

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: FOIAonline	System Owner: Brian K Thompson
Preparer: Tim Crawford	Office: OMS/OEIP
Date: January 05, 2020	Phone: 202-566-0690
Reason for Submittal: New PIA ____ Revised PIA ____ Annual Review __X__ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input checked="" type="checkbox"/>	
Operation & Maintenance <input type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u>	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</u>	

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

FOIAonline 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.

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 USC 552b

- 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 completed and has or will be issued an authorization to operate. The ATO expires 2/7/2022

- 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 ICR 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?**

Yes, and data are stored in the Amazon Cloud that is FedRamp approved. The use of the cloud is IaaS.

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 traveller's crossing national borders, requesters' parents' names, user names and passwords for registered users, 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. An individual's financial account information is not collected or maintained in FOIAonline.

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 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.

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 by FOIAonline to process FOIA requests and FOIA appeals.

Agencies specify the data they require from requesters to process requests effectively

in their FOIA regulations. In some cases, agencies request very specific information to be able to access records requested. 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:

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.

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 6 roles with decreasing levels of permissions. The system also has a section in each casefile where records can be uploaded and access is restricted to only users within the same organization.

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

Access controls are contained in user manuals and emphasized during training.

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

FOIAonline includes a division of duties and functions by role. These include System Administrators, Agency Administrators and Account Administrators.

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?

No,-in order to provide support and assistance, system administrators and help desk operators have access to agency information. Each follows the applicable NIST and EPA information management requirements identified in the system security plan and associated controls that are applicable for systems containing sensitive information (e.g., NIST 800-53r4)...

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.

Yes: Records Control Number 0263, which has a corresponding retention period of six (6) years. Any cases under litigation are not eligible for destruction until the litigation has been removed.

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:

The System does not auto delete information. Information may be retained in the system for longer or shorter than the corresponding record retention schedule

Mitigation:

The system owner does not own the information. Partner agencies are responsible for management of retained information. The system allows agency users the ability to run reports for the disposition of records and take appropriate action based on the record 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.

External Information management is the responsibility of the information owner, or partner

agency.

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

External sharing is central to the purpose of Regulations.gov, which is intended to provide the public with one-stop access to rules and notices, supporting docket content, search capabilities, and the ability to comment on rules and notices published in the Federal Register.

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?

All dissemination and management of information is the sole responsibility of the partner agency and not EPA. Yes, the system has MOUs with each partner agency that is updated annually. The following is a portion of the security language included in MOU's with agencies that are agreed to and renewed annually, "All users must take steps to protect all transferred and stored data in accordance with the Privacy Act (5 U.S.C. § 552a), the Trade Secrets Act (18 U.S.C. § 1905), and the Unauthorized Access Act (18 U.S.C. §§ 2701 and 2710)." In the event of a system security incident, such as a successful system intrusion resulting in a data breach, EPA will follow reporting guidelines issued by OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information and as reflected in EPA's *Procedure for Responding to Breaches of Personally Identifiable Information* (EPA Classification Number: CIO 2151-P-02.2).

4.4 Does the agreement place limitations on re-dissemination?

All dissemination and management of information is the sole responsibility of the partner agency and not EPA (See above example language included in agency agreements.)

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:

A partner agency may mismanage information.

Mitigation:

The system provides configurable levels of review prior to release of records. Records marked for release to the public are color coded to help agency users more easily identify which records are marked for release. The system also restricts access to information, as well as tracks 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?

System users cannot see information submitted to another agency unless that agency has made it available to the general public. The information that can be made available is limited to the requester's name, organization or affiliation if one exists, description of the request, supporting materials and responsive records. Requester contact information is not available to the public unless it is contained within these items.

Within the agency that received the request, the system has the ability to "wall off" access by organization to ensure sensitive information is only accessed by those system users within that organization that loaded the information.

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

Each agency is responsible for the training of their employees in terms of proper access, management and protection of PII. The Interagency Agreement with agencies includes their

responsibility to provide this training to FOIAonline system users.

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.

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 by FOIAonline to process FOIA requests and FOIA appeals. Agencies specify the data they require from requesters to process requests effectively in their 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.)*

Agencies may access requester specific information by requester name, organization, tracking number, and based on a future implementation, SSN for a particular organization within the Social Security Administration.

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.]

FOIAonline does not determine what type of information each of its partner agencies require from the public to submit requests. The personal information that is collected intentionally from requesters is based on the particular agency's policies and procedures where the request is being directed. Each partner agency is then responsible for the receipt and management of that information and as well as evaluating the business or programmatic requirement to collect that information and any associated risk to continue to do so.

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.

Mitigation:

All communication flows are encrypted. Access to information is limited to authorized account holders

***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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

Requesters have the option of not submitting a request through the system by following alternative methods of submission provided in each agencies FOIA regulations. This can include mailing request to an agency using postal address. For convenience, agencies can include a link to their regulations in the instructions of their FOIAonline web form.

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:

Partner agencies provide customized instructions to public users, some of which include alternative means to submit FOIA requests. Public users also have to affirm they 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:

None. There is appropriate procedure in place to address all request related to redress.

Mitigation:

None