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:	OCIO Azure Hosting
System or Project Acronym:	OAH
Date submitted for review:	March 13, 2026
System Operational Status:	Operational

Point of Contact

Name:	Dianna Taylor
Title:	Associate Privacy Officer
Office:	Office of the Chief Information Officer
Phone:	703-787-1763
E-mail:	dianna_taylor@ios.doi.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

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

This PIA is being updated to align with the current Department of the Interior (DOI) Privacy Impact Assessment (PIA) template and guidance. A review of the OAH environment confirmed that there have been no significant changes to system functionality, the categories of personally identifiable information (PII) processed within the hosting environment, or the way OAH performs its authorized technical processing functions since approval of the previous PIA.

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

The OCIO Azure Hosting (OAH) system is a cloud-based infrastructure service managed by the Department of the Interior (DOI), Office of the Chief Information Officer (OCIO), and hosted within the DOI Azure environment with support from the OCIO Enterprise Service Delivery Division. OAH provides secure, scalable cloud hosting services

to the OCIO Shared Services Center (SSC), which delivers business management support services to DOI bureaus and external federal agencies.

OAH provides and administers the cloud hosting infrastructure within its authorization boundary and is responsible for the secure operation, administration, monitoring, maintenance, backup, and protection of that environment. In performing these functions, OAH may store, transmit, safeguard, back up, monitor, log, and permit authorized administrative access to hosted mission system data, including records containing personally identifiable information (PII), as necessary to support hosting services, cybersecurity, auditing, incident response, continuity of operations, and other infrastructure support functions.

OAH also collects, maintains, and uses limited platform-level PII and user-linked technical identifiers necessary to authenticate authorized users, manage privileged access, administer the hosting environment, maintain audit logs, and support security operations. This platform-level PII is addressed in this PIA.

OAH does not determine the mission purpose, legal authority, or authorized business use of records maintained within hosted mission applications. Responsibility for the collection, use, maintenance, disclosure, Privacy Act compliance, System of Records Notice (SORN) coverage, Privacy Act Statements, Paperwork Reduction Act (PRA) requirements, records retention, and procedures for individual access and amendment remains with the respective mission system owner, information owner, or Privacy Act System Manager.

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.

The OCIO Azure Hosting (OAH) system is registered in BisonGRC under UII code **010-000002507**. The system record includes current security categorization and supports the Authorization and Assessment (A&A) process in accordance with DOI requirements.

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

The Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) operates as the Department of the Interior's (DOI) cloud hosting platform and collects, maintains, uses, and generates limited platform-level personally identifiable information (PII) and user-linked technical information necessary to administer, secure, and operate the hosting environment. This includes identity, credential, authentication, account management, privileged-access, logical-access, audit, monitoring, and other user-linked technical records associated with authorized users and administrators. The following authorities govern OAH's collection, maintenance, use, and protection of platform-level PII:

- **Privacy Act of 1974, 5 U.S.C. § 552a** – Establishes requirements for the collection, maintenance, use, and dissemination of PII in federal systems of records. This applies to systems hosted within OAH that may retrieve records by personal identifier.
- **E-Government Act of 2002, Section 208** – Requires agencies to conduct Privacy Impact Assessments (PIAs) for systems that collect, maintain, or disseminate PII. This applies to systems hosted within OAH. OMB Circular A-130, Managing Information as a Strategic Resource – Establishes federal policy for information governance, including privacy and security requirements for federal information systems. This applies to OAH as a DOI-operated cloud hosting environment.

- **44 U.S.C. § 3551 et seq., Federal Information Security Modernization Act (FISMA) of 2014 –** Requires federal agencies to develop, document, and implement programs to secure federal information systems. This applies to OAH as the infrastructure supporting systems that process PII.
- **Department of the Interior Manual, 383 DM 1–13, Privacy Act Policy and Responsibilities** – Establishes DOI-specific privacy policy requirements for managing PII. This applies to systems hosted within OAH and their respective system owners.
- **5 U.S.C. § 301, Departmental Regulations** – Authorizes federal agencies to establish regulations for the governance of their operations, including management of information systems such as OAH.
- **44 U.S.C. Chapter 35, Paperwork Reduction Act (PRA)** – Governs the collection of information from the public. This applies to systems hosted within OAH that may collect information from individuals and require OMB approval.
- **40 U.S.C. § 1401, Clinger-Cohen Act of 1996** – Establishes requirements for federal agencies to use information technology to improve mission performance. This applies to OAH as part of DOI's enterprise IT infrastructure supporting mission operations.

In addition to maintaining platform-level information, OAH provides the infrastructure within which hosted mission systems may collect, maintain, process, transmit, store, and dispose of mission-related PII. Responsibility for identifying the legal authorities supporting the collection, maintenance, use, disclosure, and retention of mission-related information including applicable Privacy Act requirements, System of Records Notice (SORN) coverage, Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), Paperwork Reduction Act (PRA) requirements, and other mission-specific privacy obligations remains with the respective mission system owner, information owner, or Privacy Act System Manager.

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

OCIO Azure Hosting (OAH) maintains limited platform-level personally identifiable information (PII) and user-linked technical records necessary to operate and secure the hosting environment. These records include identity, credential, authentication, account-management, logical-access, privileged-access, and related user activity information associated with authorized users and administrators.

PII maintained as part of the OAH hosting boundary is governed, as applicable, by:

- INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007), as modified at 86 FR 50156 (September 7, 2021); and
- GSA/GOVT-7, HSPD-12 US Access, 80 FR 64416 (October 23, 2015).

These SORNs apply to identity, credential, authentication, logical-access, account-management, and related records maintained to authorize, manage, monitor, and document access to DOI systems and resources.

OAH also provides the authorized infrastructure boundary in which DOI bureaus, offices, and other federal agency may develop, host, or operate mission applications. Records created, collected, maintained, used, or retrieved by those mission applications are not governed solely by the OAH platform SORNs. Each mission application or system owner remains responsible for identifying and documenting the SORN or SORNs applicable to its mission records, based on the purpose of the collection, the categories of individuals and records involved,

and whether the records are retrieved by a personal identifier.
Accordingly:

- Platform-level identity, credential, access, account, and related administrative records maintained within the OAH boundary are governed by INTERIOR/DOI-47 and GSA/GOVT-7, as applicable.
- Mission records maintained by applications operating within the OAH boundary are governed by the applicable System of Records Notice (SORN) or SORNs identified by the responsible DOI bureau, office, or other authorized Federal agency.
- Hosting a mission application within OAH does not transfer responsibility for the application's Privacy Act compliance, SORN coverage, notice, access, amendment, disclosure, or records-management obligations to OAH.

Each hosted mission system must maintain its own approved PTA and PIA, as applicable, and must document the SORN or SORNs that govern its records.

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

☐ Yes
☒ No

The OCIO Azure Hosting (OAH) system does not directly collect information from members of the public and therefore does not require OMB approval under the Paperwork Reduction Act. OAH functions as the Department's cloud hosting platform and does not collect information from members of the public. Any information collection conducted by applications or systems hosted within OAH are the responsibility of the respective system owners, who are responsible for obtaining OMB approval if required.

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

The OCIO Azure Hosting (OAH) system does not include minor applications or subsystems under this PIA. OAH functions as a cloud hosting platform, and applications or systems hosted within the environment are separately managed by their respective system owners and are covered under their own PTAs and PIAs, as applicable.

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)	☐ Home telephone number	☐ Employment or resume info
☐ Aliases/nickname	☐ Personal Email	☐ Full or Truncated SSN
☐ Driver's license	☐ Mailing or home address	☐ Physical characteristics
☐ Citizenship	☐ Religious preference	☐ Biometrics or facial recognition
☐ Legal Status	☐ Mother's maiden name	☐ Vehicle information
☐ Sex	☐ Marital status	☐ Passport information
☐ Race or ethnicity	☐ Spouse Information	☐ Travel information
☐ Date of birth	☐ Child or family information	☐ Parent's name
☐ Place of birth	☐ Emergency contact info	☐ Credit card number

☐ Personal cell phone number ☐ Financial information ☐ Nationality
☐ Tribal or other ID number ☐ Education information ☐ Disability Information
☐ Military records ☒ Other: Describe below

The OCIO Azure Hosting (OAH) system processes limited platform-level personally identifiable information (PII) necessary to administer, secure, and operate the hosting environment. The categories of PII maintained within the OAH authorization boundary include:

- **Full Name** – Used to identify authorized users and associate individuals with administrative or privileged accounts.
- **Work Email Address** – Used to support account administration, communications, and identity management.
- **Username/User ID/Account Identifier** – Used for authentication, access control, account management, and audit logging.
- **Agency or Organization** – Used to identify the employing DOI bureau, office, or other authorized Federal agency associated with an authorized account.
- **Assigned Role and Privilege Information** – Used to administer role-based access, privileged account management, and authorization decisions.
- **Authentication and Access Information** – Includes account status, authentication events, multi-factor authentication (MFA) associations, and logical access records necessary to verify authorized access.
- **Audit Logs and User Activity** – Includes login activity, successful and failed authentication attempts, date and time of access, account activity, administrative actions, and other audit records used for security monitoring, incident response, and compliance.
- **Network and Device Information –** Includes Internet Protocol (IP) addresses, device identifiers, system-generated identifiers, and other user-linked technical metadata associated with authorized access and system administration.

OAH provides cloud hosting services to internal Department of the Interior (DOI) bureaus and offices, as well as other authorized Federal agencies. As part of providing those services, OAH may store, transmit, back up, safeguard, monitor, log, and permit authorized administrative access to mission-related data hosted within the OAH environment, including records containing personally identifiable information (PII), as necessary to support hosting operations, cybersecurity, auditing, incident response, continuity of operations, and other infrastructure support.

Applications hosted within OAH may collect, maintain, process, use, disclose, retain, or dispose of additional categories of PII based on their respective missions, legal authorities, and operational requirements. Responsibility for identifying those categories of PII, documenting applicable legal authorities, Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), records schedules, Privacy Act compliance, and other privacy requirements remain with the respective mission system owner, information owner, or Privacy Act System Manager.

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

☒ Individual ☒ DOI Records
☒ Federal Agency ☐ Third Party Records
☐ Tribal Agency ☐ State Agency

☐ Local Agency ☒ Other: *Describe Below*

OAH collects limited platform-level personally identifiable information (PII) necessary to administer, secure, and operate the hosting environment. The sources of this PII include:

- **Individuals** – Authorized Department of the Interior (DOI) personnel and authorized users from supported Federal agencies provide identity and account information during account provisioning, privileged access requests, and account management activities.
- **DOI Records** – Identity and account information is obtained from DOI enterprise identity and access management services, including DOI Access, Active Directory, and other authorized DOI administrative records used to authenticate users and manage logical access.
- **Federal Agencies** – Supported Federal agencies provide identity and account information for authorized personnel requiring access to hosted mission system resources within the OAH environment.
- **Other** – Additional identity and account information may be provided through supervisors, Contracting Officer's Representatives (CORs), and Information Technology Service Management (ITSM) processes (e.g., Remedy) used to create, modify, approve, and manage user, administrative, and privileged accounts. Platform-generated records, including authentication events, audit logs, login activity, Internet Protocol (IP) addresses, device information, and other user-linked technical metadata, are generated through the operation, administration, security monitoring, and maintenance of the OAH hosting environment.

OAH also provides the infrastructure within which hosted applications may collect, maintain, process, transmit, store, or dispose of PII from sources necessary to support their respective missions. Responsibility for identifying the sources of mission data and documenting those sources in the applicable Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), System of Records Notice (SORN), records schedule, and legal authorities remains with the respective mission system owner, information owner, or Privacy Act System Manager.

