



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:	Office of Hearing and Appeals - Internal
System or Project Acronym:	OHA-I
Date submitted for review:	March 19, 2026
System Operational Status:	Operational

Point of Contact

Name:	Adrienne Brooks-Hill
Title:	Privacy Officer
Office:	Office of the Secretary
Phone:	202-208-1605
E-mail:	DOI_Privacy@ios.doi.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

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

OHA-I was last assessed in 2013 and has undergone significant changes affecting the system, technology, and privacy documentation. This PIA updates the prior assessment to reflect the current OHA-I system boundary, functionality, data, safeguards, and privacy risks.

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

The Office of Hearings and Appeals–Internal (OHA-I) system is an internal repository used by authorized OHA personnel to store, organize, search, and research finalized OHA decisions and associated records from completed cases.

OHA-I supports legal research, precedent analysis, and consistency in adjudicatory decision-making by providing authorized staff access to historical case materials. Active cases that have not reached a final or published decision are not maintained in OHA-I.

The system may contain PII and other sensitive case information concerning appellants, claimants, decedents, heirs, parties, witnesses, and other individuals reflected in completed OHA case records. Access is restricted to authorized personnel with an official business need.

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.

UII Code: 010-000002878

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

This system is authorized by the Administrative Procedure Act, 5 U.S.C. 301,551 et seq. and other statutes that require or authorize the Department to conduct administrative hearings and appeals, including 16 U.S.C. 791 et seq.; 25 U.S.C. 2, 9, 372, 373, 373a, 373b, 374, 2201 et seq; 30 U.S.C. chap 2, 3, 3A, 5, 7, 15, 16, 23, 25 and 29; 43 U.S.C. 315a, 1201, 1331 et seq., 1601 et seq., and 1701 et seq.

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

Hearings and Appeals Files--Interior, OS-09 // 80 FR 26291 (May 7, 2015); Modification published 86 FR 50156 (September 7, 2021).

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

- ☐ Yes
☒ No

N/A

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

Windows Virtual Machines: used for data storage.

Perceptive Search: indexes files stored on Virtual Machines and enables internal teams to search records and case notes.

BarCode: ensures scanned records and scanned / filed in appropriate folders.

Ricoh Scanner: enables teams to digitally store records when physical copies are received.

Any PII in these applications stems from the originating legal case files.

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/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 |
| ☒ Username / user ID / acct ID | ☐ IP address / network ID | ☐ Device ID / online ID |
| ☐ Geolocation / GPS / location | ☐ Photos / video / audio | ☒ Health / medical information |
| ☒ Tribal or other ID number | ☒ Education information | ☒ Disability Information |
| ☒ Criminal / disciplinary info | ☒ Military records | ☐ Other: Describe below |

OHA-I contains PII reflected in finalized OHA case records and associated historical case materials. The specific PII varies based on the subject matter of the underlying proceeding.

Common categories may include names, aliases, addresses and contact information, dates of birth, Social Security numbers or other identifiers, family and relationship information, property or financial information, Tribal or trust-related information, employment information, medical or disability information, and other case-specific information contained in the official adjudicatory record.

OHA will validate the checked PII categories against the actual categories maintained in finalized OHA records and remove categories that are not present in the system.

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: <i>Describe Below</i> |

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

- | | |
|--|---|
| ☒ Paper Format | ☒ Fax |
|--|---|

- | | |
|---|---|
| ☒ Email | ☐ Telephone Interview |
| ☐ Face-to-Face Contact | ☒ Shared Between Systems: <i>Describe</i> |
| ☐ Website | ☐ Other: <i>Describe</i> |

Information maintained in OHA-I originates from completed OHA case records and supporting materials received through OHA adjudicatory processes. Source records may include information previously obtained from DOI systems such as TAAMS.

OHA-I does not have an automated system-to-system interface with TAAMS or other DOI systems. Information from those sources is incorporated into OHA case records through manual case-file processes.

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

PII maintained in OHA-I is used by authorized OHA personnel to identify and research finalized cases, locate relevant historical decisions and supporting records, analyze precedent, and support consistency in future adjudicatory work.

The information is retained as part of completed OHA case materials and is used for authorized legal research, records reference, and related official OHA functions.

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

OHA-I does not independently collect additional PII for unrelated purposes. The system maintains information contained in finalized OHA case records and associated materials necessary to preserve the completed adjudicatory record and support authorized legal research.

OHA limits access and use of the information to authorized personnel with an official need-to-know. The system is not used to supplement completed case files with unrelated PII.

Retention and disposition are governed by the applicable NARA-approved records schedule rather than by a general determination that individual data elements are no longer needed.

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 OHA: Authorized OHA personnel may access and share case information as necessary for legal research, records administration, and other official OHA functions.

Other DOI bureaus and offices: Finalized case information may be shared with BIA and other DOI bureaus or offices when necessary for authorized legal, administrative, records, or program purposes related to the underlying OHA matter.

OHA-I has no automated technical interface for external sharing. Information is shared through authorized manual case-file or records processes.

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

OHA-I does not currently rely on an MOU, MOA, or ISA as the basis for the manual case-file sharing described in this PIA. OHA-I has no automated interface with another agency or system for these disclosures.

Case-related disclosures are governed by the applicable statutory and regulatory authorities, Privacy Act requirements, INTERIOR/OS-09, and OHA adjudicatory procedures.

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.*

OHA-I does not provide individuals a separate opportunity to consent to the maintenance or authorized use of information contained in completed OHA case records. Information maintained in OHA-I originates from the adjudicatory record and is retained and used in accordance with applicable legal authorities, Privacy Act requirements, INTERIOR/OS-09, and records-management requirements.

Individual rights concerning access to and amendment of Privacy Act records are addressed in Sections 7.8 and 7.9.

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

- | | |
|---|--|
| ☐ Privacy Act Statement: | ☐ Other: <i>Describe Below</i> |
| ☒ Privacy Notice: | ☐ None: <i>Example - law enforcement cases.</i> |

OHA-I is a repository for completed OHA case records and does not serve as the direct point at which individuals submit information to the system.

Public notice concerning OHA-I's maintenance and use of Privacy Act records is provided through this PIA and

INTERIOR/OS-09, Hearings and Appeals Files.

Any notice associated with the original collection of information occurs through the applicable OHA adjudicatory or originating program process rather than through OHA-I itself.

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

The OHA-Internal (OHA-I) system operates as a standalone database that allows authorized users to retrieve data using specific case identifiers. These include the case title, which typically includes the name of the appellant or person requesting a hearing for cases managed by the Office of Hearings and Appeals. For cases handled by the Probate Hearings Division, the case title is the name of the decedent whose heirs are being determined. Additional identifiers, such as the docket number or case type, can also be used to search for and access case information. This structured retrieval process ensures efficient access to relevant data while maintaining the integrity of case management.

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

OHA-I contains finalized decisions, orders, and associated historical case information concerning identifiable individuals. Authorized OHA personnel may retrieve and review these records for legal research, precedent analysis, and other official OHA purposes.

OHA-I may also support internal reports or search results concerning completed cases. Access is limited to authorized personnel with an official business need.

OHA-I does not generate adjudicatory decisions or orders for active cases.

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

The accuracy of data received from external sources is confirmed through a combination of procedural safeguards and verification methods. In adjudicatory proceedings, parties involved in appeals or hearings can challenge the accuracy of information by filing pleadings, briefs, or other documents. They can also present testimony and cross-examine witnesses during hearings to ensure the reliability of the information provided.

Additionally, judges evaluate the credibility of witnesses and the validity of the information presented before making legal determinations. In some cases, data may be cross-checked with official DOI records or other authoritative sources to verify its accuracy. If necessary, the data subject may be contacted directly to clarify or confirm specific details. These methods ensure that the information used in the OHA-Internal (OHA-I) system is accurate and reliable, supporting fair and informed decision-making. Verification is always performed because accurate data is essential for resolving disputes and appeals effectively.

Section 4: Data Management and Retention

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

OHA-I contains multiple categories of records that may be subject to different NARA-approved disposition authorities.

Finalized OHA case records, working papers, reference copies, debt-collection matters, and system-generated records are retained and disposed of according to the disposition authority applicable to the specific record series and recordkeeping copy.

Where the originating DOI bureau or office remains the official custodian of the underlying administrative record, OHA returns or transfers that record in accordance with the applicable adjudicatory and records-management process. Records for which OHA is the official recordkeeping office are retained under the applicable OHA/Office of the Secretary NARA-approved disposition authority.

System shutdown, migration, storage location, or technical deletion capability does not independently establish a records-retention period.

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

Measures to validate the accuracy and completeness of data received from external sources are built into the adjudicatory proceedings. Judges and parties involved play a critical role in ensuring that the case record is complete and contains all necessary information for resolving the case. Procedural safeguards allow parties to challenge the accuracy of data by filing pleadings, briefs, or other documents, as well as presenting testimony and cross-examining witnesses during hearings.

