U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: DOI Privacy Act Access and Consent Forms
Bureau/Office: Office of the Chief Information Officer
Date: June 27, 2023
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Department of the Interior (DOI, Department) developed two forms, DI-4016, *Request for Individual Access to Records Protected under the Privacy Act*, and DI-4017, *Consent for Disclosure of Records Protected Under the Privacy Act*, in accordance with the Office of

Management and Budget (OMB) Memorandum M-21-04, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act*, and the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act).

The Privacy Act of 1974, as amended, 5 U.S.C. 552a, governs how Federal agencies collect, maintain, use, and disseminate information about individuals that is maintained in a system of records, which is a group of records under the control of a Federal agency from which information is retrieved by the name of the individual or some other unique identifier assigned to the individual. The Privacy Act allows individuals to seek access to and amendment of their records subject to certain exemptions. The Privacy Act also requires Federal agencies to publish system of records notices (SORNs) in the *Federal Register* to provide notice to the public on the maintenance of their systems of records, including the purpose of the system, categories of individuals whose records are maintained, what information is collected and maintained on individuals, the agency's legal authorities for maintaining records, what organizations may receive records on individuals, how individuals may seek access to or correction of their records, and other information on managing and safeguarding the records. DOI records subject to the Privacy Act are maintained under government-wide, Department-wide, and bureau or office SORNs that may be viewed on the DOI Privacy Program SORN page.

The CASES Act modernized the Privacy Act of 1974 and required OMB to issue guidance to agencies for the creation of electronic consent forms and how individuals can request access to, and consent to, the disclosure of protected records under the Privacy Act. OMB M-21-04 mandated agencies digitally accept electronic identity proofing and authentication processes allowing an individual to provide prior written consent for the disclosure of their records under the Privacy Act. Prior to the enactment of the CASES Act and OMB M-21-04, Privacy Act requests were hand-delivered or mailed, and required a wet signature or notarization to validate the identity of the requesting individual making the Privacy Act request.

The DI-4016 and DI-4017 forms help individuals make requests for access to, or consent to the disclosure of, records protected under the Privacy Act and are based on the templates mandated in OMB M-21-04. The DI-4016 form will be used by individuals to submit a Privacy Act request to the Department for access to their records. The DI-4017 form will be completed and submitted by individuals to authorize the disclosure of their records to another person or entity. These forms may also be submitted by parents on behalf of minors or from legal guardians on behalf of incompetents.

Individuals may request access to records that are maintained in a system of records in the possession or under the control of DOI by complying with DOI Privacy Act regulations at 43 CFR part 2, subpart K and following the procedures outlined in the applicable SORN that covers the records being requested. The DI-4016 and DI-4017 access and consent forms will be managed under the Privacy Act and DOI's Privacy Act request process and the DOI Privacy Act regulations, which provide procedural guidance on how individuals may determine whether DOI maintains records on them and how they may seek access to or correction of their records, as well as exemptions that apply to DOI systems of records under the Privacy Act.

These forms are managed by the DOI Privacy Office and will be posted on the DOI Privacy Act Requests website, which also provides instructions on how individuals can download, complete and submit Privacy Act requests to the Department. Completed and signed forms and supporting documents may be submitted to the Privacy Act System Manager identified in the applicable SORN or the Associate Privacy Officer (APO) at the DOI bureau of office where the records are located. The forms may also be submitted to the DOI Privacy Office, which are forwarded to the appropriate bureau/office APO for processing. In addition to accepting these forms submitted via postal mail, DOI has developed web versions of these forms so individuals may choose to submit Privacy Act requests digitally in accordance with the requirements of the CASES Act and OMB M-21-04.

DOI is developing a workflow to leverage Login.gov, the General Services Administration (GSA) owned and operated government-wide remote identity verification system, to ensure individuals are properly identity proofed and authenticated before providing access to protected records. Individuals will be able to complete, sign, and submit Privacy Act requests using the web versions of the DI-4016 and DI-4017 forms on the DOI Privacy Act Request website once the service is implemented. Although DOI receives and maintains personally identifiable information (PII) from individuals through submission of these forms, only the requester's name, email address, contact information, and other limited information provided by individual requesters is routinely shared with DOI. The government issued identification and sensitive PII collected and used by GSA for identity proofing and authentication through Login.gov are maintained by GSA and is generally not shared with DOI, however, this information may be shared with DOI in cases where there is a legitimate business need or to meet a legal requirement or obligation under Federal law and policy. This PIA will be updated to reflect additional information handling practices, any potential risks and impacts to individual privacy, and mitigating controls implemented as the Login.gov workflow is completed. Individuals may also view GSA's Login.gov PIA for evaluation of privacy risks related to the collection, use, storage and sharing of PII and safeguards employed to mitigate or manage these risks. GSA has also published a SORN, GSA/TTS–1, Login.gov.