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

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

Information Shared Between Systems

For system administration, elevated privileged accounts supporting infrastructure-level systems within OAH that do not directly integrate with DOI Active Directory (AD) are established through account request forms submitted through the DOI Information Technology (IT) Service Management (ITSM) workflow system (Remedy). OAH also receives identity and account information through system-to-system exchanges with DOI enterprise identity and access management services, including DOI Access and Active Directory, to support authentication, logical access, and account management. Administrator input is used, as necessary, to provision, modify, and manage authorized user accounts and privileges. Information received through these processes is handled as Controlled Unclassified Information (CUI) in accordance with the OS/OCIO/IBC IBCM-CIO-6300-003, Information Classification and Handling Policy.

Other

OAH also generates platform-level personally identifiable information (PII) and user-linked technical records

through normal system operations. These records include authentication events, login activity, automatically generated audit logs, system monitoring records, Security Information and Event Management (SIEM) feeds, Internet Protocol (IP) addresses, device information, and other technical metadata associated with authorized access and administration of the OAH environment. These records are used to support cybersecurity, continuous monitoring, auditing, incident response, and operational oversight.

Mission applications hosted within OAH determine their own methods for collecting mission-related PII based on their operational requirements and legal authorities. Each mission system owner is responsible for documenting those collection methods, providing any required Privacy Act Statements or privacy notices, and identifying applicable collection authorities in the system's Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), System of Records Notice (SORN), records schedule, and other required privacy documentation.

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

OAH uses platform-level personally identifiable information (PII) for the following purposes:

- **Account Validation and Authentication** – Employee username/user identification (ID), work email address, and full name are used to validate user identities, authenticate authorized users, and support logical access to infrastructure-level systems. Identity information is maintained in coordination with DOI enterprise identity and access management and directory services.
- **Administrative and Privileged Account Management** – Platform-level PII is used to provision, manage, modify, monitor, suspend, and deactivate administrative and privileged accounts; assign roles and privileges; and support account lifecycle management.
- **Security Operations, Monitoring, and Auditing** – Authentication records, audit logs, login activity, Internet Protocol (IP) addresses, device information, and other user-linked technical metadata are used to support cybersecurity operations, continuous monitoring, auditing, incident detection and response, forensic investigations, and compliance with Federal security requirements.
- **Hosting Environment Administration** – OAH uses platform-level PII to administer, secure, monitor, maintain, back up, and protect the hosting environment and to provide operational support for systems operating within the OAH authorization boundary.

As the Department's cloud hosting provider, OAH may store, transmit, back up, safeguard, monitor, log, and permit authorized administrative access to mission-related data hosted within the OAH environment, including records containing personally identifiable information (PII), as necessary to provide hosting services, cybersecurity, continuity of operations, auditing, incident response, and infrastructure support. While OAH performs these technical processing functions within its authorization boundary, it does not determine the purpose of mission, authorized business use, or legal authority governing the records maintained by hosted mission systems.

Responsibility for determining the purpose of collection, legal authority, mission use, disclosure of records, Privacy Act compliance, System of Records Notice (SORN) coverage, Privacy Act Statements, Paperwork Reduction Act (PRA) requirements, records retention, and procedures for individual access and amendment remains with the respective mission system owner, information owner, or Privacy Act System Manager.

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

OAH limits the collection and use of PII to only what is necessary to support authentication and administrative functions at the infrastructure level.

- **Limited PII for Authentication** – OAH limits platform-level PII to information necessary to support identity verification, account administration, privileged access management, user authentication, logical access control, security monitoring, auditing, incident response, and other operational support activities. This generally includes employee names, work email addresses, usernames/user identification (ID), account identifiers, assigned roles and privileges, authentication records, audit logs, Internet Protocol (IP) addresses, device information, and other user-linked technical metadata.
- **Enterprise Identity Management** – Identity information used to administer the hosting environment is obtained through DOI enterprise identity and access management and directory services, reducing the need for OAH to independently collect or maintain additional PII.
- **No Unnecessary Sensitive PII** – OAH does not intentionally collect or maintain sensitive PII, such as Social Security numbers, financial account information, or biometric data, for platform administration unless required to support an authorized capability operating within the hosting environment.
- **Technical Processing Within the Hosting Environment** – As the Department's cloud hosting provider, OAH may store, transmit, back up, safeguard, monitor, log, and permit authorized administrative access to mission-related data hosted within the OAH environment, including records containing personally identifiable information (PII), as necessary to provide hosting services, cybersecurity, continuity of operations, auditing, incident response, and infrastructure support. OAH limits these technical processing activities to those necessary to operate, maintain, and secure the hosting environment.
- **Mission System Responsibilities** – Each hosted mission system is responsible for applying data minimization principles to the mission-related PII it collects, uses, maintains, shares, and retains in accordance with its authorized purpose, applicable legal authorities, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), System of Records Notice (SORN), records schedule, and other applicable privacy requirements.
- **Periodic Review** – OAH periodically reviews platform-level PII collection and processing through privacy compliance activities, including updates to this Privacy Impact Assessment (PIA), to ensure continued alignment with operational requirements and the principle of collecting and maintaining only the minimum information necessary.

Through these measures, OAH ensures that the collection and use of PII is limited to what is directly relevant and necessary to support authentication and administrative functions at the infrastructure level.

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.

OAH shares limited PII with authorized recipients to support system administration, account management, and

security operations.