These processes ensure that all information is thoroughly reviewed and verified before being used in decision making. By requiring active participation from both the judge and the parties, the system maintains a high standard of accuracy and completeness for external data, supporting fair and informed resolutions.

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

- ☒ Yes
☐ No

OHA-I maintains audit and security logs that record user authentication and system activity. Windows server login activity and other relevant security events are collected through DOI-authorized monitoring tools, including the current security-monitoring platform identified in the system's authorization documentation.

Audit information is accessible only to authorized personnel with security, administrative, or investigative responsibilities and is used to detect unauthorized access, investigate security events, and support system accountability.

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?

Historical case-record risk: OHA-I contains finalized adjudicatory records that may include extensive PII and sensitive information concerning parties and other individuals. There is a risk that historical information could be accessed or used beyond an authorized legal or records purpose. Access is limited to authorized OHA personnel based on role and need-to-know.

Search and retrieval risk: Perceptive Search and related indexing capabilities allow authorized personnel to locate historical case information efficiently. Search capabilities increase the potential impact of inappropriate access. OHA mitigates this risk through access restrictions, authentication, audit logging, and security monitoring.

Disclosure risk: Finalized case records may contain information subject to Privacy Act, adjudicatory, confidentiality, or other disclosure restrictions. Information is shared only through authorized OHA processes and under applicable legal authority.

Retention risk: Historical case information may be retained longer than authorized or duplicate copies may persist. OHA mitigates this risk by applying the applicable NARA-approved disposition authority and coordinating recordkeeping responsibilities with the originating bureau or office and OHA Records Management.

Accuracy/context risk: Historical records may contain disputed evidence, allegations, or information considered during adjudication. OHA-I preserves finalized case records in context and does not treat all information appearing in a historical case file as an independently verified current fact about an individual.

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

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

- ☐ Yes: *Provide explanation below*
☒ No

No, newly generated or inferred data will not be placed in an individual's official record. The OHA-Internal (OHA-I) system does not create or infer new data about individuals through aggregation or analysis. Instead, it only stores information that is directly provided by the parties involved in a case or required for case management. This ensures that the system focuses solely on maintaining accurate and relevant records for adjudicatory purposes without adding unnecessary or speculative information.

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

- ☐ Yes: *Provide explanation below*
☒ No

No, the system does not make determinations about individuals. The OHA-Internal (OHA-I) system is designed solely to store and recall data for legal search and case management purposes. It does not generate or infer new data, nor does it make decisions, predictions, or assessments about individuals. All determinations are made by judges or authorized personnel based on the original information provided during the adjudicatory process, ensuring the system functions as a secure repository for case-related data.

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.

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?

N/A. OHA-I does not use AI or machine learning models.

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

- ☐ Yes
☐ No

N/A. OHA-I does not make or support AI-based decisions affecting individuals.

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

- ☐ Yes
☐ No

N/A. OHA-I does not use AI or machine learning models that could introduce AI-specific bias or unintended consequences.

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

- ☐ Yes
☐ No

N/A. OHA-I does not use AI or machine learning models requiring periodic review or retraining.

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

- ☐ Yes
☐ No

N/A. OHA-I does not use federated learning or conduct AI or machine learning model training.

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 | ☒ System Administrator |
| ☐ Contractors | ☐ Other: <i>Describe below</i> |
| ☐ Developers | |

User Groups with Access to Project Data:

System Administrators: Responsible for managing and maintaining the system.

Program Staff: Includes OHA employees who require access to perform case management and adjudicatory duties.

Access Determination, Authorization, and Restriction:

Access to project data is determined based on role-based access controls and the principle of need-to-know. Each user's access level is assigned according to their job responsibilities and the specific data they require to perform their duties.

Authorization is granted through a documented process, where supervisors submit written requests specifying the level of access required for the user. These requests are reviewed and approved by the system manager or IT specialist.

Access is restricted through technical controls, such as user authentication, and periodic access reviews are conducted to ensure that access remains appropriate and necessary. Additionally, all users must complete annual IT security and privacy training to reinforce their understanding of proper data handling practices.

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

N/A. This is not a cloud hosted system.

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

The OHA-Internal (OHA-I) system monitors and detects unauthorized access, use, or exfiltration of Personally Identifiable Information (PII) through a combination of advanced tools and processes.

[REDACTED] are used to track user activity and server interactions, capturing detailed audit logs of login attempts, system access, and actions performed within the system. These logs are regularly reviewed to identify suspicious behavior, such as unauthorized access attempts or unusual patterns of data usage.

Additionally, the system employs firewalls to control and monitor network traffic, blocking unauthorized connections and isolating sensitive data from external threats. Alerts are configured to notify administrators of potential security incidents, such as large data transfers or failed login attempts. These measures ensure that any unauthorized access or misuse of PII is quickly detected and addressed, maintaining the integrity and security of the system.

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

OHA-I performs user-linked security and system-activity monitoring as part of normal cybersecurity and system-administration functions.

Audit and monitoring information may include user authentication events, system access, administrative activity, and other security-relevant actions.

Monitoring is conducted for authorized cybersecurity, system-administration, troubleshooting, compliance, and incident-response purposes. Access to audit and monitoring information is restricted to authorized personnel with an assigned role and need-to-know.

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

- ☐ Design
☐ Development
☐ Maintenance

N/A.

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

Physical Controls

- | | |
|--|---|
| ☒ Security Guards | ☐ Cipher Locks |
| ☐ Key Guards | ☒ Identification Badges |
| ☒ Locked File Cabinets | ☐ Safes |

- | | |
|---|---|
| ☒ Secured Facility | ☐ Combination Lock |
| ☒ Closed Circuit Television | ☐ Other: <i>Describe Below</i> |

OHA-I infrastructure is maintained in a federally controlled secured facility. Physical access is restricted to authorized personnel through Federal facility access controls. Applicable facility protections include identification requirements, controlled access, monitoring, and other safeguards established under DOI and Federal physical-security requirements.

Technical Controls

- | | |
|---|--|
| ☐ Password | ☐ Intrusion Detection Systems (IDS) |
| ☒ Firewall | ☒ Virtual Private Network (VPN) |
| ☒ Encryption | ☒ Public Key Infrastructure (PKI) Certificates |
| ☒ User Identification | ☐ Biometrics |
| ☐ Other: <i>Describe Below</i> | |

The OHA-Internal (OHA-I) system employs several technical controls to protect Personally Identifiable Information (PII) and ensure the security and privacy of sensitive data. Public Key Infrastructure (PKI) certificates are used to secure communications and authenticate users accessing the system, ensuring that only authorized individuals can access the system and that data transmitted is encrypted and protected from interception. Firewalls are implemented to monitor and control network traffic, blocking unauthorized access and isolating OHA-Internal network traffic from other networks to safeguard sensitive information. Data stored in the system is encrypted, ensuring that even if accessed improperly, it cannot be read or used without the proper decryption keys. The encryption is deployed at rest and in-transit. User identification is enforced through unique credentials and multi-factor authentication (MFA), adding an extra layer of security to verify the identity of users accessing the system. Additionally, a Virtual Private Network (VPN) is used to create a secure connection for remote users, encrypting data transmitted over the network and protecting it from unauthorized access, even when accessed outside the office. Together, these technical controls ensure compliance with privacy and security standards while protecting PII from unauthorized access or disclosure.

Administrative Controls

- | | |
|--|---|
| ☐ Periodic Security Audits | ☒ Methods to Ensure Only Authorized Personnel Have Access |
| ☒ Backups Secured Off-site | ☒ Encryption of Backups Containing Sensitive Data |
| ☐ Rules of Behavior | ☒ Mandatory Security, Records and Privacy Training |
| ☐ Role-Based Training | ☒ Regular Monitoring of Users' Security Practices |
| ☐ Other: <i>Describe Below</i> | |

The OHA-Internal (OHA-I) system uses several administrative controls to protect Personally Identifiable Information (PII) and ensure it meets all privacy and security requirements.

To prevent data loss, the system's information is regularly backed up and stored securely at an off-site location. These backups allow critical data to be safely restored if there is a system failure, natural disaster, or other emergencies.

Access to the system is limited to authorized personnel only. Access levels are assigned based on job duties and the need-to-know principle. Supervisors must submit a written request that explains the type of access a user needs, and each request is reviewed and approved by the system manager or an IT specialist.

All personnel with access to the system must complete required security, records management, and privacy training every year. This training ensures users understand how to handle PII responsibly and follow established policies and procedures. In addition to training, the system undergoes continuous monitoring to detect potential risks or unauthorized activity.

User activity and security practices are monitored through tools described in the System Security Privacy Plan (SSPP). [REDACTED]

[REDACTED] provides enhanced monitoring of server activity and supports stronger compliance with security standards.