C. What is the legal authority?

Privacy Act of 1974, as amended, 5 U.S.C. 552a; Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act); OMB Memorandum M-21-04, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act*; DOI Privacy Act regulations, 43 CFR part 2, subpart K.

D. Why is this PIA being completed or modified?

☒ New Information System
☒ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System

☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
☒ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	N/A	N/A	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

- DOI Privacy Act requests submitted by requesters, responsive records from other systems of records, and related correspondence are maintained under INTERIOR/DOI-57, Privacy Act Files, 81 FR 45527 (July 14, 2016), modification published at 86 FR 50156 (September 7, 2021).

- Records that include consolidated FOIA and Privacy Act requests and responsive records are maintained under INTERIOR/DOI-71, Electronic FOIA Tracking System and FOIA Case Files, 81 FR 33544 (May 26, 2016), modification published at 86 FR 50156 (September 7, 2021). This SORN is being updated and renamed to reflect modifications to the system and the consolidation with the INTERIOR/OS-69 system of records.

- Records of appeals filed by individuals on decisions on Privacy Act and FOIA requests are maintained under INTERIOR/OS-69, Freedom of Information Act Appeals Files, 64 FR 16986 (April 7, 1999), modification published at 86 FR 50156 (September 7, 2021). This system of records is being consolidated with the INTERIOR/DOI-71 system of records. This SORN will be rescinded once the updated SORN for the consolidated system is published.

- Responsive records may be obtained from other originating systems of records that are maintained under government-wide, Department-wide, or bureau/office SORNs. DOI SORNs may be viewed on the DOI SORN website.

- GSA maintains records on individuals who utilize Login.gov and has published a SORN for the Login.gov system, GSA/TTS–1, Login.gov, 82 FR 6552, (January 19, 2017), modification published 82 FR 37451 (August 10, 2017).

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*

OMB Control Number 1093-0013, DOI Access & Consent Forms; Expiration date: January 3, 2026

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Birth Date
☒ Other Names Used
☒ Personal Email Address
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

DOI collects a minimum amount of PII through the DI-4016 and DI-4017 forms to identify the individual requester and locate the records being sought for the Department to provide a response. PII collected on both forms from the individuals submitting the Privacy Act request includes: full name, alias or other names used email address; current home address; date of birth; address for receiving requested records; and information about the records to help the bureau, office or program locate the requested records. Other information may be requested to verify the individual's identity or to process the Privacy Act request. Parents or legal guardians seeking access to records of a minor or an incompetent must provide the name of record subject and relationship of record subject. The name of the recipient, either a person or entity that is authorized to receive the records are required in the DI-4016 and DI-4017 forms. Both forms require a signature and date of the individual submitting the request.

Individuals may voluntarily choose to submit an electronic request and authenticate through GSA's Login.gov service. Login.gov requires individuals to create a user account by providing a valid email address and creating a password. DOI will identify the requester by their email address used in creating their Login.gov accounts. Login.gov also requires users to set up a multi-factor authentication (MFA) using either a phone number, security key, or an

authentication application. GSA may require users to provide the following personal information to verify their identity including but not limited to full name, date of birth, home address, Social Security number (SSN), type and number of state-issued identification card (ID) such as driver's license or state ID. The GSA Login.gov system may also use the contact phone number provided by the user to confirm home address with the user's consent.

A user's email address, phone number, and agency specific universal unique identifier (UUID) may be needed to grant access to services and Personal Identity and Verification (PIV) or Common Access Card (CAC) for Federal and Department of Defense (DoD) employees or service members. This information may be shared with DOI as a participating partner agency. No other PII data will shared with DOI. Please refer to the GSA Login.gov PIA for information on how requester PII data is collected, used, stored, and disseminated by GSA's Login.gov service.

The DOI Privacy Program website provides information to the public on the DOI Privacy Policy, DOI's inventory of published SORNs and exemption rules, published PIAs, publicly available reports and policy, and privacy contacts for the Senior Agency Official for Privacy, Departmental privacy officials, and bureau and office Associate Privacy Officers. The DOI Privacy Act page provides the posted DI-4016 and DI-4017 forms and instructions on how to submit Privacy Act requests. Individuals are not required to provide personal information to visit or view the DOI Privacy Act website, though may choose to provide PII when submitting a Privacy Act request using the web version of the DI-4016 or DI-4017 form. Once a web form is submitted, additional communication or correspondence with the requester will be managed through email, mail or phone calls. However, DOI may collect metadata from visitors to the Privacy Act website, such as device information internet domain, Internet Protocol address, browser type, operating system, date and time, session cookies, other pages visited on DOI website and search terms used from an external agency to get to DOI.gov. This information is collected by default to enhance user experience and allow an electronic device to remember specific information about the user's session while on the DOI website to improve the experience as outlined in the DOI Privacy Policy. The DOI Privacy Act website does not use persistent cookies that collect PII, as outlined in OMB M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☐ Tribal agency
☐ Local agency
☐ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

Information is obtained from submission of the DI-4016 and DI-4017 forms and is provided by the individual who is the requester or the parent or legal guardian of a minor or an incompetent to submit a request for their records under the Privacy Act.

