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 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: FOIAXpress
Bureau/Office: Office of the Secretary (OS)/Office of the Solicitor (SOL)
Date: August 29, 2024
Point of Contact
Name: Preston Griffin
Title: OS Associate Privacy Officer
Email: os_privacy@ios.doi.gov
Phone: 202-240-1464
Address: 1849 C Street NW, Washington, D.C. 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 Freedom of Information Act (FOIA), 5 U.S.C. § 552, and Privacy Act of 1974, 5 U.S.C. § 552a, as amended, provide means for the public to submit requests and obtain records of agency activities and access to individual records maintained by an agency, to ensure openness and transparency in all government agencies. A request where an individual is seeking only records about themselves is generally considered a Privacy Act request, while an individual or organization seeking information about other individuals or Department of the Interior (DOI, Department) business operations is generally considered a FOIA request. Requests for agency records may be processed under both the FOIA and Privacy Act as a combined request.

FOIAXpress is a third-party FedRAMP-authorized cloud-based tracking and management system that will assist DOI in managing the entire lifecycle of FOIA requests, combined FOIA/Privacy Act requests, and FOIA and Privacy Act appeal files. DOI will utilize FOIAXpress as its primary internal tool to aid the Department and its bureaus and offices in receiving and processing FOIA requests, communicating with requesters regarding their requests, providing status updates for requests, keeping track of payment information for requests that are charged a fee, providing access to account holders, and facilitating the dissemination of information to the public.

FOIAXpress uses a Public Access Link (PAL) add-on between FOIAXpress and Login.gov, a Federal service owned and operated by the General Services Administration (GSA). The FOIAXpress PAL is a secure public facing web portal that provides the public with a single access point for requestors to create individual user accounts, submit requests, access requested records, review request status based on tracking number and communicate with DOI. While the Departmental FOIA Office within the Office of the Solicitor (SOL) manages the FOIAXpress system, each bureau and office is responsible for managing its own records within the system. The GSA is responsible for managing user accounts created through Login.gov and providing authentication and identity verification for individual users who submit requests to DOI. Please refer to the GSA Login.gov privacy impact assessment (PIA) for information regarding privacy evaluation, which can be accessed at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

C. What is the legal authority?

5 U.S.C. 552, The Freedom of Information Act, as amended; 5 U.S.C. 552a, The Privacy Act of 1974, as amended; DOI FOIA Regulations, 43 CFR Part 2; and 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: Updates made to reflect personnel changes with new Acting Associate Privacy Officer and Information System Security Officer. Also, updated the Privacy Act Statement with the updated SORN.

E. Is this information system registered in the Governance, Risk, and Compliance platform?

☒ Yes:

UII Code: 010-000002752
System Security and Privacy Plan: FOIAXpress

☐ 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	None	No	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 FOIA Program records, including FOIA case files and records of appeals created and maintained across the Department, are covered by the Department-wide SORN, INTERIOR/DOI-71, Freedom of Information Act (FOIA) Files, 89 FR 25897 (April 12, 2024).

As appeals records are currently covered under the INTERIOR/DOI-71 SORN, a rescindment notice will be published for INTERIOR/OS-69, Freedom of Information Appeals Files, 64 FR 16986 (April 7, 1999); modification published at 86 FR 50156 (September 7, 2021).

Requests for records submitted under the Privacy Act by requesters will be referred to the DOI Privacy Program for processing. Privacy Act requests and complaints are maintained under INTERIOR/DOI-57, Privacy Act Files, 81 FR 45527 (July 14, 2016), modification published at 86 FR 50156 (September 7, 2021).

Responsive records may be obtained from other originating systems of records that are maintained under government-wide, Department-wide, or bureau/office SORNs, which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

GSA maintains records on individuals who utilize Login.gov and has published a SORN for the Login.gov system, GSA/TTS–1, Login.gov, 87 FR 70819 (November 21, 2022).

☐ No

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

☒ Yes: The FOIAXpress system does not require an OMB Control Number, however, DOI forms that may be used by individuals to request records under the Privacy Act are covered under OMB Control Number 1093-0013, DOI Access & Consent Forms; Expiration date: January 3, 2026.

