

PRIVACY IMPACT ASSESSMENT

(Rev. 07/2018)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Brooks, Patricia at brooks.patricia@epa.gov or (202) 564-3717.

System Name: EPA Public Access-Internet Operations and Maintenance and Enhancements (IOME)

Preparer: Michael Hessling

Office: OMS/OIM/WCSD

Date: 29 Jan 2019

Phone: 202-566-0441

Reason for Submittal: New PIA Revised PIA Annual Review X 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:

EPA's Internet Operations, Maintenance, and Enhancements (IOME) is a cluster of Apache web servers, loosely known as buckeye, that powers www3.epa.gov, archive.epa.gov, and snapshot.epa.gov. IOME used to be the primary public interface for providing public access to environmental information, but now serves as repository for content that cannot be moved into other applications (like Drupal WebCMS).

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?

- Federal Information Security Modernization Act of 2014 (Pub. L. 113-283);
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," revised, July 26, 2016;
- DHS Management Directive MD 140-01, "Information Technology Systems Security," July 31, 2007;

- National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, "Minimum Security Requirements for Federal Information and Information Systems," August 2013; and
- Homeland Security Presidential Directive 12 (HSPD-12), "LincPass", August 12, 2004
- NIST Special Publications (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.
- Additional programmatic authorities may apply to maintenance of the credential.

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?

Yes, and it can be found in the Agency's security document repository, Xacta 360. May 6, 2019

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 is 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?

No.

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).

The system does not collect names or other PII from the public. It is purely a static repository of environmental information. The information given to the public is collectively written by EPA staff and subject matter experts. There is voluntary submission of Names and email addresses when submitting comments or requests for information.

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

The information sources are obtained by EPA subject matter experts and posted on [www3](#), [archive](#), and [snapshot](#). From the public comment and contact us links.

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.

EPA staff is responsible for the accuracy of the information posted. Any information submitted by public via comments or contact-us is voluntarily submitted and data accuracy cannot be verified for accuracy.

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:

None. These are publicly accessible websites.

Mitigation: N/A

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?

This is a public website. There is no system, database, or application to access.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

N/A

3.3 Are there other components with assigned roles and responsibilities within the system? NO

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?

Yes, the FAR is complied with, recognizing that there is no sensitive PII contained in the system.

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.

N/A. While the Website itself is subject to Schedule 95, the voluntarily submitted email addresses do not appear on Web pages.

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:

None

Mitigation:

N/A

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.

No

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:

None

Mitigation:

N/A

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 in accordance with stated practices in this PIA?

There is no PII collected or stored on the website and no system to contain this information.

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

The agency's annual mandatory training requirements, e.g., security awareness, ethics, privacy, and FOIA.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: None

Mitigation: N/A

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.

N/A.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ 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.)

No. There is no system or data to retrieve.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

None

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:

None

Mitigation:

N/A

*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.

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?

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:

Mitigation:

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?

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

8.3 How does the system notify individuals about the procedures for correcting their information?

8.4 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:

Mitigation: