EPA United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

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

If you need further assistance contact Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

System Name: EPA Action Management System (EAMS)

Preparer: Caryn Muellerleile **Office: OA/OP/ORPM/RMD**

Date: 07/31/2018 **Phone: (202) 564-2855**

Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____

This system is in the following life cycle stage(s):

Definition ☐ Development/Acquisition ☐X Implementation ☐

Operation & Maintenance ☐ Rescindment/Decommissioned ☐

Note: 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 of the system:

The objective of this project is to support the development of the EPA Action Management System (EAMS) through iterative development and the deployment of the application at the National Computing Center (NCC). The Office of Policy's Office of Regulatory Policy and Management (ORPM) is building a user friendly application that will collect and display data about Agency actions, support approval workflows, simplify reporting required across the Agency, and facilitate an internal, paperless regulatory process. This new system will replace all critical and major business processes supported today by the legacy Lotus Notes systems in use by EPA staff.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the system in question?

Authorizing EPA statutes, 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?

The system security plan is underway.

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.

EPA rulemaking activity may be subject to the Paperwork Reduction Act (PRA), but does not itself impose PRA requirements.

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 elements the system collects and maintains include: Regulatory Information Number (RIN) #, Docket #. Additionally, the system collects names of EPA staff members who are listed as points of contacts on rulemakings and other regulatory activity, e.g. guidance documents. Information collected is: Name, Office Location, Office Telephone Number, Office Email Address.

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

Information is internally collected by EPA staff. Information about EPA staff will be 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 system is generated from a commercial or public source. The data created and maintained is internal to government.

2.4 Discuss how accuracy of the data is ensured.

The system will generate reports for EPA staff verify accuracy of data for its internal audience.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: None.

Mitigation: None.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the system uses the information.

The Office of Regulatory and Policy Management (ORPM) in 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 regulatory actions, generating status reports for senior management, preparing and transmitting documents to the Office of the Federal Register and Office of Management and Budget.

3.2 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, or title/key word of a given rulemaking.

3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?

Information is not retrieved by a personal identifier.

3.4 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information? None

3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.

No.

3.6 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: None.

Mitigation: No disaster or catastrophic impacts if privacy is compromised. Users entering the system view a government-only notification message prior to log-in.

Section 4.0 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.

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

At login, individual users must read a privacy and security statement. This language is available at https://eamsstg.epa.gov/RMS/#/login.

4.2 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?

System users will receive notification before first accessing to inform them of use of system for government purposes only.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: None.

Mitigation: None.

Section 5.0 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.

5.1 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 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.

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

Yes, various internal roles provide differing levels of access within the system.

5.3 Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act) will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

Internal parties are EPA employees and external parties are only IT contractors who conduct development and O&M on the system. All contractors must follow FAR clauses applicable to the Privacy Act.

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

The System Administrator in OP will assign each user role which determines what type of data they can access and edit. The determination is based upon the user's job duties and management assignment.

5.5 Explain how long and for what reason 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 (RCS) 0089.

5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes.

5.7 Privacy Impact Analysis: Related to Retention

Privacy Risk: None.

Mitigation: N/A

Section 6.0 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.

6.1 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 shared outside of EPA is only with other federal agencies:

- Office of Management and Budget: interagency review documents under Executive Order 12866, transmitted via OMB's password-protected private data system ROCIS;
- Office of Federal Register: Federal Register publication documents, submitted via delivery of certified copy or electronic Public Key Infrastructure, or PKI, locked digital signature; and
- General Services Administration: Semiannual Agenda data, submitted via Extensible Markup Language, or XML file, via government to government electronic mail.

All information exchanged between these agencies is considered deliberative and internal until the related regulatory action (proposed or final rule) is published in the Federal Register.

6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

As described in 6.1, EPA's data sharing only occurs with other federal agencies.

6.3 Does the agreement place limitations on re-dissemination?

The Federal Register Act, Administrative Procedures Act, Regulatory Flexibility Act, and Executive Order 12866 require EPA to share various data elements with OFR, GSA, and OMB for purposes of Federal Register publications and Unified Agenda updates.

6.4 Describe how the system maintains a record of any disclosures outside of the Agency.

The system does not house records but certain statutory activity for information distributed to OFR and OMB is maintained under Records Management Policy (CIO 2155.3).

6.5 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?

The EAMS system is internal to EPA only. No outside access is granted to external users.

6.6 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Low

Mitigation: Information sharing risks are mitigated by sharing information solely with federal partners, such as OMB and OFR, by way of secure, password-protected systems.

Section 7.0 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.

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

Information about individuals would only include their work place contact information, based on EPA's Active Directory, and their participation in the development of given regulatory activities. All EPA employees have read-access to the system.

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

Should incorrect information about a given employee's work place or participation on a regulatory work group be listed, any editorial user can correct the erroneous data by request.

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

The system will not have a mechanism to notify users of procedures but user manuals will be provided on SharePoint or EPA intranet.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Low.

Mitigation: No compromise of personal data or other catastrophic impacts if erroneous individual information is listed.

Section 8.0 Auditing and Accountability

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

8.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

Because of deliverables that EPA delivers to its federal partners (e.g., OMB, OFR, etc.), if practices are not followed, then EPA's regulatory objectives are not met in accordance with law.

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

EPA's annual privacy and information security trainings are provided to all users.

8.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: Low

Mitigation: There is a low risk for leaking internal deliberative documents and OP mitigates those risks by controlling access through roles and creating a log or record of who edits an action.