- DI-4016, *Request for Individual Access to Records Protected under the Privacy Act*
- DI-4017, *Consent for Disclosure of Records Protected Under the Privacy Act*

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

The data collected and maintained within FOIAXpress may include personally identifiable information (PII) about individuals, such as their name, address, home telephone and fax numbers, and other pertinent information related to processing and responding to their FOIA requests. Users who create an account in order to submit and access FOIA requests through FOIAXpress must also provide name, email address, username, password, and answers to security questions. In order to access the account, the user must authenticate using multi-factor authentication (MFA), which may include a one-time password. Additionally, the system may include final determination letters and other documents related to the processing of FOIA requests. Letters, email messages, and responsive records may contain unredacted PII, which is most frequently encountered when the request pertains to the requester's personal information. Responsive records provided to the requester may contain the entire case file or redacted

documents if records are subject to exemptions. According to the scope of the request, case files may contain a significant quantity of information, including records from Privacy Act systems that contain PII of individuals, such as names used, physical address, email address, phone number, contact information, date of birth, Social Security number (SSN), work history, education history, personnel records, and other information pertaining to the records requested. Information may be of concern to employees if they have filed a FOIA request with one of the bureaus/offices in their individual capacity. FOIAXpress also monitors the user information of DOI employees who are either designated as FOIA personnel and, as such, necessitate access to the database to administer requests under the FOIA and Privacy Act, or who require access to the database to oversee the system.

In addition, DOI is leveraging GSA's Login.gov service to enable requesters to create user accounts to access FOIAXpress and to submit and manage requests for records, and to implement the Office of Management and Budget (OMB) Memorandum M-21-04, *Modernizing Access to and Consent of Disclosure of Records Subject to the Privacy Act,* which directs Federal agencies to "accept remote identity-proofing and authentication for the purpose of allowing an individual to request access to their records or to provide prior written consent authorizing disclosure of their records under the Privacy Act." With this connection, DOI can leverage the remote identity verification services conducted by Login.gov. Login.gov provides the same function to other Federal agencies who choose to utilize it, helping consolidate the identity verification process across Federal services and platforms. Once verified an automated message from Login.gov containing the requester's first and last name will be added to the FOIAXpress correspondence tab. Login.gov requires individuals to create a user account by providing a valid email address and creating a password. Login.gov also requires users to set up 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, 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. 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.

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: The information in FOIAXpress comes mainly from individuals who submit FOIA requests, internally generated documents, and users of FOIAXpress.

Individuals who opt to utilize Login.gov to authenticate their identity are required to furnish their information to GSA, who oversees Login.gov. GSA maintains this information as part of their service and only shares the PII necessary to provide authentication and identity proofing in order to protect privacy. At a minimum, a user's first and last name will be shared with DOI once their identity has been authenticated.

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

GSA Login.gov collects information directly from individuals when they create user accounts. When requesters choose to create Login.gov user accounts, Login.gov may share limited personal information with DOI as a partner agency.

☐ Other: *Describe*

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

PII will be used to manage individual accounts created by users who submit requests, provide requesters with access to requested records, process FOIA requests for records, facilitate communication with DOI about the status of a request, make fee determinations, and provide records in response to FOIA requests. The information collected in the FOIAXpress system is necessary in order to respond to requests for agency records directly related to the reason for which the system was designed.

Login.gov will use the requester's PII to verify their asserted identity and authenticate them via a secure connection and return verification to DOI to process the 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:

PII will be shared with authorized personnel within the Departmental FOIA Program within SOL and the appropriate bureau or office to locate records and process FOIA requests. Each bureau and office is granted access to their records stored in FOIAXpress and is solely responsible for

managing their own records. Only DOI personnel specifically authorized by the Bureau FOIA Officers will have access to FOIAXpress. The Department has established access levels and permission levels, which are only authorized to individuals who require access to the system's information to carry out their duties. In accordance with OMB Circulars A-123 and A-130, FOIAXpress has implemented measures to prevent unauthorized access to the data within the system. Security measures and controls encompass firewalls, passwords, FOIAXpress user identification, database permissions, and software controls.

