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: EPA Action Management System (EAMS)	
Preparer: Caryn Muellerleile	**Office:** OA/OP/ORPM/RMD
Date: 9/29/2021	**Phone:** (202) 564-2855
Reason for Submittal: New PIA____ Revised PIA____ Annual Review_X__ Rescindment ____	
This system is in the following life cycle stage(s): Implementation	
Definition ☐ Development/Acquisition ☐ Implementation X	
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:

The EPA Action Management System (EAMS) is a user-friendly application to collect and display data about agency regulatory activity. It will support approval workflows, simplify reporting required across the agency, and facilitate an internal, paperless regulatory process. This new system is replacing all critical and major business processes used in the legacy Lotus Notes applications.

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?

Authorizing EPA statutes, such as Clean Air Act and Clean Water Act; Administrative Procedure Act (APA; 5 U.S.C. 500 et. seq.); Federal Register Act (44 U.S.C. 1501 et.

seq.); Regulatory Flexibility Act (5 U.S.C. 602); Executive Order 12866 (58 FR 51735, 10/4/1993).

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?

SSP is completed and uploaded into XACTA; the ATO was granted on 8/28/2019 and will expire 10/1/2022.

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.

1.4 No information collection (ICR) is required for the EAMS system. **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, EAMS data will be maintained at the National Computing Center (NCC) on secured servers.

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).

Data information the EAMS system contains: Regulatory Information Number (RIN), Docket Number(s), EPA staff listed as points of contacts on rulemakings. Staff information kept includes First/Last name, Office Location, Office Telephone Number, Office Email.

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

EAMS information is collected and maintained by EPA staff. Information about EPA staff is generated from EPA's Active Directory within Microsoft O365.

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 information in the EAMS system is generated from a commercial or public source. The data created and maintained is internal to the federal government.

2.4 Discuss how accuracy of the data is ensured.

The EAMS system will have the capacity to generate reports for EPA staff to verify accuracy of data for an internal audience.

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. The PII contained in the system is already public.

Mitigation:

None.

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, EAMS has control levels in place to prevent unnecessary access and allows assigned system users to do their job. All EPA federal employees will have read-only access to this internal system. EAMS inherits access control procedures from EPA common controls, as detailed in the System Security Plan (SSP).

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

As outlined in the SSP in XACTA, the System Administrator in OA\OP (Office of the Administrator, Office of Policy) assigns each EAMS user a role, which determines what type of data they can access and edit. Individual user access to EAMS is managed according steps defined in the EAMS Governance Procedures section 6.i. Access Control.

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

Yes, various internal roles provide different levels of access and approval within the system. These procedures ensure proper role assignment and the system provides access limited by roles according to least privilege.

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?

Internal parties are EPA employees and external parties are only IT contractors who conduct

development and O&M (operations and maintenance) on the system. All contractors must follow FAR clauses applicable to the Privacy Act.

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.

The EAMS database falls under Records Control Schedule (RSC) 0089 -
"Close when no longer needed for current agency business. Destroy immediately after file closure."

.

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:

There is a low risk with retention of data beyond the appropriate Records Schedule.

Mitigation:

This risk is mitigated by following the Records Schedule appropriately.

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.

There is no external sharing.

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

None applicable.

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?

None applicable.

4.4 Does the agreement place limitations on re-dissemination?

None applicable.

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. EPA does not provide external sharing.

Mitigation:

None.

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 (Section 6.1)?

EAMS contains audit logs to display system usage. Data audit logs are regularly reviewed to ensure information are used for the intended purpose of collection.

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

EPA's annual information security and privacy training are provided to and required for all users.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of inappropriate audit to account for all PII usage in the system.

Mitigation:

Audit logs are frequently reviewed.

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.

The Office of Regulatory Policy and Management (ORPM) within EPA's Office of Policy (OP) leads the agency's Action Development Process (ADP), which is EPA's regulatory,

policy, and guidance development process. ORPM provides numerous services in support of the ADP, including tracking of regulatory actions, generating status reports for senior management, preparing and transmitting documents to the Office of Federal Register and to the Office of Management and Budget. The EAMS application collects and displays data about ADP and other Agency actions, supports customizable workflows, simplifies reporting on regulatory activity, and facilitates an internal, paperless regulatory process.

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

Data elements that are used to retrieve information include tracking numbers, such as RIN, and title/key word of a given rulemaking. These data elements are associated with individual EPA regulatory actions, which in turn list a staff person's name and telephone number (as required by the Federal Register Act) for members of the public to contact in the event of questions about the published regulatory action.

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:

Low risk of inappropriate usage.

Mitigation:

Audit logs are reviewed to detect inappropriate usage of data.

*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: