forms or other capabilities may require separate PRA evaluation depending on the collection activity.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

The following Microsoft Office 365 Cloud applications and service capabilities are covered under this PIA:

- **Outlook** – enterprise email and calendar services used for official communication and scheduling.
- **SharePoint Online** – collaborative sites, document libraries, and team content repositories.
- **OneDrive for Business** – cloud-based storage for documents and files created, stored, and shared by authorized users.
- **Microsoft Teams** – chat, meetings, collaboration, calling, file sharing, recordings, and integrated teamwork functions.
- **Office Online / Microsoft 365 web apps** – browser-based Word, Excel, PowerPoint, OneNote, and related document collaboration functions.
- **Microsoft Forms** – web-based forms, surveys, quizzes, and polls.

- **Microsoft Copilot** – approved Microsoft generative AI capability operating within the Microsoft 365 environment, including in-app Copilot experiences in Word, Excel, PowerPoint, Teams, Outlook, and related Microsoft 365 applications.
- **Microsoft Copilot Studio** – approved Microsoft generative AI capability used to configure and manage approved agent, workflow, and conversational experiences within the Microsoft enterprise service environment.

These applications and service capabilities operate within the Microsoft Office 365 Cloud enterprise service boundary and administrative structure covered by this PIA. Additional Microsoft 365 capabilities may be incorporated after DOI completes the required privacy, security, records, acquisition, and AI governance review and determines whether this PIA must be updated.

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

☒ Name (full, first or last)
☒ Aliases/nickname
☒ Driver's license
☒ Citizenship
☒ Legal Status
☒ Sex
☒ Race or ethnicity
☒ Date of birth
☒ Place of birth
☒ Personal cell phone number
☒ Username / user ID / acct ID
☒ Geolocation / GPS / location
☒ Tribal or other ID number
☒ Criminal / disciplinary info
☒ Home telephone number
☒ Personal Email
☒ Mailing or home address
☒ Religious preference
☒ Mother's maiden name
☒ Marital status
☒ Spouse Information
☒ Child or family information
☒ Emergency contact info
☒ Financial information
☒ IP address / network ID
☒ Photos / video / audio
☒ Education information
☒ Military records
☒ Employment or resume info
☒ Full or Truncated SSN
☒ Physical characteristics
☒ Biometrics/facial recognition
☒ Vehicle information
☒ Passport information
☒ Travel information
☒ Parent's name
☒ Credit card number
☒ Nationality
☒ Device ID / online ID
☒ Health / medical information
☒ Disability Information
☒ Other: Describe below

Other: Work email address, work phone number, work address, title, organizational information, authentication-related identifiers, access tokens or session-linked identifiers, prompt content, uploaded files, interaction history, response history, recordings, administrative metadata, usage logs, and generated outputs where those data elements are linked to an identifiable user or contain information about identifiable individuals.

All listed categories of PII could potentially be included by authorized users of the Microsoft Office 365 Cloud environment depending on the business purpose, the specific Microsoft 365 service used, and the data uploaded, transmitted, stored, or created within the environment. At the enterprise platform level, the environment contains workforce-linked information such as usernames, work email addresses, work phone numbers, work addresses, titles, and related organizational information required for access, authentication, administration, and enterprise collaboration. Outlook may contain contact and correspondence information; SharePoint Online and OneDrive for Business may contain documents, reports, correspondence, forms, contracts, permits, meeting materials, and other records that include PII; Teams may include meeting content, chats, recordings, and participant information; Forms may collect a variety of PII depending on the purpose of

the form; and Copilot/Copilot Studio may process prompts, uploads, histories, outputs, and related metadata within the approved enterprise service boundary.

2. What is the source for the PII collected? Check all that apply.

☒ Individual
☐ Federal Agency
☐ Tribal Agency
☐ Local Agency
☐ DOI Records
☐ Third Party Records
☐ State Agency
☒ Other: *Describe Below*

Other: DOI enterprise identity and access management services, DOI records and content stored or shared in the environment, external correspondents and collaborating entities in the course of official business, provider-generated service metadata, administrative logs, and AI-generated outputs tied to an identifiable user.

