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: FOIAonline
Date: August 7, 2020
Bureau/Office: Office of the Secretary (OS)/Office of the Solicitor
Point of Contact:
Name: Danna L. Mingo
Title: OS Associate Privacy Officer
Email: OS_Privacy@ios.doi.gov
Phone: (202) 208-3368
Address: 1849 C Street, NW, Room 7112, 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

B. What is the purpose of the system?

The Environmental Protection Agency (EPA) FOIAonline system is a multi-agency web-application that enables the public to submit FOIA requests to participating agencies, track the progress of an agency’s response to a request, search for information previously made available, and generate up-to-the-minute reports on FOIA processing. FOIAonline also is a workflow system and repository that enables partner agencies to receive, manage, track, and respond to FOIA requests, generate reports including the annual FOIA report that is submitted to the

Department of Justice, communicate with requestors, and manage their FOIA case files as electronic records.

The current Department of Interior (DOI) Electronic FOIA Tracking System (EFTS) will be decommissioned and all data within the records retention schedule will be migrated to the FOIAonline system. All records not migrated will be disposed of in accordance with the governing records retention schedule.

C. What is the legal authority?

5 U.S.C. 552, The Freedom of Information Act, as amended; and 5 U.S.C. 552a, The Privacy Act of 1974, as amended.

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:

E. Is this information system registered in CSAM?

☒ Yes:

The SSP Name: FOIAonline
CSAM ID: 2578
The UII Code: 010-000002752

☐ 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: DOI-71, Electronic FOIA Tracking System and FOIA Case Files, 81 FR 33544, May 26, 2016, which may be viewed at: https://www.govinfo.gov/content/pkg/FR-2016-05-26/html/2016-12541.htm. The SORN is currently being amended to address the migration to the FOIAonline system.

☐ No

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

☐ Yes:
☒ 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:

The DOI data within FOIAonline may contain personal information about individuals, e.g., home telephone and fax numbers, and other pertinent information related to processing and responding to their FOIA requests. The system may also include final determination letters and other documents related to the processing of FOIA requests. Information may concern employees if they have filed a FOIA request with one of the bureaus/offices in their individual capacity. It also tracks user information of DOI employees who: 1) are designated as FOIA personnel and, as such, require access to the database to administer the laws or 2) who require access to the database in order to administer it.

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:

Information in the FOIAonline comes primarily from the individuals who submit FOIA requests, internally-generated documents, and FOIAonline users.

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:
☐ Other:

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

Information collected in the FOIAonline system is necessary to respond to requests for agency records which is directly related to the reason for which the system has been designed.

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

☒ Within the Bureau/Office:

Access to FOIAonline will only be granted to DOI personnel 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. In accordance with OMB Circular A-123 and A-130, FOIAonline has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of firewalls, passwords, FOIAonline user identification, database permissions and software controls.

☒ Other Bureaus/Offices:

Access to FOIAonline will only be granted to DOI personnel 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. In accordance with OMB Circular A-123 and A-130, FOIAonline has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of firewalls, passwords, FOIAonline user identification, database permissions and software 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 DOI-71: Electronic FOIA Tracking System and FOIA Case Files, system of records notice, which may be viewed at: https://www.gpo.gov/fdsys/pkg/FR-2016-05-26/html/2016-12541.htm. The SORN is currently being amended to address the migration to the FOIAonline system.

☒ 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 DOI-71: Electronic FOIA Tracking System and FOIA Case Files, system of records notice, which may be viewed at: https://www.gpo.gov/fdsys/pkg/FR-2016-05-26/html/2016-12541.htm. The SORN is currently being amended to address the migration to the FOIAonline system.

☒ 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 DOI-71: Electronic FOIA Tracking System and FOIA Case Files, system of records notice, which may be viewed at: https://www.gpo.gov/fdsys/pkg/FR-2016-05-26/html/2016-12541.htm. The SORN is currently being amended to address the migration to the FOIAonline system.

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

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

☒ Yes:

Individuals voluntarily choose to provide information when filing FOIA requests and may choose to not provide the information requested. However, individuals must provide minimum contact information and individual identifying information in order to correspond on requests for records, make fee determinations, and provide records in response to FOIA requests.

☐ No:

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

☒ Privacy Act Statement:

A Privacy Act Statement will be developed and placed on the Agency Selection screen within FOIAonline.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice for FOIAonline can be reviewed at:
https://FOIAonline.gov/FOIAonline/action/public/privacy

Privacy notice is also provided through the publication of this privacy impact assessment and the published DOI-71: Electronic FOIA Tracking System and FOIA Case Files system of records notice, which may be viewed at https://www.govinfo.gov/content/pkg/FR-2016-05-26/html/2016-12541.htm The SORN is currently being amended to address the migration to the FOIAonline system.