Together, these administrative controls (access management, training, data backups, and continuous monitoring) work to protect PII within the OHA-I system and ensure that sensitive information is managed securely throughout its entire lifecycle

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

Individuals can submit a Privacy Act complaint by contacting the Department of the Interior (DOI) Privacy Office or the designated Privacy Officer. Complaints should be submitted in writing and include a clear description of the issue, such as concerns about the collection, use, or disclosure of their Personally Identifiable Information (PII). The following points of contact are available for submitting complaints:

- Mailing Address:

U.S. Department of the Interior
Privacy Office
OS/OCIO, Room 7112
1849 C Street, N.W.
Washington, D.C. 20240

- Email Address:

DOI_Privacy@ios.doi.gov

- Website: <https://www.doi.gov/privacy/privacy-civil-liberties>.

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

Individuals seeking access to records about themselves maintained in OHA-I may submit a Privacy Act request in accordance with DOI Privacy Act regulations and the notification and access procedures applicable to INTERIOR/OS-09.

Requests are reviewed under the Privacy Act and other applicable legal requirements. Any applicable restriction, exemption, privilege, or limitation on access is determined through the authorized review process.

Direct system access to OHA-I is limited to authorized OHA personnel and is separate from an individual's statutory right to request access to records about themselves.

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

The OHA-Internal (OHA-I) system provides processes for individuals to correct inaccurate or erroneous information in accordance with the Privacy Act of 1974. Individuals can submit requests for correction or amendment of their Personally Identifiable Information (PII) through established procedures that the DOI Privacy Office established. See <https://www.doi.gov/privacy/privacy-act-requests>. These requests are reviewed and adjudicated by the organization, which evaluates the validity of the claims and determines whether corrections are warranted.

If corrections are made, the organization ensures that all authorized recipients of the PII are informed of the updated information. Additionally, individuals are notified of the changes made to their records. In cases where a request for correction is denied, individuals are provided with the reasons for the denial and given the opportunity to appeal the decision or request further review. These processes demonstrate the organization's commitment to maintaining accurate and reliable data while supporting individuals' rights to redress.

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?

The System Owner is responsible for assuring the proper use of data and for reporting any loss, compromise, unauthorized disclosure, or unauthorized access of privacy-protected information. Their duties include overseeing compliance with privacy policies, ensuring that data is used only for authorized purposes, and implementing safeguards to protect Personally Identifiable Information (PII).

In the event of a privacy incident, the System Owner is required to promptly report the incident to the Department of the Interior's Computer Incident Response Center (DOI-CIRC) in accordance with DOI policy. This includes providing details about the incident, actions taken to mitigate harm, and steps to prevent future occurrences. The System Manager works closely with the Privacy Officer and Information System Security Officer (ISSO) to ensure proper handling and resolution of privacy incidents.

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 the OHA-Internal (OHA-I) system, the following steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies:

Mitigation of Harm: Immediate actions will be taken to contain the breach, such as securing affected systems, disabling unauthorized access, and identifying the scope of the incident. Immediate reporting to DOI Cyber Incident Report Council within one hour of discovery. A privacy risk assessment will be conducted to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals. Mechanisms to mitigate harm, such as offering credit monitoring or identity theft protection, will be implemented if necessary.

Notification of Affected Individuals: Individuals whose Personally Identifiable Information (PII) was compromised will be promptly notified. Notifications will include details about the breach, the type of information exposed, potential risks, and steps they can take to protect themselves. Notifications may be sent via mail, email, or other appropriate methods, depending on the nature of the breach.

Reporting to Oversight Agencies: The breach will be reported to the Department of the Interior's Senior Agency Official for Privacy (SAOP) and other relevant oversight bodies, such as the Office of Management and Budget (OMB) or the National Archives and Records Administration (NARA), as required by law or policy. Incident reports will include a summary of the breach, actions taken to mitigate harm, and plans for preventing future incidents.

These steps ensure a coordinated response to privacy breaches, minimizing harm to individuals and maintaining compliance with legal and regulatory requirements.

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

OHA-I will be reviewed annually through the applicable DOI Privacy Threshold Analysis process and whenever a material change to system functionality, technology, data, retrieval, sharing, retention, security capabilities, or operations may affect privacy risk.

This PIA will be updated when a material change makes the current public assessment inaccurate or incomplete. When review confirms that no material privacy change has occurred and the PIA remains accurate, it may be reaffirmed in accordance with DOI privacy procedures.