Sources of PII include DOI employees, contractors, volunteers, and other authorized users who create, send, upload, store, share, or manage information in the Microsoft Office 365 Cloud environment; DOI enterprise identity and access management services used to provision and authenticate accounts; DOI records migrated from earlier services or added through ongoing business use; and information received from external correspondents or entities in the course of official business..

3. How will the information be collected? Check all that apply.

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Website
☐ Fax
☐ Telephone Interview
☒ Shared Between Systems: *Describe*
☒ Other: *Describe*

Information is collected through enterprise authentication and account provisioning, email and calendar use, user-entered content, uploaded files, shared documents, SharePoint collaboration, Teams chat and meeting functions, Forms submissions, synchronized directories, prompts and uploads in approved Copilot capabilities, and exchanges between Microsoft Office 365 Cloud and supporting DOI or provider-hosted services.

4. What is the intended use of the PII collected?

PII is used to provision and manage access, authenticate and authorize users, deliver enterprise communication and collaboration services, support email, calendar, document storage, sharing, meeting support, and related official business functions, administer the system, and maintain security and oversight of the environment. At the local and program level, PII may also be used in documents, correspondence, forms, chats, meeting materials, prompts, outputs, or other records created and maintained by authorized users in support of DOI missions. Copilot-related PII is used only within the approved enterprise capability to support user-specific AI functionality, logging, administration, and approved low-risk productivity support.

5. How does this project limit the collection and use of PII to only what is necessary?

Microsoft Office 365 Cloud is a controlled enterprise service for authorized DOI users and collects and uses the information necessary to provision access, operate the service, maintain security, and support authorized communication, collaboration, and productivity uses. DOI limits collection and use through access controls, user

authentication, least privilege, enterprise administration, rules of behavior, training, data loss prevention controls, approved-use limitations, and local program responsibility for ensuring that mission-specific uses meet privacy, records, and security requirements. Use of Copilot and Copilot Studio is further limited through human oversight, role-based access, platform restrictions, and separate review for higher-risk downstream uses.

Section 3: Data Sharing and Individual Rights

1. With whom will the PII be shared, both within DOI and outside DOI? Check all that apply.

☒ **Within the Bureau/Office:** Describe how the data will be used below.
☒ **Tribal, State or Local Agencies:** Describe how the data will be used below.
☒ **Other Bureaus/Offices:** Describe how the data will be used below.
☒ **Contractor:** Describe how the data will be used below.
☒ **Other Federal Agencies:** Describe the federal agency and how the data will be used
☒ **Other Third-Party Sources:** Describe how the data will be used below.

Within DOI, PII may be shared with authorized users, administrators, security personnel, records personnel, Privacy Office personnel, and program or technical officials with a need to know for official communication, collaboration, access management, security monitoring, troubleshooting, compliance review, incident response, and approved operational support. Across DOI bureaus and offices, data may be shared through the enterprise collaboration environment to support official business.

Outside DOI, data may be shared with other Federal, Tribal, state, or local agencies, contractors, or other third parties as necessary to meet legal or mission requirements or in the course of authorized official business. Microsoft, as the cloud service provider, operates the environment under contractual controls. Approved Copilot and Copilot Studio processing may involve provider-hosted handling of prompts, uploads, outputs, logs, and related metadata within the authorized Microsoft enterprise service environment.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

☐ Yes
☒ No

At the platform level, Microsoft Office 365 Cloud is not established primarily through interagency information-sharing agreements. Sharing that occurs in the course of official business is governed by DOI mission authorities, contracts, policies, applicable SORNs, and any program-specific agreements required for particular sharing activities.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent*

to specific uses.
☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Each authorized DOI user voluntarily requests access to DOI computing resources and consents to applicable rules of behavior and system notices before being granted access. Workforce account and contact information required to create and maintain Microsoft Office 365 Cloud accounts cannot be withheld if the individual seeks access to DOI network and computing resources necessary for official duties. For other information in the environment, individuals may limit the information they voluntarily add, store, or share, although some business uses are driven by official duties and program requirements.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

☐ Privacy Act Statement:
☒ Privacy Notice:
☒ Other: *Describe Below*
☐ None: *Example - law enforcement cases.*

Notice is provided through publication of this PIA, system banners and login notices, rules of behavior, user guidance, training, and other DOI notices presented when users access DOI systems and equipment. Additional notice for specific forms, public-facing collections, or mission-specific uses is the responsibility of the program office conducting that activity.

5. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Records may be retrieved by name, email address, username, account identifier, directory entry, document metadata, keyword, meeting or chat information, calendar attributes, prompt history, and other content or administrative identifiers depending on the Microsoft 365 service. Outlook supports retrieval by sender, subject, date, attachment status, and message text; calendar information may be searched by name and event content; OneDrive and SharePoint support keyword and metadata searching; Teams and related collaboration services support contact and content searching; and platform-level administrative and audit records may be retrieved by user-linked identifiers.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

☒ Yes: Describe the use of these reports and who will have access to them.
☐ No

Administrative, audit, eDiscovery, and other service-level records may be produced in limited circumstances, including where records are responsive to legal process, oversight activity, or administrative need. Access to such reports is limited to authorized administrators, security personnel, support personnel, auditors, records officials, legal officials, and others with an official need to know. The purpose of these reports is to administer the service, monitor compliance, support incident response, investigate anomalies, ensure authorized use, and respond to legal or records obligations.

7. How will data collected from sources other than DOI records be verified for accuracy?

Because Microsoft Office 365 Cloud is a communication and collaboration environment, accuracy is generally supported at the point of creation, submission, or business use by the responsible user, program office, or system administrator, depending on the data type. Enterprise identity and access management processes support the accuracy of account and access information, while users and program offices are responsible for the relevance and accuracy of content they create, upload, maintain, or rely on in the environment. Copilot-generated outputs are not treated as inherently authoritative and must be reviewed and validated by the user before use in official work.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

Retention varies depending on the type of record and the program purpose. Administrative and access-related records for the Microsoft Office 365 Cloud environment are maintained under applicable DOI and NARA-approved schedules governing information technology system maintenance, system planning, and system-use records. Program records, emails, documents, SharePoint content, Teams content, Forms data, and other business records created or stored in the environment are retained and disposed of under the applicable Departmental or bureau/office records schedule or General Records Schedule approved by NARA for the relevant record category. Because Microsoft Office 365 Cloud is an enterprise platform, multiple records schedules may apply depending on the content and business use. Copilot-related prompts, outputs, logs, and related administrative records are retained in accordance with the applicable enterprise retention configuration, approved records schedules, and any receiving system's retention where content is incorporated into an official business record.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

Accuracy and completeness are supported through user review, administrative review, identity and access controls, program-level controls, and verification at the point of use. For external communications or uploaded records, the responsible office or user must verify the information for relevance and accuracy before relying on it for official purposes. For AI-generated outputs, users must validate relevance, completeness, and accuracy before use in official work.

3. Does the project include logging capabilities to record and monitor access to PII?

☒ Yes
☐ No

Microsoft Office 365 Cloud includes logging and monitoring capabilities appropriate to the enterprise service boundary. Administrative actions, user access, security-related events, and other activity can be logged and reviewed by authorized personnel for administration, auditing, troubleshooting, incident response, eDiscovery, records management, and security oversight.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

Collection risks: Users may upload, transmit, or store more PII than necessary in Outlook, OneDrive, SharePoint, Teams, Forms, or approved Copilot capabilities. This risk is mitigated through rules of behavior, training, DLP controls, role-based access, enterprise administration, approved-use limitations, and local program responsibility.

Use risks: Authorized users may use or share information beyond official need-to-know, set permissions too broadly, or over-rely on generated content. This risk is mitigated through authentication, least privilege, access controls, audit logging, monitoring, human review, rules of behavior, and annual privacy, security, and records training.

Retention risks: Information may be retained longer than necessary or under the wrong schedule. This risk is mitigated through approved records schedules, records-management responsibilities, enterprise oversight, retention controls, and annual records training.

Disclosure risks: Information may be exposed to unauthorized users, over-shared inside the environment, disclosed through external communications, recorded meetings, guest access, or provider-hosted processing. This risk is mitigated through access controls, meeting controls, authentication, encrypted cloud services, audit logging, DLP, secured cloud architecture, FedRAMP oversight, and user training.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

☒ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
☐ No

Approved Copilot capabilities may generate summaries, draft language, extracted themes, reorganized content, workflow-support content, or other generated output based on user prompts, connected content, retrieved context, uploaded materials, or configured functions. At the foundational platform level, these outputs are intended for low-risk administrative support and are not approved for autonomous decision-making or direct reliance in decisions affecting individual rights, benefits, eligibility, access, investigations, enforcement, or personnel actions. The privacy risk is that generated content may be inaccurate, biased, privacy-sensitive, or improperly reused. These risks are mitigated through human review, use limitations, training, and separate review for higher-risk downstream uses.

3. Will the new data be placed in the individual's record?

☒ Yes: *Provide explanation below*
☐ No

New information created in Microsoft Office 365 Cloud may be incorporated into an individual's record when an authorized user places that content into another DOI recordkeeping system or official business record. At the foundational platform level, Copilot-generated content is not approved through this PIA alone for direct use to create, modify, validate, enrich, finalize, or otherwise update an official record about an individual without appropriate program review and any required downstream privacy or SORN analysis.

4. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Provide explanation below*
☒ No

Microsoft Office 365 Cloud is a communications, storage, collaboration, and productivity environment and is not intended at the platform level to make determinations about individuals. Approved Copilot capabilities are not authorized for autonomous decision-making or direct reliance in decisions affecting individuals.

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

Any new information created or derived within the Microsoft Office 365 Cloud environment is verified for relevance and accuracy by DOI officials at the time it is collected, created, used, or incorporated into official work, and only for authorized purposes. AI-generated outputs must be reviewed by authorized users for relevance, accuracy, completeness, context, and appropriateness before use in official work.

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

☒ Yes
☐ No, *Proceed to Section 7.*

2. How are models validated for fairness, accuracy, and transparency?

At the foundational platform level, DOI does not train or fine-tune the underlying Microsoft foundation model. DOI validates the use of the service through governance, approved-use limitations, provider and implementation review, user guidance, training, and human oversight of outputs. Users are informed that outputs may be inaccurate, incomplete, biased, or otherwise unsuitable for direct reliance without human review.

3. Are individuals notified of AI-based decisions that affect them?

☒ Yes
☐ No

At the foundational platform level, Microsoft Copilot and Copilot Studio are not approved for autonomous decision-making or direct reliance in decisions affecting individuals' rights, benefits, eligibility, access, investigations, enforcement, or personnel actions. Human review is required before outputs are used in official work, and downstream higher-risk uses remain subject to separate review.

4. Are safeguards in place to prevent bias or unintended consequences?

☒ Yes
☐ No

Safeguards include human review requirements, role-based training, approved-use limitations, restrictions on decision-making uses, logging and monitoring, incident reporting processes, and separate review for higher-risk downstream AI uses. These safeguards reduce the risk of inappropriate reliance on generated content.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

☐ Yes
☒ No

Not by DOI at the foundational platform level. Microsoft provides the underlying AI service, and DOI does not itself retrain the foundation model for the enterprise implementation. DOI reviews provider and configuration changes, approved-use limitations, and changing privacy risks, and updates the PIA when material changes occur.

6. Is federated learning used for privacy-preserving model training?

☒ Yes
☐ No

Federated learning is not used by DOI as part of the approved enterprise Microsoft Office 365 Cloud generative AI posture.

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe below*

Access is limited to authorized DOI workforce users, system administrators, approved contractor support personnel, and other authorized officials with a need to know based on role and function. Access is determined through DOI identity and access management processes, role-based access controls, least privilege, administrative approval, and periodic review. Different categories of users receive different levels of access depending on whether they are end users, administrators, security officials, auditors, or support personnel.

2. What data protection policies apply to cloud-based PII storage?

Cloud-based PII storage and processing for Microsoft Office 365 Cloud must comply with applicable Federal and DOI requirements, including FedRAMP authorization requirements, FISMA, OMB Circular A-130, NIST SP 800-53 Rev. 5 security and privacy controls, DOI cloud and security policy requirements, DOI privacy guidance, and applicable contractual or licensing provisions governing Microsoft's handling of DOI data. These requirements are implemented through the authorization process, configuration management, access controls, encryption, logging, monitoring, and contractual oversight.