- **Within the Bureau/Office** – The Office of the Chief Information Officer (OCIO), Enterprise Service Delivery Division, Hosting Services Branch shares platform-level identity and access records, including employee names, work email addresses, usernames/user identification (ID), account identifiers, assigned roles and privileges, privileged account records, authentication records, audit logs, login activity, Internet Protocol (IP) addresses, device information, and other user-linked technical metadata with authorized OCIO personnel to support identity verification, account provisioning and management, privileged access administration, system administration, security monitoring, auditing, incident response, continuity of operations, and implementation of security controls.
- **Other DOI Bureaus/Offices** – Platform-level records may be shared with authorized DOI bureaus and offices to support account management, authentication, cybersecurity operations, auditing, incident response, infrastructure support, and operational coordination. Information may also be shared with the Department of the Interior Computer Incident Response Capability (DOI-CIRC), cybersecurity personnel, the Insider Threat Program, or other authorized Department officials to detect, investigate, respond to, and mitigate cybersecurity incidents, insider threats, or other activities affecting the security of the hosting environment. DOI bureaus and offices may also receive information related to privileged accounts or administrative activities associated with their hosted mission systems when necessary to support operations, security, or incident response
- **Contractors** – Contractor personnel supporting OAH administration are granted role-based access to platform-level records only to the extent necessary to perform authorized hosting, account administration, technical support, maintenance, monitoring, auditing, and cybersecurity functions. Contractor access is governed by applicable contracts, nondisclosure requirements, Federal security controls, and the principle of least privilege.
- **Other Federal Agencies** – Platform-level records may be shared with authorized Federal agencies supported by the OAH environment, as well as partner agencies, to support account administration, authentication, cybersecurity operations, auditing, incident response, continuity of operations, and infrastructure support. Information may also be shared with the Office of Inspector General (OIG), the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), or other authorized Federal entities when necessary to investigate potential violations of law or policy, respond to cybersecurity incidents, mitigate threats, support forensic investigations, or satisfy applicable legal or regulatory requirements.

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

OAH does not have formal MOU, MOA, or ISA agreements specific to the sharing of PII. OAH functions as a cloud hosting platform, and any sharing of information associated with applications and systems hosted within OAH is the responsibility of the respective system owners. Any required agreements governing information sharing are established and maintained by those system owners based on their specific system requirements.

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.*

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.*

Identity and account information required to establish and maintain administrative or privileged access to the Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) environment is collected as a condition of receiving authorized access to perform official duties. Individuals may decline to provide the required information; however, OAH cannot create or maintain the requested administrative or privileged account without the information necessary to verify identity, authenticate the user, and administer authorized access.

Identity information used to support OAH administrative and privileged accounts is obtained through the Department of the Interior (DOI) enterprise identity and access management process, including DOI Access, and, as applicable, through administrative account requests submitted via the Information Technology (IT) Service Management (ITSM) workflow system (Remedy). Identity information is originally collected through DOI Access via the applicable notice process. Users are also presented with the DOI Security Warning Banner when accessing DOI information systems, which advises that system activity is subject to monitoring and that there is no expectation of privacy.

OAH uses this platform-level personally identifiable information (PII) only for identity verification, authentication, account administration, privileged access management, security monitoring, auditing, incident response, and administration of the hosting environment.

Hosted mission systems may collect and use mission-related PII for their authorized business purposes. Responsibility for providing any required Privacy Act Statements or other privacy notices, obtaining consent where required by law, informing individuals how their information will be used, and documenting those practices in the applicable Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), System of Records Notice (SORN), and other required privacy documentation remains with the respective mission system owner, information owner, or Privacy Act System Manager.

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

The Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) retrieves limited platform-level personally identifiable information (PII) necessary to administer and secure the hosting environment. Platform-level records may be retrieved by full name, username, user ID, account identifier, or other user-linked identifiers to support account administration, authentication, privileged access management, security monitoring, auditing, incident response, and other authorized operational activities.

Platform-level information may be retrieved manually by authorized personnel or through automated processes,

including system monitoring, audit logging, reporting, and other security and administrative functions.

Hosted mission systems may retrieve mission-related PII using identifiers and retrieval methods appropriate to each application's authorized business purpose. Retrieval practices for mission records are determined by the respective mission system owner and are governed by the applicable mission-related System of Records Notice (SORN) and associated privacy documentation, including the Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA), as applicable.

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

The system produces reports in the form of audit logs documenting user access and activity within the system.

- **Audit Reports** – The system includes audit logs documenting user access and activity within the system. The audit logs contain details relating to the use of the system, including username, date/time, user's last date of login, failed login attempts, data/reports accessed, and data exported.
- **Access and Purpose** – The audit logs are available to designated DOI personnel responsible for reviewing audit log data for monitoring and oversight of system activity.

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

Data provided to OAH is verified for accuracy through the following processes:

- **Supervisor and COR Validation** – Administrative user information is provided by Supervisors and Contracting Officer Representatives (CORs) who attest to validation of the match to an existing identity in DOI Access (via an existing Active Directory account). If the full name provided is not accurate, the request will not be processed and is returned to the requesting supervisor or COR.
- **Hosted Mission System Responsibilities** – Identity and account information provided by hosted mission systems or other authorized Federal organizations for user account provisioning is presumed to be accurate, complete, and current when submitted. The respective mission system owner is responsible for ensuring the accuracy and completeness of mission-related PII maintained within the hosted system.
- **OAH Administrative Role –** OAH is responsible for administering platform-level identity and access controls, provisioning and managing authorized accounts, and implementing infrastructure security controls necessary to protect the hosting environment. OAH does not determine the accuracy or completeness of mission-related PII maintained within hosted mission systems.
- **Security and Privacy Controls** – Platform-level records and hosted information maintained within the OAH authorization boundary are protected through administrative, technical, and physical safeguards, including identity validation, access controls, audit logging, continuous monitoring, and other security controls designed to protect information from unauthorized access, alteration, or disclosure.

These processes help ensure the integrity of platform-level information maintained by OAH, while responsibility for the accuracy and completeness of mission-related PII remains with the respective mission system owner, information owner, or Privacy Act System Manager.

Section 4: Data Management and Retention

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

OAH retains data in accordance with applicable NARA-approved schedules and DOI records management policies.