GSA may share information collected through Login.gov that is provided by individuals for identity verification and authentication with DOI as a partner agency. Users' phone number provided for MFA purposes will not be shared with DOI. Data shared will encrypted and transmitted via Transport Layer Security over Hypertext Transfer Protocol Secure and as an additional security step, secured in Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) both authentication protocols that authenticate users, and provide identity data for access control and as a communication method for a user's identity.

C. How will the information be collected? Indicate all that apply.

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

The signed DI-4016 and DI-4017 forms and any supporting documents may be electronically submitted via email or the web forms and the paper versions may be submitted via mail. In some cases, individuals may also choose to visit a DOI facility and present the forms to request access to or consent to disclosure of records in person. Information may be collected from the requester via telephone or email communication to clarify or obtain additional information to process a Privacy Act request.

GSA Login.gov collects information directly from individuals who create user accounts. Login.gov may share limited personal information with DOI as a partner agency when requesters choose to create Login.gov user accounts to verify their identity and authenticate them to access the DOI Privacy Act Request website which is managed by the DOI Privacy Office.

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

The PII collected is used to verify the identity of the requester or parent or legal guardian to protect individual privacy and ensure confidential Privacy Act information is not improperly released. The PII is also used to locate the requested records and obtain the recipient information to send the records. This information is required to process the Privacy Act request and allow individuals access to their records that are maintained in a DOI system of records. Any additional information requested from the individual is limited to the information needed to locate the records and provide responsive records.

Login.gov will use requester's PII to verify their asserted identity and authenticate them via a secure connection and return verification to DOI in order to process the Privacy Act request and provide responsive records.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

The DOI Privacy Office is located within the Office of the Chief Information Officer (OCIO) and is responsible for centrally coordinating and overseeing Privacy Act requests for the Department. The DOI Privacy Office will review and forward Privacy Act requests to the appropriate APO at the DOI bureau or office that maintains the record being sought for processing. Information will also be shared with System Managers for the applicable system of records to locate the requested records and respond to the Privacy Act request. Information may also be shared with the DOI Freedom of Information Act (FOIA) Office for combined FOIA and Privacy Act requests or the DOI (FOIA)/Privacy Act Appeals Officer for appeals to a denial of access.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

The DOI Privacy Office will review and forward Privacy Act requests to the appropriate APO at the DOI bureau or office that maintains the record being sought for processing. Bureau/office APOs will work with the applicable Privacy Act System Manager to locate the records within their organization and process the response to the requester. Information will also be shared with System Managers to locate the requested records and respond to the Privacy Act request. Information about the requester or request for records may also be shared FOIA Offices to process combined requests under the Privacy Act and FOIA or with the FOIA and Privacy Act Appeals Officer to process appeals submitted by requesters.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Information may be disclosed externally to organizations by DOI officials to process Privacy Act requests or support the Privacy Act system of records, including but not limited to the Department of Justice as authorized and necessary to provide support on litigation; National Archives and Records Administration, Office of Government Information Services to resolve disputes; a debt collection agency for collecting debts owed for processing requests; another Federal agency to assist in responding to a request or assist in a data breach; or other organizations as authorized under the Privacy Act or as a routine uses outlined in the DOI-57 or other applicable SORN.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Information may be shared with other Tribal, state or local agencies as needed and authorized to process a Privacy Act request as described in the routine uses in the applicable SORN.

☒ Contractor: *Describe the contractor and how the data will be used.*

Information may be shared with a contractor or expert providing services for maintenance of the system or records or that supports the Department and bureau privacy offices, FOIA offices, and the Privacy Act System Managers for the applicable system of records to locate records and process requests.

Contractors are provided limited access to Drupal CMS and DOI Privacy Act Request website as authorized users to provide program support or technical support in managing the tool.

☒ Other Third-Party Sources: *Describe the third party source and how the data will be used.*

GSA's Login.gov service may share personal information provided by members of the public to contracted third party organizations for identity verification and authentication purposes. Please refer the Login.gov PIA for details on how PII data is shared with third party entities.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

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

Providing information is voluntary and individuals may decline to provide information when completing the forms. However, requests will be delayed or not processed if the required information is not provided to locate the records requested or if the individual does not provide sufficient information to be identity proofed and authenticated. Individuals are provided a Privacy Act statement on the forms and consent to the specific use of their PII through the process of signing and submitting the forms. The DOI Privacy Act Requests page contains a Privacy Act statement and information on how individuals may submit requests or complaints. The DOI Privacy Policy also provides information on how information is collected, processed, and stored when visiting the website.

