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: Electronic FOIA Tracking System (EFTS)
Bureau/Office: Office of the Secretary
Date: October 2, 2017
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 Electronic FOIA Tracking System (EFTS) is a major application that facilitates the manageability and efficiency of the Freedom of Information Act (FOIA) and Privacy Act (PA) process throughout the Department of the Interior (DOI). The EFTS allows tracking of FOIA/PA requests from receipt to completion; provides valuable information to DOI FOIA coordinators; identifies duplicate requests; ensures consistency in responses; reduces the time in processing requests; supports action on FOIA requests, appeals and litigation; facilitates reporting and reviews; and improves customer service.

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: *Describe*

E. Is this information system registered in CSAM?

☒Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

The UII code is 010-000000318. The Electronic Freedom of Information Tracking System SSP is being updated to reflect the title "Electronic FOIA Tracking System" to ensure consistency with DOI FOIA policy and program activities.

☐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-71, Electronic FOIA Tracking System and FOIA Case Files, 81 FR 33544, May 26, 2016, which may be viewed at: https://www.gpo.gov/fdsys/pkg/FR-2016-05-26/html/2016-12541.htm.

☐No

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

Information collection requirements are currently under review by the DOI Information Clearance Officer and Office of the Solicitor. This PIA will be updated if a determination is made that OMB approval is required for the DOI FOIA form in accordance with the Paperwork Reduction Act.

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 EFTS contains personal information about individuals, e.g., home telephone and fax numbers, and other pertinent information related to processing and responding to their FOIA and Privacy Act requests. This 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/PA request with the DOI or one of the bureaus/offices in their individual capacity. It also tracks user information of DOI employees who are designated as FOIA/Privacy Act personnel and, as such, require access to the database to administer the laws or DOI employees 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: *Describe*

Information in the EFTS comes primarily from the individuals who submit FOIA/PA requests, internally-generated documents, and EFTS 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: *Describe*

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

Information collected in the EFTS is necessary to respond to requests for agency records and locate 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: *Describe the bureau/office and how the data will be used.*

Access to the EFTS 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, the EFTS has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of firewalls, passwords, EFTS user identification, database permissions and software controls.

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

Access to the EFTS 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, the EFTS has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of firewalls, passwords, EFTS user identification, database permissions and software controls.

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

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.

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

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.

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

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.

☐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: *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 or PA 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 and PA requests.

☐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.*

The DOI FOIA request form contains a Privacy Act statement that advises individuals of the purpose and uses of the information requested. Individuals have opportunities to grant consent to the collection and uses of their information at the time they complete and submit a FOIA request form, which may be viewed on the DOI FOIA website at: https://www.doi.gov/foia/foia-request-form.

☒Privacy Notice: *Describe each applicable format.*

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.gpo.gov/fdsys/pkg/FR-2016-05-26/html/2016-12541.htm.

☐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.).

Data in the EFTS may be retrieved by various fields including, name of the requester, date of the request, subject of request, FOIA number, the organizational affiliation of the requester, etc.

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 EFTS users to determine certain information regarding the requests submitted including types of requests, categories of requests, numbers of requests, dates pertinent to requests cost associated with the requests, etc. EFTS 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?

Data in the EFTS is received from the individual FOIA/PA requesters and is only as reliable as that provided by the requester and inputted by EFTS users.

B. How will data be checked for completeness?

The EFTS is designed to require specific information be entered in order to consider the FOIA/PA request complete. If the required information is not entered into the system, the FOIA/PA request will not be saved by the EFTS.

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

Information in the EFTS is received from individual FOIA/PA requesters and is only as reliable as that provided by the requester and inputted by the EFTS 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 for FOIA and Privacy Act request files, correspondence, reports, and other program administration and financial management records, which is approved by the National Archives and Records Administration (NARA)(DAA-0048-2013-0001). 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. Records not covered by DRS-1 are maintained under General Records Schedule 4.2: Information Access and Protection Records (DAA-GRS-2013-0007).

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

Procedures for disposition of the EFTS data are in accordance with NARA guidelines. Records in the system are disposed of in accordance with DOI Records Schedules and approved Departmental disposition methods outlined in 384 DM 1.

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 the EFTS. These risks are mitigated through administrative, physical and technical controls that have been implemented to protect the confidentiality, integrity and availability of the information. The DOI FOIA web form is hosted on the DOI.gov 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/PA request is voluntary. Privacy notice is provided to individuals through a Privacy Act statement posted on the DOI FOIA form, the publication of the DOI-71 system of records notice, the DOI Privacy Policy, and this privacy impact assessment.

EFTS 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 the EFTS is limited to authorized EFTS users within the Department during the collection, use, retention, processing, disclosure, and destruction of information. The EFTS is protected by both physical and electronic means, in order to protect individual privacy and mitigate privacy risks. Computer servers in which electronic records are stored are located in secured DOI facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI network and information assets.

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.

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 the EFTS 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: *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.*

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

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

The EFTS is designed to protect data fields once the FOIA/PA request has been completed. Additionally, access to the EFTS 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, the EFTS has controls in place to prevent unauthorized access to the date in the system. Security measures and controls consist of firewalls, passwords, EFTS 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: *Describe*

EFTS users include: FOIA/PA 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?

Access to the EFTS data by a EFTS user (i.e., DOI employees who are designated as FOIA/Privacy Act personnel and, as such, require access to the database, or DOI employees who require access to the database in order to administer it) is determined by the "need-to-know" requirements of the Privacy Act, the EFTS user's profile based on the EFTS user's job requirements, managerial decisions, etc. and is

dependent on a compatible purpose for which the data was collected. The criteria, procedures, controls and responsibilities regarding access are documented in the business rules and guidelines and rules of behavior and comply with the intent of the Federal Information Security Modernization Act of 2014 for standards and guidelines on security and privacy. Electronic data is protected through user identification, passwords database permissions and software controls. Such security measures establish different access levels for different types of EFTS users. For example, in the EFTS, system administrators may have access to all of the data for their specific bureau or office.

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 were involved with the design and development of the EFTS, but are not involved in the maintenance of the system. A Privacy Act clause was included as part of the statement of work and the contractor was provided with copies of the Department's Privacy Act regulations and applicable policies.

☐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*
☒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?

The EFTS is only accessible by those authorized DOI employees who have been assigned usernames and passwords and whose IP address has been configured for server and application access. The following controls will be used to prevent unauthorized monitoring:

- Network Intrusion Detection System
- Host Space Intrusion Detection System
- Firewalls

- User Authentication by user name, password and IP address

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 EFTS 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.

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