- **User Account and Administrative Data** – The retention period for account information varies depending on the hosted system, including account type, operating system, or database, as documented in the Control Implementation Statement for NIST 800-53 controls in the OAH System Security and Privacy Plan. Generally, account information is maintained for the duration of the requirement for the account, and accounts are removed 60–90 days after non-use, termination, or cancellation.
- **General System Records** – The retention schedules are DRS 1.4A(1) DAA-0048-2013-0001-0013, DRS 1.4A(2) DAA-0048-2013-0001-0014, and DRS 1.4B DAA-0048-2013-0001-0015, which are approved by the National Archives and Records Administration (NARA). The dispositions are temporary, and cutoff varies depending on the types of files. Records are destroyed no later than 3 years after cutoff for records covered under DRS 1.4A(1) and DRS 1.4A(2), and no later than 7 years after cutoff for records covered under DRS 1.4B.
- **System Backups** – System backups vary in duration of retention requirement, but generally 90 days of backups are maintained and may contain user account data that could be tied to full name.
- **Privileged Account Request Records** – Request forms for privileged accounts (add, change, or delete) are maintained in accordance with operational and audit requirements to support security, accountability, and compliance.
- **Hosted Mission System Data** – The retention periods for data maintained within systems hosted in the OAH environment vary depending on the hosted mission system and the types of records or data maintained by the responsible DOI bureau, office, or other authorized Federal agency. Hosted mission system owners are responsible for managing and disposing of their records in accordance with applicable National Archives and Records Administration (NARA)-approved records schedules or General Records Schedules (GRS).

If new data elements or categories are introduced that are not covered under existing records schedules, OCIO will coordinate with the appropriate Bureau Records Officer to develop and obtain NARA approval for an updated schedule prior to collection.

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

The OAH applies multiple measures to validate the accuracy and completeness of data received from external sources:

- **Supervisor and COR Attestation** – Administrative user information is provided by Supervisors and Contracting Officer Representatives (CORs) who attest to validation of the user's identity against DOI Access (via an existing Active Directory account). Requests that do not match an existing identity are not processed and are returned for correction.
- **Enterprise Identity Management** – Platform-level identity and account information is obtained through Department of the Interior (DOI) enterprise identity and access management services, including DOI

Access and Active Directory, helping ensure the accuracy and consistency of identity information used to administer the hosting environment.

- **Hosted Mission System Responsibilities** – Hosted mission systems are responsible for validating the accuracy and completeness of mission-related personally identifiable information (PII) collected, maintained, and processed within their applications. Responsibility for ensuring the quality and integrity of mission records remains with the respective mission system owner, information owner, or Privacy Act System Manager.

These measures ensure that externally sourced PII is maintained in accordance with DOI requirements for accuracy and completeness, while responsibility for validating and maintaining data within hosted systems remains with the respective system owners.

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

☒ Yes
☐ No

The system includes logging capabilities to record and monitor user access and activity within the system.

- **Audit Logs** – The system includes audit logs documenting user access and activity, including successful and failed login attempts, date/time of access, user's last login, and actions such as data or reports accessed and data exported.
- **PII-Related Activities Monitored** – Logging captures activities associated with Administrative/Privileged Accounts, including authentication attempts and user activity within the system.
- **Security of Logs** – Auditing is addressed in the OAH System Security and Privacy Plan, with components provided by OAH and the Bison Shield information system. Logging information is maintained at the local system or database level and then forwarded to a centralized Security Information and Event Management (SIEM) system. Access to audit data is controlled through segmentation of system administrators, application of the least privilege principle, and enforcement of the Access Control (AC) family of NIST SP 800-53 controls.
- **Retention** – Audit logs are retained in accordance with applicable NARA-approved records schedules and DOI policies for system and audit records.
- **Review Process** – Audit logs are available to designated DOI personnel responsible for reviewing audit log data for monitoring and oversight of system activity.

These measures support DOI's ability to detect, monitor, and respond to potential unauthorized access or misuse of PII within the system.

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?

The Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) provides the cloud hosting infrastructure that collects, maintains, uses, generates, stores, transmits, protects, monitors, backs up, and supports authorized administrative access to platform-level personally identifiable information (PII), including identity, credential, account, authentication, privileged-access, audit, monitoring, and other user-linked technical

information necessary to administer and secure the hosting environment. OAH also provides the infrastructure within which hosted mission systems may collect, maintain, use, transmit, store, retain, disclose, and dispose of records containing mission-related PII. While OAH is responsible for protecting information processed within its authorization boundary through infrastructure security and operational controls, hosted mission system owners remain responsible for determining the legal authority for collection, the purpose and use of mission-related information, applicable disclosure requirements, records retention, and compliance with applicable privacy requirements. The privacy risks and mitigations associated with OAH's infrastructure-level responsibilities throughout the information lifecycle are described below.

Collection Risks – There is a risk that platform-level account information may be inaccurate, incomplete, or that more personally identifiable information (PII) than necessary could be collected to administer the hosting environment.

- **Mitigation** – OAH limits platform-level PII to the minimum information necessary to establish, authenticate, and manage administrative and privileged accounts. Identity information is validated through the Department of the Interior (DOI) enterprise identity and access management process, including DOI Access, and administrative account requests are verified before access is granted. Access is limited to authorized personnel with a demonstrated business need.

Use Risks – There is a risk of unauthorized access, misuse of PII, excessive privileged access, contractor misuse, configuration errors, or inappropriate use of information while administering the hosting environment.

- **Mitigation** – OAH implements role-based access controls, separation of duties, least privilege, multi-factor authentication, privileged account management, continuous monitoring, centralized Security Information and Event Management (SIEM) logging, audit logging, configuration management, and periodic access reviews. Personnel, including contractors with authorized administrative access, must complete required security, privacy, and Rules of Behavior training before receiving access.

Storage, Transmission, and Backup Risks – There is a risk that records containing PII could be exposed during storage, transmission, backup, restoration, or other infrastructure operations**.**

- **Mitigation –** OAH protects information through encryption, secure network architecture, access controls, backup protections, media safeguards, and other administrative, technical, and physical safeguards consistent with Federal Information Security Modernization Act (FISMA) Moderate and National Institute of Standards and Technology (NIST) security requirements. Backup media and replicated data receive the same security protection as production systems.

Retention and Data Remanence Risks – There is a risk that platform-level records, backups, or residual data may be retained longer than necessary or remain accessible after systems or storage media are retired.

- **Mitigation** – Account information is maintained only for the duration of the account requirement and removed 60–90 days after non-use, termination, or cancellation. Records are managed and disposed of in accordance with NARA-approved records schedules. System backups are retained for limited durations, and lifecycle management processes are in place to address data remanence and ensure proper handling and disposal of data and media in accordance with NIST 800-53 controls.