Individuals opting to use Login.gov must authorize sharing of their PII data in order to access services and information provided by the Department, and to allow DOI to recognize that user to process requests. Login.gov will use DOI branding at the sign in and account creation process to ensure the individual is aware their PII information may be disclosed to DOI. GSA has published a SORN and PIA for Login.gov and the Login.gov website has clear detailed instructions on the steps and PII involved with establishing a user account and provides a detailed Login.gov Privacy Act statement that describes the authority, purpose, routine uses and consent mechanism.

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

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

Individuals are provided a Privacy Act statement on both the DI-4016 and DI-4107 forms and a Privacy Act statement and detailed instructions on the DOI Privacy Act Requests website where the forms are posted.

Requesters opting to use a Login.gov account to remotely identity proof when submitting a Privacy Act request to DOI can review the Login.gov privacy policy and Login.gov Privacy Act statement.

☒ Privacy Notice: *Describe each applicable format.*

Individuals are also provided notice through the publication of this PIA, the DOI-57 SORN and other applicable SORNs.

Individuals can also refer to the GSA Login.gov PIA and GSA/TTS–1, Login.gov, SORN for details on specific collection, use, storage or sharing of their PII by GSA.

☐ Other: *Describe each applicable format.*

☐ None

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

Information may be retrieved by the name and email address of the requester or the parent or legal guardian of the subject of the record during the Privacy Act request process and to respond to the request.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

DOI may produce reports on individual requesters to track and manage Privacy Act requests, ensure they are timely processed, document completed requests, and develop metrics to improve the service. These reports may include name of requester, dates of receipt, completion and response, and status of requests.

GSA Login.gov may produce compliance/audit reports on individuals' actions in the system for investigatory and fraud mitigation purposes. Please see the GSA Login.gov PIA for information on reporting functions within the system and how reports on individuals is generated, used or shared.

☐ No

Section 3. Attributes of System Data

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

Data is collected directly from the requester or the parent or legal guardian of the subject of the record through the DI-4016 and DI-4017 forms, and is presumed to be accurate at the time it was provided by the individuals. Inaccurate information may be verified with the applicable Privacy Act system of records or directly with the individual via email or phone. Individuals requesting amendment of their records must submit the request to the Departmental Privacy Officer, bureau/office APOs, or Privacy Act System Manager, and meet the requirements of 43 CFR 2.246.

DOI will rely on GSA for identity proofing and authentication services. For individuals opting to create user accounts for identity verification purposes, Login.gov may require additional PII such as full name, date of birth, and SSN. Login.gov may validate an individual's additional PII data against other records using a third-party identity proofing service to confirm the user's identity prior to authenticating and granting accessing a participating agency's service. Requesters opting to utilize the Login.gov service can review the GSA Login.gov PIA for information on how their PII is verified for accuracy.

B. How will data be checked for completeness?

Data is collected directly from the requester or the parent of legal guardian of the subject of the record through the DI-4016 and DI-4017 forms and is presumed to be complete at the time it was provided by the individuals. Incomplete information may be verified with the applicable Privacy Act system of records or directly with the individual via email or phone. Individuals requesting amendment of their records must submit the request to the Departmental Privacy Officer, bureau/office APOs, or Privacy Act System Manager, and meet the requirements of 43 CFR 2.246.

PII data provided by individuals for Login.gov user accounts will be verified by GSA. Individuals must ensure that their email address and phone number provided for account creation are accurate and complete, and that they have access to the email address and phone number. Login.gov will confirm a user's email address and phone number by sending a one-time security code to that phone number requiring them to enter for multi-factor authentication purposes.

Users can also sign-up to use Login.gov authentication application. Requesters opting to utilize the Login.gov service can review the GSA Login.gov PIA for information on how their PII is checked for completeness.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Data is collected directly from the requester or the parent of legal guardian of the subject of the record through the DI-4016 and DI-4017 forms, and is presumed to be current at the time it was provided by the individuals. Information that is not current may be verified with the applicable Privacy Act system of records or directly with the individual via email or phone. Individuals requesting amendment of their records must submit the request to the Departmental Privacy Officer, bureau/office APOs, or Privacy Act System Manager, and meet the requirements of 43 CFR 2.246.