☒ Other Bureaus/Offices:

As necessary, PII will be shared with authorized personnel within bureaus and offices to locate records and process FOIA requests. Access to FOIAXpress shall be granted solely to DOI personnel who have been specifically authorized by the Bureau FOIA Officers. The Department has established access levels and permission levels, which are only authorized to individuals who require access to the system's information to carry out their duties. In accordance with OMB Circulars A-123 and A-130, FOIAXpress has implemented measures to prevent unauthorized access to the data within the system. Firewalls, passwords, FOIAXpress user identification and database permissions are some of the security measures and controls.

☒ Other Federal Agencies:

Information may be shared with other Federal agencies to assist that agency in responding to an inquiry by the individual to whom that record pertains, or when an agency has a subject matter interest in a request or an appeal or a decision thereon. Information may also be shared with the National Archives and Records Administration, Office of Government Information Services (OGIS) to the extent necessary to fulfill its responsibilities in 5 U.S.C. 552(h), to review administrative agency policies, procedures, and compliance with the FOIA, and to facilitate OGIS' offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies. Other authorized routine uses are outlined in the applicable SORNs that cover the system, INTERIOR/DOI-71, Freedom of Information Act (FOIA) Files, and INTERIOR/DOI-57, Privacy Act Files.

☒ Tribal, State or Local Agencies:

Information may be shared with Tribal, state, or local agencies as authorized and outlined in the routine uses in the applicable SORNs, INTERIOR/DOI-71, Freedom of Information Act (FOIA) Files, and INTERIOR/DOI-57, Privacy Act Files.

☒ Contractor:

Information may be shared with contractors who support the administration of the system and for authorized purposes outlined in the routine uses in the applicable SORNs, INTERIOR/DOI-71, Freedom of Information Act (FOIA) Files, and INTERIOR/DOI-57, Privacy Act Files.

☒ Other Third-Party Sources:

Other third-party sources do not have direct access to FOIAXpress. Third party sources may include a log of FOIA requests, congressional offices responding to an inquiry, or a debt collection agency for the purpose of collecting outstanding debts owed to the Department for fees associated with processing FOIA/Privacy Act requests.

The Login.gov service provided by GSA may disclose personal information provided by members of the public to contracted third-party organizations for the purpose of identity verification and authentication. For further details on how PII data is shared with third party entities, please refer to the Login.gov PIA.

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.*

Individuals voluntarily choose to provide information when filing FOIA requests and may choose to not provide the information requested. However, it is imperative that individuals provide minimal contact information and individual identifying information to correspond with requests for records, make fee determinations, and furnish records in response to FOIA requests.

Individuals who are referred to Login.gov for authentication and identity proofing voluntarily consent to the sharing and use of their PII data 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.*

A Privacy Act statement is provided on the FOIAXpress PAL web page.

A Privacy Act statement is provided to users who submit the DOI forms, DI-4016, *Request for Individual Access to Records Protected under the Privacy Act*, or DI-4017, *Consent for Disclosure of Records Protected Under the Privacy Act*, that are processed as a combined request.

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

☒ Privacy Notice: *Describe each applicable format.*

A link to the DOI Privacy Policy is provided on the FOIAXpress webpage at https://foiaxpresspal.doi.gov/, which provides information to members of the public on information handling practices and links to the DOI Privacy Program webpage where individuals can review guidance on how to submit Privacy Act requests and complaints.

Privacy notice is also provided through the publication of this PIA and the published INTERIOR/DOI-71, Freedom of Information Act (FOIA) Files, and INTERIOR/DOI-57, Privacy Act Files, SORNs, which may be viewed on the DOI SORN page at https://www.doi.gov/privacy/sorn.

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.*

Users who choose not to use FOIAXpress are directed to FOIA.gov which is managed by the Department of Justice. A Privacy Act statement is posted on each DOI bureau and office page on FOIA.gov.

☐ None

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

Agencies may access requester specific information by requester name, organization, and tracking number.

I. Will reports be produced on individuals?

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

The reports enable FOIAXpress users to determine certain information regarding the requests submitted including types of requests, categories of requests, numbers of requests, dates pertinent to requests, and costs associated with the requests. FOIAXpress users will be able to

produce reports using various parameters, as discussed above, but PII in the reports is limited to the information that has been provided by the requester.