Disclosure and Breach Risks – There is a risk of unauthorized disclosure of PII resulting from unauthorized

access, security incidents, or data breaches affecting the hosting environment.

- **Mitigation** – OAH implements layered administrative, technical, and physical safeguards, including centralized monitoring, audit logging, incident detection, incident response procedures, and breach reporting processes. Authorized administrative access to hosted information is limited to personnel with a demonstrated business need and only to the extent necessary to administer, maintain, secure, monitor, audit, troubleshoot, or restore the hosting environment. Administrative activities are logged, monitored, and subject to an audit.

Hosted Misson System Responsibilities

Hosted mission systems may collect, maintain, retrieve, use, disclose, retain, and dispose of mission-related personally identifiable information (PII) to support their authorized business purposes. Responsibility for establishing the legal authority for collection, providing Privacy Act Statements or other required notices, obtaining consent where required by law, maintaining applicable System of Records Notice (SORN) coverage, determining records retention requirements, responding to requests for notification, access, amendment, or other rights under the Privacy Act, and completing required Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and other applicable privacy documentation remains with the respective mission system owner, information owner, or Privacy Act System Manager. While OAH provides the secure hosting infrastructure and implements the administrative, technical, and physical safeguards necessary to protect information processed within the authorization boundary, mission system owners remain responsible for the privacy governance and lifecycle management of mission-related information maintained within their applications.

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

OAH does not generate new data or inferences through aggregation or analytics. The system functions as a cloud hosting platform and only uses limited PII for authentication, account management, and system administration purposes. Any data processing, aggregation, or analytics performed within applications hosted in OAH is the responsibility of the respective system owners.

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

☐ Yes: *Provide explanation below*
☒ No

OAH does not generate new data or inferred data; therefore, no new data is added to an individual's record.

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

☐ Yes: *Provide explanation below*
☒ No

OAH does not generate new data or perform analytics that would enable determinations about individuals. The system is limited to supporting authentication and administrative functions at the infrastructure level.

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

N/A. OAH does not generate or derive new data; therefore, no verification of new data for relevance or accuracy is required.

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?

Not applicable. Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) does not use AI, machine learning, or analytical models.

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

☐ Yes
☐ No

Not applicable. Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) does not make or support AI-based decisions about individuals.

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

☐ Yes
☐ No

Not applicable. Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) does not use AI or model-driven capabilities that could introduce model bias or AI-specific unintended consequences.

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

☐ Yes
☐ No

Not applicable. Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) does not use AI or analytical models requiring periodic review or retraining.

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

☐ Yes
☐ No

Not applicable. Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) does not use AI or model training; therefore, federated learning is not used.

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 to OAH data is restricted to authorized users whose roles require access to support system administration, account management, and security operations.

User Roles and Access Levels:

- **System Administrators**: System administrators have administrative access to manage system infrastructure, user accounts, and security controls within OAH. Access is granted based on role and official duties and are restricted in accordance with the principle of least privilege. Segmentation of duties is enforced to ensure separation of roles and prevent unauthorized access.
- **Contractors**: Contractors supporting OAH operations have role-based access necessary to perform system administration and maintenance functions. Contractor access is limited to assigned responsibilities and governed by DOI policies and contractual requirements.
- **Authorized DOI Personnel**: Designated DOI personnel have access to audit logs and system data for monitoring, auditing, and oversight of system activity. Access is limited to authorized personnel with need-to-know.

Authorization and Restrictions:

Access is granted through established account request processes, including validation by Supervisors and Contracting Officer Representatives (CORs) and linkage to DOI Access for identity verification. Criteria, procedures, controls, and responsibilities regarding access are documented in the OAH System Security and Privacy Plan.

All access is restricted through role-based access controls, enforcement of the least privilege principle, and segmentation of administrative duties. Multi-factor authentication is required for access to the DOI network. User activity is monitored through audit logs and centralized SIEM capabilities.

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

The Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) operates within a Department of the

Interior (DOI)-managed Microsoft Azure cloud environment that protects platform-level personally identifiable information (PII) and supports the secure storage, transmission, processing, and backup of mission-related PII in accordance with applicable Federal and Departmental security and privacy requirements. OAH has undergone a formal Assessment and Authorization (A&A) and is categorized as Federal Information Security Modernization Act (FISMA) Moderate in accordance with National Institute of Standards and Technology (NIST) standards.

Cloud-based PII storage complies with:

- **DOI Cloud and Information Security Policy** – Requires the use of approved cloud services and implementation of security and privacy controls consistent with Federal and Departmental requirements.
- **FISMA Moderate Security Baseline** – Ensures implementation of NIST SP 800-53 security controls appropriate to the sensitivity of the system, including access control, auditing, and incident response.
- **NIST SP 800-53 Rev. 5 and NIST SP 800-144** – Provide guidance for implementing security controls and managing risks associated with cloud computing environments, including protection of confidentiality, integrity, and availability of data.

OAH operates under a shared responsibility model for protecting information within the hosting environment. Within its authorization boundary, OAH is responsible for implementing, operating, and maintaining applicable inherited and shared infrastructure controls that protect information processed within the hosting environment. These controls include physical security, network protection, identity and access management, encryption, audit logging, centralized monitoring, backup and recovery, incident response support, vulnerability management, configuration management, and other hosting security controls necessary to protect information stored, transmitted, processed, or backed up within the environment.

Hosted mission systems are responsible for implementing application-level and mission-specific security and privacy controls, including determining the legal authority for collection, the purpose and use of the information, access restrictions, disclosure requirements, records retention, applicable System of Records Notice (SORN) coverage, and other privacy requirements specific to their systems.

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

OAH uses monitoring and auditing capabilities to record and monitor user access and activity within the system.

- **Automated Monitoring and SIEM** – Logging information is maintained at the local system or database level and then sent to a centralized Security Information and Event Management (SIEM) system.
- **Access Audit Logs** – Audit trail features are used to record and monitor user access and activities in the system, including event types, date and time of events, user identification, successful or failed access attempts, and security actions taken by system administrators.
- **Monitoring and Review** – OAH uses strict access controls and continually monitors user activity throughout the system's lifecycle. These controls are maintained and monitored in accordance with Federal laws, regulations, policies, and standards.