Login.gov collects PII directly from the individual opting to use their identity authentication and verification service, therefore it is presumed to be current at the time provided by individuals. Individuals are responsible for updating their email address or phone number on the Login.gov account page, however, in order to update or amend their additional PII data, users must first delete their current identity verified Login.gov user accounts, then create a new account for identity proofing. Requesters opting to utilize the Login.gov service can review the GSA Login.gov PIA for information on how their PII data is kept current.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

DOI records are maintained under the Departmental Record Schedule (DRS) 1.1A Short Term Administrative Records, which was approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-0001-0001). These records have a temporary disposition and are determined obsolete when they are no longer needed for administrative, legal, audit, or other operational purposes, and destroyed no later than 3 years after cut-off. Cutoff after date of reply. Records maintained for access and consent forms belong to DOI and are retained in accordance with applicable agency records retention schedules or General Records Schedules approved by NARA.

When a request is denied, or appealed, for Privacy Act amendments, or any erroneous releases: Temporary, DAA-0048-2013-0001-0002 (DRS 1.1.0002) – Long Term Administration Records. Cutoff after upon agency agreement to amend, final determination by agency, on expiration of time in which a requester can file suit, or on final adjudication by the courts, whichever is later. Destroy 7 years after cutoff.

GSA is responsible for managing its Login.gov records in accordance with the Federal Records Act and approved records retention schedules.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

DOI maintains records in accordance with records retention schedules approved by NARA and is responsible for the disposal of the records in accordance with the approved disposition methods include shredding or pulping for paper records and degaussing or erasing electronic records in accordance with NARA guidelines and Departmental policy.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate privacy risk to individuals due to the sensitive PII collected on the forms and any supporting documents obtained by the individual or the originating system of records for the records being requested. DOI collects and maintains PII to process Privacy Act requests and is required to include sufficient PII to identify records contained within a specified DOI SORN and requesters are required to provide PII and basic contact information to process requests. The requester must sign the forms with a perjury statement or the signature must be notarized, if requesting information pertaining to themselves. The requester can choose to request access to or consent to disclosure of their records by submitting the request under 18 U.S.C. § 1001 and 5 U.S.C. § 552a(i)(3), which permits statements to be made under penalty of perjury in substitution of notarization. DOI may also contact a requester to provide further information to verify their identity or to process their request and provide the records being sought.

There is a risk that individuals may not know that DOI maintains records on them or that individuals providing information do not have adequate notice or have an opportunity to consent to how their PII will be collected or used. Individuals may seek the existence of records maintained on them by following the procedures outlined in the DOI Privacy Act regulations at 43 CFR part 2, subpart K, viewing the instructions on the DOI Privacy Act requests website, or contacting the appropriate privacy official at the Department, bureau or office. The risk of adequate notice and opportunity to consent is mitigated by the Privacy Act statements provided on the DI-4016 and DI-4017 forms and posted the DOI Privacy Act request website, the publication of this PIA and INTERIOR/DOI-57, Privacy Act Files, and related SORNs. GSA also provides a Privacy Act Statement on the Login.gov website and published the GSA Login.gov PIA, and Login.gov SORN. Individuals are also provided with general notice of the existence of Privacy Act records through the DOI Privacy Program website and the published DOI and Government-wide SORNs posted on the DOI SORN website.

There is a risk that individuals may not know how to seek access, redress or amendment of their records. Instructions on how to access or amend individual records maintained in DOI Privacy Act systems are provided in applicable DOI and Government-wide SORNs published in the *Federal Register* and posted on the DOI SORN website. Procedures for submitting requests for access to or amendment of records is also outlined in the DOI Privacy Act regulations and on the DOI Privacy Act Requests website. Individuals seeking redress may submit requests for correction through established procedures outlined in DOI Privacy Act regulations at 43 CFR

2.246 and in the applicable published SORN. The DOI Privacy and Civil Liberties web page also provides information on how individuals may submit a complaint or a request to correct erroneous information. However, DOI has exempted law enforcement and investigation records from one or more provisions of the Privacy Act under 5 U.S.C. 552a(j) and (k), in order to preclude an individual subject's access to and amendment of information or records related to or in support of an investigation. Individuals may also contact the appropriate DOI privacy officials for assistance or for questions, requests or complaints.

There is a risk that the DI-4016 and DI-4017 access and consent forms or any supporting information pertaining to the request could be lost or misplaced in the mail. This risk may be mitigated by individuals choosing to utilize certified mail or a courier service with tracking capability. Completed access and consent forms and supporting documents can be submitted directly to the Privacy Act System Manager identified in the applicable SORN or the APO at the DOI bureau or office where the records are located. DOI bureau and office APO contact information is available at https://www.doi.gov/privacy/contacts. Individuals may also choose to submit their Privacy Act requests electronically by using the DI-4016 and DI-4017 web forms posted on the DOI Privacy Act Requests page. Paper forms or responsive records processed will be sent to individual requesters via first class postal mail or courier service with tracking capability to mitigate risk of interception.