FOIAXpress maintains audit logs of user activity, including the users' access to and actions within the system. Audit logs are accessed by System Administrators.

☐ No

Section 3. Attributes of System Data

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

FOIAXpress allows the public to request copies of existing records managed by agencies. All data quality activities associated with the generation of the original records are applicable.

FOIAXpress provides controls, in the form of "review tasks," to help ensure the records are responsive to the request. Each bureau is responsible for applying their own rules to ensure the data are accurate.

DOI receives FOIA requests directly from the individual FOIA requesters and the accuracy of the information is only as reliable as that provided by the requester and inputted by FOIAXpress users. Inaccurate information may result in a delay or inability of the Department to process the FOIA and combined FOIA and PA requests.

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 access to 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?

Information is received directly from the individual FOIA requesters who must provide as much information as necessary to process their requests. The FOIAXpress is designed to require specific information be entered in order to consider the FOIA request complete. If the required information is not entered into the system, the FOIA request will not be saved by the FOIAXpress.

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 MFA 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).

Information in FOIAXpress is received directly from individual FOIA requesters and is only as current and reliable as that provided by the requester and inputted by the FOIAXpress users. 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.

Records are maintained under Departmental Records Schedule (DRS) 1-Administrative Records (DAA-0048-2013-0001) that cover FOIA and Privacy Act request files, correspondence, reports, and other program administration and financial management records, which has been approved by NARA. The disposition for these records is temporary and retention periods vary according to the specific record and the needs of the agency. FOIA request files and other short-term administration records are destroyed three years after cut-off, which is generally after the date of reply or the end of the fiscal year in which files are created. Long-term records that require additional retention, such as denials, are destroyed seven years after cut-off, which is generally when the record is closed. Paper records are disposed of by shredding or pulping, and records maintained on electronic media are degaussed or erased in accordance with 384 Departmental Manual-1 and NARA Guidelines. GSA is responsible for managing its Login.gov user account 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?

All records eligible for destruction will be detailed in an index and provided with the destruction request DI-1941 form for authorization by the bureau or office Responsible Records Officer before the data is purged from the system. Records in the system are disposed of under the approved disposition methods including shredding or pulping paper records and degaussing or erasing electronic records in accordance 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 are privacy risks to individuals due to the volume of PII and types of documents that are processed in response to FOIA requests. The primary privacy risks include unauthorized access, unauthorized disclosure, and misuse of the data in the system that may lead to potential harm such as identity theft, fraud, misuse, or exposure of sensitive information. Other risks include lack of adequate notice on what PII is collected or opportunity to consent on how it will be used, maintaining inaccurate information, data aggregation, collecting or maintaining more information than necessary to meet the needs of the program, and maintaining records longer than necessary. These risks are addressed and mitigated through a variety of administrative and logical security controls.

FOIAXpress is rated as a moderate system under the Federal Information Security Modernization Act of 2014 (FISMA) and requires management, operational, and technical controls per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 to mitigate privacy risks to individuals for the unauthorized access, disclosure, or misuse of PII. User access is granted only to authorized individuals by system administrators and FOIA Officers and users are granted access only to the case files needed in order to perform their job duties. Only authorized users are provided access to FOIAXpress using single sign-on and validated through the DOI Active Directory. Administrative access to FOIAXpress is granted only to authorized personnel on an official need-to-know basis. Unique administrator identification and authentication, least privileges and audit logs are utilized to ensure appropriate permissions and access levels.

All users of DOI network resources, including contractors, must consent to DOI Rules of Behavior and take annual end-user security, privacy, and records training in order to obtain access to any DOI network resource. Authorized users who support the system and access or process PII must also complete role-based privacy training annually to ensure an understanding of their roles and responsibilities for protecting privacy.

FOIAXpress has a hierarchical administration consisting of a System Administrator(s), and multiple FOIA Officer and Action Office Leads. The System Administrator is responsible for controlling and monitoring access to users who are given access to case files for their bureau or office. The System Administrator(s) and authorized employees are only granted access to documents and data in FOIAXpress to the extent it is necessary for the performance of their job duties.

Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized monitoring. In addition, firewalls and network security arrangements are built into the architecture of the system, and NIST guidelines and Departmental policies are implemented to

ensure system and data security. System administrators will review the activities of the users to ensure that the system is not improperly used, including for unauthorized monitoring.

Access is restricted to only those individuals authorized by System Administrators on a need-to-know basis in order to perform their job duties consistent with the purposes of the system. This includes limiting authorized individuals' access to selected repositories of documents and data within the system, such as the authorized individual's bureau or office. Limitations on access are maintained through role defined by the FOIAXpress Administrator and validated upon user login and authentication. If necessary, an audit log for FOIAXpress may be used to run reports on individual users' access to and actions within the system.

There is a risk that individuals may not have adequate notice regarding the collection of information, the purposes for collection or an opportunity to consent to how the information will be used. Notice is provided through the publication of this PIA, applicable SORNs, and related PIAs that apply to the original source documents. A Privacy Act statement is provided on the FOIAXpress PAL webpage where users register to create accounts that provides notice to individuals on the authorities, purpose of the collection, how information will be used and shared and the voluntary nature of the request. Users who choose not to use FOIAXpress are referred to FOIA.gov, a DOJ service, as an alternative which provides a Privacy Act statement on each DOI bureau and office request page. GSA also provides a Privacy Act statement on the Login.gov website and published the GSA Login.gov PIA, and Login.gov SORN.

There is a risk that data from different sources may be aggregated and may provide more information about an individual, or that the data may become outdated or inaccurate. Only the minimal amount of information needed to perform the functions of the system and FOIA program is collected and maintained. The system maintains case files that may include existing agency records that are responsive to FOIA requests, it does not create new records or make determinations about individuals based on the responsive records. The requests for agency records are submitted by individuals and organizations who must provide sufficient identifying information to verify identity and process requests. Individuals who create user accounts have access to monitor and update their account profiles and FOIA requests. The INTERIOR/DOI- 71 and INTERIOR/DOI-57 SORNs outline procedures for individuals to contact the System Manager to request amendment or correction of any record they believe is outdated or inaccurate. Individuals may also contact the appropriate Departmental, bureau or office privacy official for such requests by following the procedures outlined on the DOI Privacy Act Requests website at https://www.doi.gov/privacy/privacy-act-requests.

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, privacy, and records management awareness training that specifically includes handling and disposal of sensitive

information, as well as role-based privacy training. Also, there is a system alert when records are eligible for disposal based upon the records management schedule and needs of the agency.

There is a risk that data may not be appropriate to store or be adequately protected in a cloud service provider's (CSP) system, or that the vendor may not handle or store information appropriately according to DOI policy. As a FedRAMP authorized provider, the CSP will implement protections and controls to restrict access to DOI data by unauthorized parties and comply with the FISMA, Privacy Act of 1974, OMB policy, and NIST standards. The CSP does not share agency information in the information system with third-party vendors or other agencies or organizations unless explicitly authorized and to fulfill legal requirements.

There is a risk associated with use of Login.gov to authenticate and identify proof users. 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. GSA provides DOI with the individual's first and last name after the user is authenticated. The GSA Login.gov identity verification system is currently undergoing a third-party assessment for certification that the service meets the Identity Assurance Level 2 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 Login.gov provides strong identity assurance using an identity verification process that includes:

- Document authentication and records check – PII information submitted by users to Login.gov will be 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 or any other requested mailed notifications as authorized in the GSA/TTS-1 SORN.
- In person proofing – The United States Postal Service 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 process the requests may be shared with GSA's Login.gov system. DOI will not share information related to the request 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. 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.

To support fraud investigations, Login.gov may reidentify 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. The Login.gov PIA details the types of information collected from individuals and how this information is collected and used. The GSA Login.gov system may aggregate data on users' devices 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.

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:

The information collected in FOIAXpress is necessary and is directly related to the reason for which the system has been designed. Majority of the data elements are required to process requests for agency records pursuant to the FOIA and for preparation and submission of the FOIA Annual Report to Congress (5 U.S.C. 552(e)).