These monitoring and auditing capabilities support DOI's ability to identify, track, and respond to potential unauthorized access or misuse of system data.

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

OAH includes monitoring of user activity to support system security, auditing, and operational oversight.

Monitored Activities:

- Login attempts (successful and failed)
- User access and activity within the system
- Data or reports accessed and data exported
- Date, time, and user identification associated with system activity

Controls for Appropriate Use:

- Access to monitoring data is restricted to authorized personnel with need-to-know.
- Role-based access controls and segmentation of system administrators are enforced.
- The principle of least privilege is applied to all access.
- DOI Rules of Behavior and required training (IMT awareness and role-based privacy training) govern appropriate use

Monitoring activities are conducted in accordance with the OAH System Security and Privacy Plan and applicable Federal laws, regulations, and policies.

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

☒ Design
☒ Development
☒ Maintenance

Contractors are involved in the following OAH project activities:

- **Design** – Contractors support the design of system components and infrastructure within OAH.
- **Development** – Contractors facilitate development activities associated with system functionality, configuration, and enhancements within the OAH environment.
- **Maintenance** – Contractors' handle system administration, maintenance, account management, and operational support for OAH.

Some contractor personnel may have access to Administrative/Privileged account information as necessary to perform assigned duties related to system operations and account management. All contractor personnel with access are required to:

- Comply with Federal Acquisition Regulation (FAR) Privacy Act clauses and applicable privacy terms and conditions included in the contract.
- Complete DOI-approved annual privacy and security training, including Information Management and Technology (IMT) awareness training and role-based privacy training.

- Follow DOI Rules of Behavior and system-specific access procedures.

Contractor access is provisioned based on role and responsibilities, restricted through the principle of least privilege, and controlled through segmentation of duties.

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*

The OCIO Azure Hosting (OAH) system employs multiple layers of physical, technical, and administrative controls to protect PII.

- Physical security controls are provided by a FedRAMP-certified service provider that meets all Federal requirements for physical security of the information system.
- Access to facilities is restricted to authorized personnel through identification badge controls.
- The hosting environment enforces physical safeguards in accordance with Federal security standards applicable to cloud service providers.

Technical Controls

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Other: *Describe Below*
☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

- Multi-factor authentication is required for access to the DOI network and systems.
- Role-based access controls and the principle of least privilege are enforced to restrict access to authorized users.
- Segmentation of system administrators is implemented to enforce separation of duties.
- Audit logging and continuous monitoring are implemented, with logs maintained at the system level and forwarded to a centralized Security Information and Event Management (SIEM) system.

System security controls are implemented and maintained in accordance with NIST SP 800-53 requirements and documented in the OAH System Security and Privacy Plan.

Administrative Controls

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Methods to Ensure Only Authorized Personnel Have Access
☒ Encryption of Backups Containing Sensitive Data

☒ Rules of Behavior
☒ Role-Based Training
☒ Other: *Describe Below*
☒ Mandatory Security, Records and Privacy Training
☒ Regular Monitoring of Users' Security Practices

OAH has been formally approved to operate and meets Federal security requirements at a moderate level. The system uses a combination of its own security controls and controls provided by other connected systems. All systems hosted in OAH rely on these shared controls, which meet Federal security standards. Details about these controls are documented in the System Security and Privacy Plan.

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

Individuals may file a Privacy Act complaint regarding the OAH system through the Department of the Interior's established Privacy Act complaint process.

- **Submission Methods** – Complaints may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240, or through the DOI FOIA/Privacy Act request portal.
- **Responsible Office** – The DOI Chief Privacy Officer receives all Privacy Act complaints and assigns them to the appropriate Departmental Privacy Analyst for review and coordination with program officials.
- **Review Process** – The assigned reviewer evaluates the complaint, coordinates with the OAH Information System Owner and Information System Security Officer (ISSO) and determines whether a Privacy Act violation or policy issue occurred. If a potential breach is identified, DOI breach response procedures are initiated in accordance with the DOI Privacy Breach Response Plan.
- **Resolution and Response** – DOI provides a written response to the complainant outlining findings and any corrective action taken. Responses are generally issued within the timeframes established under 43 CFR Part 2, Subpart K.
- **Notice to Individuals** – Information on how to submit Privacy Act requests is provided through Privacy Notices and is available through the DOI Privacy Program website.

This process complies with 43 CFR Part 2, Subpart K, and ensures that Privacy Act concerns are addressed in accordance with DOI policy and established procedures.

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

Individuals may access their records in OAH by submitting a written Privacy Act request in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and DOI regulations at 43 CFR Part 2, Subpart K.

- **Request Methods** – Requests may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240, or through the DOI FOIA/Privacy Act request portal. The request must include sufficient identifying information, a description of the records sought, and verification of identity, such as a signed declaration under penalty of perjury or a notarized statement.
- **Processing and Review** – Upon receipt, the DOI Privacy Office verifies the requester's identity, determines whether responsive records exist, and coordinates with the appropriate OAH officials or hosted mission system owner, as applicable, to locate responsive records.
- **Hosted Mission System Records** – Requests involving mission-related records maintained within hosted applications are coordinated with the respective mission system owner or Privacy Act System Manager,

who is responsible for determining the releasability of records maintained under their authority, including any applicable System of Records Notice (SORN).
- **Notice to Individuals** - Information on how to submit Privacy Act requests is provided through the DOI Privacy Program website.

This process supports compliance with the Privacy Act while protecting the confidentiality, integrity, and security of information maintained within the OAH authorization boundary.

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

Individuals may request correction or amendment of inaccurate or erroneous information maintained by the Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and Department of the Interior (DOI) regulations at 43 CFR Part 2, Subpart K.