There is a risk that a Privacy Act request may be denied based on the submission of inaccurate information. All information is obtained directly from the individuals for identity proofing and locating records, so it is presumed to be complete and accurate when it is submitted by the individual. Any inaccurate information provided by the individuals may be corrected during review and processing with the individuals. Individuals may also seek amendment of any outdated or incorrect information about them by submitting a request to amend a record as outlined in DOI Privacy Act regulations and instructions on the DOI Privacy Act Requests page.

There is a risk that PII may be used outside the scope of the purpose for which it was collected. Privacy Act statements on the DI-4016 and DI-4017 forms describe the purpose for the information collection and how this information will be used. DOI will use PII information provided by requesters through the DI-4016 and DI-4017 forms to respond to and process Privacy Act requests as necessary and authorized under the Privacy Act and other laws and regulations. Information will be disclosed to System Managers, APOs, and other authorized DOI personnel with a need-to-know to perform their official duties to respond to the requests and in accordance with the applicable SORNs. All DOI personnel must complete initial and annual privacy awareness training and acknowledge DOI Rules of Behavior. Privacy personnel and System Managers and officials who process or support Privacy Act systems must also complete role-based privacy training annually to ensure ongoing awareness and understanding of their responsibilities for handling and safeguarding Privacy Act records.

There is a risk that forms or records may be maintained longer than necessary to achieve the DOI mission or that paper or electronic forms may not be properly destroyed. This risk is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. Users are reminded through policy and training that they must follow the applicable

retention schedules and requirements of the Federal Records Act, NARA guidelines, and Departmental policy. Authorized users undergo annual security and privacy awareness training, and records management training that specifically includes handling and disposal of sensitive information. The records retention schedule was also placed directly on the DI-4016 and DI-4017 forms to ensure proper retention and disposal.

There is a risk that unauthorized persons could potentially gain access to the PII on the forms or the website or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties. Access to administrative functions is strictly controlled and user authentication protocols are enforced based on the user's role and permissions, i.e., personal identity verification (PIV) cards, multi-factor authentication (MFA), and two step verification. Government employees, contractors, and partners (collectively, Government Users) will be required to use multi-factor authentication to access network resources. The web forms are hosted in the Drupal, the Department's web content management system. Completed forms will be transmitted to a controlled email account managed by the DOI Privacy Office within the Department's Microsoft Office 365 (O365) email system. The PII or submitted forms will be stored within the Department's secure O365 system and will not be stored or maintained in Drupal. The forms will be protected by access controls, Controlled Unclassified Information (CUI) markings, encryption, and other controls to protect the data. Paper records will be secured in locked cabinets in secure DOI facilities. Access to the completed paper and web forms will be limited to authorized users in the DOI Privacy Office who review incoming submissions and appropriate bureau or office APOs, officials and support staff to process, maintain and monitor requests to ensure timely response and compliance with the Privacy Act, OMB and Departmental policy. Transmissions of PII and forms will be encrypted with appropriate CUI marking and password protected as necessary to protect privacy. Users may view the DOI.gov/DOI Drupal Content Management System (CMS) and Microsoft Office 365 Cloud PIAs for additional information on associated privacy risks and safeguards for these DOI systems. All DOI personnel must complete initial and annual privacy, security, CUI, and records management awareness training, role-based training, and acknowledge DOI Rules of Behavior.

GSA provides the Login.gov service to all Federal agencies to verify and authenticate individuals requesting access to partner Federal agency applications, websites, and information. There are risks associated with the service for users who may not be properly identified and authenticated using the GSA Login.gov site. PII provided by requesters opting to use the Login.gov service will be used to verify the requester's asserted identity and authenticate them via Login.gov through a secure connection and return verification to DOI in order to process requests. The GSA Login.gov identity verification system currently does not meet the Identity Assurance Level 2 (IAL2) requirements as described in NIST Special Publication (SP) 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing*, and NIST Special Publication 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management* for identity proofing because it does not offer physical/remote identity proofing or biometric verification. However, Login.gov does provide strong identity assurance using an identity verification process that includes:

- Document authentication and records check – PII information submitted by users to Login.gov will shared with third-party proofing services to validate an individual's claimed identity. Users must create an account with their email, password and set up MFA. Login.gov requires the user to provide their state-issued ID, SSN, current address, and optionally a phone number to confirm home address. A user's PII data will also be matched with the user's self-asserted information and information collected from evidence against other records to establish their identity as authorized in the GSA/TTS-1 SORN.
- Address confirmation – Users will be required to verify their mailing address by completing an address confirmation form from the Government Publishing Office (GPO) or any other requested mailed notifications as authorized in the GSA/TTS-1 SORN.
- In person proofing – The United States Postal Service (USPS) will conduct an in-person identity document authentication to validate a user's claimed identity as authorized in the GSA/TTS-1 SORN.
- Fraud controls – Login.gov has implemented anti-fraud technologies embedded on the website to perform fraud checks on encrypted stored PII data. Login.gov will also monitor user activities within the system using behavioral biometrics. Please see the GSA Privacy Policy for Non-Federal Systems for details on how GSA prevents fraudulent activities on Login.gov.