☐ Other:

☐ 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, tracking number.

I. Will reports be produced on individuals?

☒ Yes:

The reports enable FOIAonline 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. FOIAonline 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.

☐ No

Section 3. Attributes of System Data

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

FOIAonline 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. FOIAonline provides controls, in the form of “review tasks,” to help ensure the records are responsive to the request. Each agency is responsible for applying their own rules to ensure the data are accurate.

The Department of the Interior receives FOIA requests from the individual FOIA requesters and the information is only as reliable as that provided by the requester and inputted by FOIAonline users.

B. **How will data be checked for completeness?**

The FOIAonline 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 FOIAonline.

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

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

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 which is approved by the National Archives and Records Administration (NARA). FOIA request files, correspondence, responses, reports, and other data in the system are cut off when the response has been generated or denied. Records should be purged from the system by the DOI data custodian 7 years after cutoff, in accordance with the DAA-0048-2013-0001-0002, Long Term Administration Records.

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 form DI-1941 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 in accordance with DOI Records Schedules.

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 risk to individual privacy due to the personal information collected and maintained in FOIAonline. These risks are mitigated through administrative, physical and technical controls that have been implemented to protect the confidentiality, integrity and availability of the information. FOIAonline is hosted on the EPA website with secure connections (HTTPS) to protect interactions and the personal information provided by individuals. Information is collected directly from the individual and the provision of information required to submit a FOIA request is voluntary. Privacy notice is provided to individuals through a Privacy Act statement that will be posted within the Agency Selection section of the FOIAonline system, the publication of the DOI-71 system of records notice, the DOI Privacy Policy, and this privacy impact assessment.

FOIAonline is rated as a FISMA moderate system and requires management, operational, and technical controls per NIST SP 800-53 to mitigate the privacy risks for the unauthorized access, disclosure, or misuse of PII. Access to FOIAonline is limited to authorized FOIAonline users within the Department during the collection, use, retention, processing, disclosure, and destruction of information. The FOIAonline system is protected by both physical and electronic means, in order to protect individual privacy and mitigate privacy risks.

Electronic records are maintained in accordance with the Office of Management and Budget and Departmental guidelines reflecting the implementation of the Federal Information Security Modernization Act of 2014 and the Privacy Act. Electronic data is protected through user identification, passwords, database permissions and software controls, and different access levels are established for different types of users. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior.

Privacy risks and mitigation for the FOIAonline system have been documented in EPA's Privacy Impact Assessment and it can be reviewed at: https://www.epa.gov/sites/production/files/2020-01/documents/foiaonline-pia-npp_final.pdf

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 information collected in FOIAonline is necessary and is directly related to the reason for which the system has been designed. The majority of the data elements are required 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:

☒ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ 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.

FOIAonline consolidates the information provided by requesters and FOIAonline users for the express purpose of providing computerized reports. Controls are discussed in more detail below.

☒ Yes, processes are being consolidated.

FOIAonline is designed to protect data fields once the FOIA request has been completed. Additionally, access to the FOIAonline 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. In accordance with OMB Circular A-123 and A-130, FOIAonline controls in place to prevent unauthorized access to the date in the system. Security measures and controls consist of firewalls, passwords, FOIAonline user identification, database permissions and software controls.

☐ 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:

FOIAonline 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. The routine use section of the DOI-71 system of the records notice identities other parties that may gain access to the information when the use is compatible with that identified in the notice. Disclosure and access to information in the system is based on DOI FOIA and Privacy Act regulation at 43 CFR Part 2.

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

Per EPA's FOIAonline Privacy Impact Assessment access controls are described in user manuals and emphasized during training. Access to DOI records in FOIAonline 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.

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

☐ 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.

☒ No

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

☐ Yes.

☒ No

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

Not Applicable.

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

FOIAonline is a FISMA Moderate system with NIST 800-53r4 controls which are designed to decrease 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. Interagency agreements include agency user roles and responsibilities associated with the proper management of sensitive information, including rules of behavior as a system user, 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 data 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 and agree to rules of behavior. Audit logs are used to monitor unauthorized activities.

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 FOIAonline Information System Owner, Information System Security Officer, and Privacy Act System Manager 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. 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 FOIAonline Information System Owner, Information System Security Officer, and Privacy Act System Manager share overall responsibility for protecting privacy, ensuring proper use of data in FOIAonline, 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.