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

The system relies on enterprise logging, audit trails, administrator logs, data loss prevention monitoring, access controls, security event review, and other DOI-approved monitoring capabilities to detect unauthorized access, use, or exfiltration of PII. Logs and monitoring data are reviewed by authorized personnel for administration, security oversight, troubleshooting, incident response, and compliance purposes.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.
☐ No

Microsoft Office 365 Cloud includes monitoring and auditing capabilities necessary to administer the platform, maintain security, investigate anomalies, respond to incidents, support records and eDiscovery obligations, and ensure appropriate use. Controls include role-based access to logs and monitoring data, policy restrictions, need-to-know limitations, administrative oversight, and alignment with DOI privacy and security requirements. The environment is not intended to track individuals for unrelated monitoring purposes.

5. Will contractors be involved in the following project activities? Check all that apply.

☒ Design
☒ Development
☒ Maintenance

Contractors and commercial vendor personnel may support design, configuration, implementation, hosting, maintenance, administration, logging, incident response, troubleshooting, workflow configuration, and other operational functions necessary to provide the approved enterprise capabilities. Such personnel must comply with applicable contractual requirements, DOI privacy and security requirements, background investigation and access requirements where applicable, rules of behavior, and required training.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

☒ Security Guards
☒ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Lock
☒ Other: *Describe Below*

Physical protections are provided through secured DOI and provider facilities, identification badges, facility access restrictions, guards, and related safeguards appropriate to the hosting environment.

Technical Controls

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Other: *Describe Below*

☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

Technical safeguards include passwords, user identification, encryption, firewalls, intrusion detection or related monitoring, VPN and PKI where applicable, PIV-based authentication, audit logging, data loss prevention controls, and other DOI-approved technical protections.

Administrative Controls

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Other: *Describe Below*

☒ Methods to Ensure Only Authorized Personnel Have Access
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Records and Privacy Training
☒ Regular Monitoring of Users' Security Practices

Administrative safeguards include periodic security audits, methods to ensure only authorized personnel have access, secured backups as applicable, rules of behavior, mandatory security, privacy, and records training, role-based training, regular monitoring of security practices, enterprise oversight, approved-use limitations for AI capabilities, and incident response procedures.

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

Individuals may submit Privacy Act complaints through the DOI Privacy Office using established Departmental complaint channels, including the Department's privacy website, designated mailing or email addresses, or other official contact methods identified by the Department Privacy Office. Complaints are reviewed, logged, and addressed in accordance with DOI privacy complaint handling procedures and applicable law and policy.

8. What processes are in place for individuals to access their information?

Individuals may request access to records about themselves, where applicable, through the Privacy Act and/or Freedom of Information Act process in accordance with DOI procedures and any applicable SORN. Requests must include sufficient identifying information to locate the records and verify the requester's identity before disclosure.

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may request correction or amendment of records about themselves, where applicable, under the Privacy Act in accordance with DOI procedures and any applicable SORN. Requests must provide sufficient information to identify the record and verify identity. Amendment requests are reviewed by the office responsible and handled consistent with DOI Privacy Act requirements.

10. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

Responsibility is shared among the Information System Owner, the Information System Security Officer, system administrators, authorized support personnel, contractor personnel within their assigned roles, and the Department Privacy Office. These officials are responsible for ensuring proper use of data within the approved service boundary, enforcing access restrictions, monitoring compliance, and promptly reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy-protected information through DOI incident reporting channels, including DOI-CIRC, in accordance with DOI policy.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

In the event of a privacy breach involving Microsoft Office 365 Cloud, DOI will follow its established incident and breach response procedures. Response actions include containment, assessment of the nature and scope of the incident, preservation and review of relevant logs and records, coordination with DOI-CIRC, notification to the Department Privacy Office, risk-of-harm analysis, mitigation steps to reduce further exposure, and notification to affected individuals and oversight entities where required by law, policy, or breach response procedures.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

This PIA will be reviewed at least annually as part of DOI system oversight, FISMA reporting, BisonGRC updates, system reauthorization, or other periodic review processes, and it will be updated whenever significant changes occur to the Microsoft Office 365 Cloud environment, including technology changes, data practices, provider relationships, approved service capabilities, AI capability changes, user populations, or privacy risk posture.