☐ 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

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

Not applicable. New data is not being created.

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*

Authorized FOIAXpress users include: FOIA officers and coordinators, system managers, attorneys and other employees of the department who have a "need to know" the information

contained in this system in order to carry out their duties. The System Administrator has access to the data in the system as necessary to carry out his/her responsibilities.

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

Access to DOI records in FOIAXpress will only be granted to those persons within the DOI and specifically authorized by the Bureau FOIA Officers. Access levels and permission levels have been established by the Department and authorized only to those persons who have a need to know the information contained in the system in order to carry out their duties.

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 information provided to DOI; however, GSA does not have access to the FOIAXpress system, 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?*

The FOIAXpress contract includes all of the IT Security, Privacy and Records clauses and terms and conditions required by both government-wide and DOI policy.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smartcards or Caller ID)?
Are there new technologies used to monitor activities of the individual in any way? Access logs may already be used to track the actions of users of a system. Describe any new software being used, such as keystroke monitoring.

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?
Most systems now provide the capability to identify and monitor individual's actions in a system (e.g., audit trail systems/ applications). For example, audit logs may record username, time and date of logon, files accessed, or other user actions. Check system security procedures for information to respond to this question.

☒ Yes. *Explanation*

FOIAXpress is not intended to monitor individuals. However, the system has the ability to audit usage of the system, including reviewable data concerning logins, including login time, to protect against unauthorized access or actions within the system. Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized monitoring. In addition, firewalls and network security arrangements are built into the architecture of the system, and NIST guidelines and Departmental policies are implemented to ensure system and data security. System administrators will review the activities of the users to ensure that the system is not improperly used, including for unauthorized monitoring.

☐ No

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

FOIAXpress is not intended to monitor individuals. However, the system has the ability to audit usage of the system, including use by authorized individuals and system administrators. Access to FOIAXpress must be approved by the system owner or designated representative before access can be granted. When active, the Action User Report has the capability to monitor individual user actions bounded by time limits. This includes reviewable data concerning actions within the system, including username, date and time of day a user accessed the system, uploading documents for review, creating overlay text used in the redaction of data under the FOIA. Audit trails are found in FOIAXpress where you can look at failed login attempts, password changes, time in software, as well as what the individual user does in the application.

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

FOIAXpress is a FISMA Moderate system with NIST 800-53 controls which are designed to prevent unauthorized access. The PII submitted to agencies is only accessible to the agency targeted to receive the request, and in some cases restricted to certain portions of the organization, and to system administrators that support agencies as needed. Agency user roles and responsibilities associated with the proper management of sensitive information are included in the rules of behavior for system users in order to remind agencies of their role to properly protect PII.

In accordance with OMB Circular A-123 and A-130, controls are in place to prevent unauthorized access to the date in the system. Security measures and controls consist of firewalls, passwords, user identification, database permissions and software controls. DOI personnel also complete annual security and privacy training, role-based training, and agree to rules of behavior.

Audit reports can be produced to review the actions of authorized system users to determine if their use of FOIAXpress and the data has been in accordance with all rules and procedures for the system. Only users with elevated rights can run audit reports. Statistical reports generated for system maintenance generally do not contain sensitive PII.

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*

(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*

(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*

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 FOIAXpress Information System Owner, Information System Security Officer, and Privacy Act System Managers share overall responsibility for protecting the privacy rights of individuals by developing guidelines and standards which must be followed and meeting the requirements of the Privacy Act and addressing Privacy Act requests and complaints in consultation with privacy officials. Bureau FOIA Officers are also responsible for ensuring the proper management of records and access controls for their area of responsibility.

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 FOIAXpress Information System Owner, Information System Security Officer, and Privacy Act System Managers share overall responsibility for protecting privacy, ensuring proper use of data in FOIAXpress, and reporting any loss, compromise or unauthorized access or disclosure of information to DOI-CIRC. DOI FOIA and privacy officers, coordinators and appropriate attorneys also share responsibility for protecting privacy and reporting any loss or compromise in accordance with Federal and DOI policy.

The CSP is responsible for reporting any potential security incident or data breach that may affect DOI data or the security of the system.

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.