There is a risk that PII information provided to DOI to process Privacy Act requests may be shared with GSA's Login.gov system. Completed DI-4016 and DI-4017 forms for Privacy Act requests submitted to DOI will not be shared with Login.gov or GSA. However, individuals choosing to create Login.gov user accounts must authorize sharing of their PII data with DOI in order to access services and information provided by DOI, and to allow DOI to recognize that user on future visits to the DOI Privacy Act website. Login.gov will use DOI branding at the sign in and account creation process to ensure the individual is aware their PII information may be disclosed to DOI. GSA developed the Login.gov PIA, which identifies and evaluates privacy risks due to the collection, use, storage and sharing of PII and safeguards employed to mitigate or manage these risks. GSA has published a SORN, GSA/TTS–1, Login.gov. Individuals using Login.gov for identity verification and authentication are subject to their Terms of Service and Privacy Policy. Login.gov users can amend or update their records submitted for identity verification and authentication or delete their Login.gov user accounts if they choose. Login.gov users may reach out to their contact center for assistance, if they have trouble signing into their accounts.

Individuals are not required to create Login.gov accounts or provide their PII to GSA to submit Privacy Act requests to DOI. Requesters have the option to download the DI-4016 and DI-4017 forms from the DOI Privacy Act Requests website, complete and sign forms with supporting documents and submit to the Privacy Act System Manager identified in the applicable SORN or the APO at the DOI bureau of office where the records are located. Requesters can also submit forms by mail to the DOI Privacy Office for processing.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The Privacy Act allows individuals to request access to their personal records maintained by a Federal agency subject to certain exemptions, and to seek correction or amendment of records that are inaccurate, incomplete, untimely, or irrelevant. The DI-4016 and DI-4017 forms are mandated by OMB M-21-04 and the CASES Act. DOI will use a requester's PII submitted through the forms to process Privacy Act requests and provide access to records, and additional PII provided will be used to verify the requester's asserted identity and authenticate them via Login.gov or other means.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

The DI-4016 and DI-4017 access and consent forms do not derive or create new data that was previously unavailable about an individual through data aggregation.

However, the GSA Login.gov system may aggregate data on users' device and behavior while using the system to detect and prevent identity impersonation or account takeover attempts. This information is maintained by GSA. Please refer to the Login.gov PIA for information on how user data is aggregated and used.

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

☐ Yes: *Explanation*
☒ No

The DI-4016 and DI-4017 access and consent forms and DOI Privacy Act website do not aggregate data. Information submitted using the DI-4016 and DI-4017 forms via the DOI Privacy website is used to process and respond to individual requests for Privacy Act records.

However, new user data derived by GSA through data aggregation may be placed on their Login.gov record. This information is maintained by GSA. Please refer to the Login.gov PIA to

determine if new user information derived from aggregated will be placed on an individual's record.

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

☐ Yes: *Explanation*
☒ No

Not applicable for DOI records. However, to support fraud investigations, Login.gov may re-identify a user by matching their assigned Universal Unique Identifier (UUID) including actions performed within the Login.gov system and each partner agency accessed by the user. Login.gov also maintains also de-identified account and transactional metadata for analytic and debugging purposes. Please see the Login.gov PIA for details the types of information collected from individuals and how this information is collected and used.

E. How will the new data be verified for relevance and accuracy?

Not Applicable. The DI-4016 and DI-4017 access and consent forms do not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

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

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Authorized access to completed DI-4016 and DI-4017 access and consent forms is based on least privilege and "need to know" principles. Access is controlled by assignment of roles and specific discrete authorizations and is limited to necessary access.

Access to Drupal CMS used in managing the DOI Privacy Act website is limited to authorized DOI personnel and is controlled through user account management and authentication with the DOI Active Directory system and DOI's centralized user account management process.

Information provided on electronic DI-4016 and DI-4017 forms is not shared with Login.gov or maintained in the Drupal CMS. Completed web forms are transmitted to a dedicated DOI Privacy Office email account within the DOI email system, which is restricted to authorized privacy personnel who have access to review and process requests. Requests submitted through the mail or in person will be restricted to authorized personnel within the organization receiving the request and will be routed to and process by the appropriate APO. Requests received by the Department for records maintained by a bureau or office will be referred to the bureau/office APO who is responsible for processing the request and for determining proper access to the records within their organizations. Access to these records is determined by the Departmental privacy officials and bureau/office APOs who will share information or records with System Managers, program officials, FOIA personnel, or support staff as necessary to facilitate their location and timely process and respond to requests.

