United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)

(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.

All entries must be Times New Roman, 12pt, and start on the next line.

If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: FOIA CMS	**System Owner:** Timothy Epp
Preparer: Antonio Haskins	**Office:** OGC-RMO
Date: 4/30/2024	**Phone:** 202-564-2433
Reason for Submittal: New PIA__X__ Revised PIA_____ Annual Review_____ Rescindment _____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☒	
Operation & Maintenance ☐ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

FOIA Express is an EPA use web-application that enables the public to submit FOIA requests, track the progress of the EPA's response to a request, search for information previously made available, and generate reports on FOIA processing. FOIA Express allows EPA staff 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 requesters, and manage their FOIA case files as electronic records.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

Freedom of Information Act (5 U.S.C. § 552)

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

The system has a security plan and will be issued an authorization to operate.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No information collection review required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

The application will be provided to EPA by AINS (Now OPEXUS) under a SaaS model within a FEDRamp moderate environment.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

A copy of each Freedom of Information Act (FOIA) request received by the EPA and a copy of all correspondence related to the request, including an individuals' names, mailing addresses, e-mail addresses, phone numbers, and in some cases social security numbers, dates of birth, alias(es) used by the requester, alien numbers assigned to traveler's crossing national borders, requesters' parents' names, FOIA tracking numbers, dates requests are submitted and received, related appeals and agency responses. Records also include communications with requesters, internal FOIA administration documents (e.g., billing invoices) and responsive records.

2.2 What are the sources of the information and how is the information collected for the system?

FOIA requesters provide the information necessary to enable an agency to understand the records of interest and how to deliver the records requested. The agency in turn supplies correspondence and responsive records.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

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

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

PII is collected and stored by FOIA Express to process requests and FOIA appeals. EPA specifies the data required from requesters to process requests effectively in their FOIA regulations. Examples of this type of information are listed in section 2.1 and which could be misused creating financial or personally sensitive impacts to the owner of the associated information.

Mitigation:

FOIA Express is a FISMA Moderate system in compliance with applicable NIST controls which

are designed to decrease unauthorized access. The PII submitted to EPA is only accessible to specifically authorized employees of the agency and to system administrators as needed.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes—the system has multiple roles with decreasing levels of permissions which are assigned to individual accounts through a process managed by the system owner.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

The system includes account management procedures which assigns controls based upon role, request type and assigned group.

3.3 Are there other components with assigned roles and responsibilities within the system?

This is delivered under a SaaS model so other roles may exist for the administration of the application and potential use of the service provider.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Specifically authorized staff within the EPA will have access to data/information in the system. System administrators with the SaaS hosting company would also have access to data. Contractors have the appropriate FAR clauses included in their contract.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Information is retained under schedules 1049 and 0030.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

Records may be retained beyond their associated records retention schedule.

Mitigation:

The FOIA Express provides a records management module, which provides a process for record identification, validation, and deletion of closed request files to be automatically through the application. Staff must review and evaluate records before they are either retained or deleted from the application. Retained records are managed under the appropriate records schedule.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Information may share with the general public as a part of the FOIA process. Other information retained by the FOIA Express is not shared outside of EPA.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency.

How were those risks mitigated?

Privacy Risk:

Inappropriate release of non-public FOIA information.

Mitigation:

The FOIA CMS provides configurable levels of review prior to release of records. The system restricts access to information by default and maintains an audit trail of system actions.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

Information is restricted by default to only authorized EPA staff members determined to have a need to access by processes established by the system owner. Individually authorized users undergo annual security and privacy training and are subject to audits based on user account. The EPA implementation of the application is reviewed by a third party annually through a formal security assessment and requires an ATO issued by the CIO for continued operation. FOIAXpress is a FedRAMP authorized application and is required to maintain this certification.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

EPA requires and provides mandatory annual training for all employees related to the Privacy Act and the correct use of Agency information. Completion of this training is centrally tracked. Administrators are required to do enhanced training as required by EPA and support contractors are also required to complete training of the same complexity.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

The required information privacy controls may not be implemented fully or correctly.

Mitigation:

Continuous monitoring has been implemented and annual security assessments are conducted to ensure compliance with all privacy requirements. Applicable NIST AR controls are additionally required such as privacy monitoring and reporting, system design with privacy as a requirement, ongoing training for all system users including contractors on privacy requirements and mandatory reporting of privacy

impacting incidents.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

PII is collected for the EPA by FOIA Express to process FOIA requests and FOIA appeals. EPA specifies the data required from requesters to process requests in accordance with EPA FOIA regulations.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X_____No___. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

Authorized EPA staff may access requester specific information by requester name, and/or FOIA tracking number.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

[The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.]

Access to the system is limited to specifically authorized EPA staff with access granted under the principle of least privilege based on job responsibilities. At present, no evaluation has been conducted.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Unauthorized access or public release of PII information can pose adverse financial and personal impacts to the individuals affected and to the EPA.

Mitigation:

All communication flows are encrypted in transit and at rest. Access to non-public information is limited to authorized EPA staff.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

This application is used to process inquiries which are originated external to the EPA and are not directly solicited by the EPA. Prior to submission, an application warning banner aligning with NIST standards, Security Control AC-8, within SP 800-53 Revision 5, is displayed and must be agreed to by the submitter. This banner details how the information will be retained and used by the Agency. Additionally, this application has a published SORN available for public review.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

Prior to submission, an application warning banner aligning with NIST standards, Security Control AC-8, within SP 800-53 Revision 5, is displayed and must be agreed to by the submitter. This banner details how the information will be retained and used by the Agency. Additionally, this application has a published SORN available for public review. The FOIA process required that information be retained by the government for use in processing the request.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

People may not be aware that they are submitting PII information to the government via a system.

Mitigation:

The EPA provides customized instructions to public users, including alternative means to submit FOIA requests. Public users also must affirm that are informed and agree with the system's Privacy and Security Notices prior to submitting a request.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

The unauthorized release of personal identifiable information.

Mitigation:

There are appropriate procedures in place to address corrections. Credit report monitoring is also provided.