- **Request Methods** – Requests for amendment may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, or through the DOI FOIA/Privacy Act request portal. The request must include sufficient identifying information, a description of the information to be corrected, and verification of identity.
- **Processing and Review** – Upon receipt, the DOI Privacy Office reviews the request, verifies the requester's identity, and coordinates with the appropriate OAH officials or hosted mission system owner, as applicable, to determine whether the requested amendment is appropriate.
- **Response** – DOI responds in accordance with applicable regulations, either making the requested correction or providing an explanation if the request is denied.
- **Hosted Mission System Records** – OAH administers and protects the hosting infrastructure but does not determine the accuracy or completeness of mission-related personally identifiable information (PII) maintained within hosted applications. Requests to correct or amend mission-related records are coordinated with the respective mission system owner or Privacy Act System Manager, who is responsible for determining whether the requested amendment should be made in accordance with applicable legal authorities, System of Records Notices (SORNs), and Departmental policy.

This process supports compliance with the Privacy Act while ensuring that amendment requests are reviewed by the officials responsible for maintaining the accuracy and integrity of the applicable records.

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 for ensuring the proper use of data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy-protected information is shared among the Office of the Chief Information Officer (OCIO) Azure Hosting (OAH) Information System Owner, Information System Security Officer (ISSO), hosted mission system owners, Privacy Officer or Privacy Analyst, and all authorized users, in accordance with their respective roles and responsibilities.

Information System Owner: The Deputy Division Chief, Hosting Services Branch, Enterprise Service Delivery Division, OCIO, serves as the OAH Information System Owner and is responsible for the overall management of the OAH authorization boundary. The ISO ensures appropriate administrative, technical, and operational safeguards are implemented to protect information within the hosting environment and oversees compliance with applicable Federal and Departmental security and privacy requirements.

Information System Security Officer (ISSO): The ISSO is responsible for implementing, operating, and maintaining infrastructure-level security controls, including identity and access management, privileged account management, audit logging, continuous monitoring, vulnerability management, configuration management, and incident response support. In the event of a suspected or confirmed incident, the ISSO supports technical containment, preserves system logs and other evidence, conducts platform-level investigation and forensic support activities, and coordinates with the Department of the Interior Computer Incident Response Center (DOI-CIRC) and other cybersecurity personnel**.**

Hosted Mission System Owner: The mission system owner is responsible for the lawful collection, use, maintenance, disclosure, retention, and disposal of mission-related personally identifiable information (PII) maintained within the hosted application. During a privacy incident, the mission system owner is responsible for identifying the affected mission data, determining the applicable System of Records Notice (SORN), identifying affected individuals, assessing mission and program impacts, ensuring compliance with applicable records management requirements, and implementing mission-specific corrective actions and mitigation measures.

Privacy Officer or Privacy Analyst: The appropriate Privacy Officer or Privacy Analyst coordinates the privacy assessment of suspected or confirmed privacy incidents, evaluates potential privacy impacts, collaborates with the Department Privacy Office, and supports determinations regarding breach risk, notification requirements, reporting, and other actions required under Departmental privacy policies and procedures.

Authorized Users: All Department of the Interior (DOI) personnel and contractors with authorized access to OAH are responsible for protecting information entrusted to the hosting environment and must promptly report the loss, compromise, unauthorized disclosure, or unauthorized access of information to DOI-CIRC and the appropriate Privacy Officer or Privacy Analyst in accordance with the DOI Privacy Breach Response Plan and Department policy.

This shared responsibility model ensures that OAH is responsible for implementing, operating, and maintaining infrastructure-level safeguards, technical security controls, monitoring, logging, incident detection and response, and the protection of information processed within the hosting environment. Hosted mission system owners remain responsible for the lawful collection, use, disclosure, retention, disposal, and privacy governance of mission-related personally identifiable information (PII) maintained within their applications, including compliance with applicable Privacy Act requirements and Departmental privacy policies.

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 OAH, DOI will follow the procedures outlined in the DOI Privacy Breach Response Plan.

1. **Immediate Reporting**-Any suspected or confirmed breach must be reported within one hour of discovery to the DOI Computer Incident Response Center (DOI-CIRC) and the DOI Privacy Officer.
2. **Containment and Mitigation**-The Information System Security Officer (ISSO) and DOI-CIRC work to secure affected systems, contain the incident, and prevent further unauthorized access or data loss.
3. **Risk Assessment**-The Privacy Officer, in coordination with the ISSO and system owner, assesses the nature and scope of the breach, including the type of information involved and the potential risk to affected individuals.
4. **Notification**-If required, affected individuals will be notified without unreasonable delay, consistent with DOI policy and applicable Federal guidance. Notifications will include a description of the incident, the type of information involved, steps individuals can take to protect themselves and contact information for assistance.
5. **Oversight Reporting**-DOI will report incidents to appropriate oversight entities, including OMB, Congress, DHS, and other required agencies, when thresholds for reporting are met.
6. **Remediation and Prevention**-Corrective actions will be implemented to address identified vulnerabilities, which may include updating security controls, revising procedures, and providing additional training to personnel.

OAH is responsible for supporting technical containment, evidence preservation, infrastructure recovery, and coordination with the Department of the Interior Computer Incident Response Capability (DOI-CIRC) for incidents affecting the hosting environment. Hosted mission system owners remain responsible for assessing the impact to mission-related personally identifiable information (PII), determining applicable System of Records Notices (SORNs), identifying affected individuals, supporting breach notification activities when required, and implementing mission-specific corrective actions.

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

The OAH Privacy Impact Assessment will be reviewed and updated at least once every three years, in accordance with DOI policy and OMB requirements.

- Interim updates will occur sooner if any of the following events take place.
- Significant changes to system functionality, architecture, or hosting environment.
- Collection of new categories of PII or expansion of data use beyond what is described in the current PIA.
- New data sharing agreements or partnerships.
- Implementation of new or emerging technologies that may impact privacy risks
  Changes to applicable privacy laws, regulations, or DOI policies.

The Information System Owner is responsible for initiating the review process in coordination with the DOI Privacy Officer. All updated PIAs will undergo the standard review and approval process and be made publicly available on DOI's website unless publication is prohibited for security or law enforcement reasons.