GSA Login.gov privileged users may have access to view data supplied by individuals to GSA for their user accounts and for identification verification and authentication but cannot amend or delete PII data within a record. GSA does not have access to DI-4016 and DI-4017 forms or any supporting documents or associated records related to individual requests submitted to DOI.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are involved in the design, development and maintenance of the DOI Privacy Act Request website on the Drupal CMS platform. Privacy Act clauses are included in the contract and they are granted access as authorized users, however, the completed web forms are immediately transmitted to the DOI Privacy Office and are not maintained in Drupal.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The system and use of the access and consent forms support Privacy Act requests submitted by individuals and identifying and authenticating the requesting individual is a primary purpose, however, the system does not locate individuals beyond collecting address information to provide responsive records and does not monitor individuals. Drupal and the O365 email system utilize system audit logs. Audit logs are only accessible to privileged users with the appropriate system roles to monitor the audit logs for security purposes.

For GSA Login.gov, all user actions are logged and monitored including metrics that track and measure user behavior and engagement with the Login.gov system. Users who opt to utilize the GSA Login.gov service may view the Login.gov website policy and PIA for additional information.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The system and use of the access and consent forms do not have the capability to monitor individuals. PII will be shared with authorized DOI personnel such as Privacy Act Managers and APOs in order to track and respond to Privacy Act requests within statutory response timelines.

The Drupal CMS system used in creating and managing the DOI Privacy Act Request website does not monitor individuals.

For GSA Login.gov, all user actions are logged and monitored including metrics that track and measure user behavior and engagement with the Login.gov system. Users who opt to utilize the GSA Login.gov service may view the Login.gov website policy and PIA for additional information.

M. What controls will be used to prevent unauthorized monitoring?

Access to the access and consent forms is limited to authorized DOI personnel. Audit logs are only accessible to privileged users with the appropriate system roles to monitor the audit logs for security purposes. Personnel must complete annual security and privacy awareness training, role-based training, and acknowledge DOI Rules of Behavior. NIST SP 800-53, *Security and*

Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. The principle of least privilege is applied to ensure the Privacy Act Requests process operates at privilege levels no higher than necessary to accomplish organizational missions or business functions. Authorized personnel may include security administrators, system administrators, system security officers, system programmers, and other privileged users.

Also, embedded within the ROB is the warning banner which is displayed upon logging into any DOI computer system. The warning banner clearly states all agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. It further states, by logging into an agency computer system, the user acknowledges and consents to monitoring of this system. These security protocols help DOI monitor user actions for appropriate use and to mitigate the risk of unauthorized monitoring.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

The system inherits controls from Drupal CMS and O365, as well as Login.gov for identity proofing and authentication.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)

☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. *Describe*

The system inherits controls from Drupal CMS and O365, as well as Login.gov for identity proofing and authentication.

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☒ Other. *Describe*

The system inherits controls from Drupal CMS and O365, as well as login.gov for identity proofing and authentication.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Senior Agency Official for Privacy (SAOP) and Departmental Privacy Officer (DPO) have Department-wide responsibility for overseeing and managing the DOI Privacy Program, ensuring adequate safeguards are implemented to protect individual privacy, and processing Privacy Act requests for notification, access, and amendment, in collaboration with bureau and office APOs. APOs, System Managers, and other authorized personnel are responsible for protecting individual privacy for the information collected, maintained, processed, used and shared in the system for their respective organizations, and for timely processing requests or complaints received, and for meeting the requirements of the Privacy Act, DOI Privacy Act regulations and policy, and other Federal laws and policies.

GSA is responsible for the management of Login.gov and for protecting individual privacy for the information collected, maintained, used and transmitted by GSA for identity verification and authentication purposes, and for meeting the requirements of the Privacy Act.

P. 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 DPO has delegated responsibility from the SAOP for oversight and management of the Privacy Act Requests website and establishing procedures for Privacy Act requests, implementing security and privacy controls in coordination with APOs and security officials, and ensuring to the greatest possible extent that data is properly managed, and that all system access has been granted in a secure and auditable manner. All Departmental and bureau/office authorized users are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC, DOI's central incident reporting portal, within 1-hour of discovery in accordance with the DOI Privacy Breach Response Plan and Federal policy and procedures. The bureau/office APOs are responsible for ensuring appropriate remedial activities are taken to mitigate any impact to individuals resulting from a breach of PII in coordination with the DPO.

GSA is responsible for Login.gov and the management and security of PII data submitted by individuals for identity verification and authentication purposes and for reporting any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data that may impact DOI upon discovery in accordance with Federal policy and established procedures.