EPA United States Environmental Protection Agency

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 Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

System Name: Correspondence Management System	
Preparer: Keith D. Livingston	**Office:** Office of the Administrator, Office of the Executive Secretariat
Date: October 12, 2018	**Phone: (202) 564-9962**

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:

CMS is EPA's correspondence tracking and workflow management system. It scans, logs, routes, tracks, and stores incoming and outgoing correspondence in all Program and Regional Offices.

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?

5 U.S.C. 301 Departmental Regulations

The head of an Executive department or military department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property. This section does not authorize withholding information from the public or limiting the availability of records to the public.

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, the system has an SSP. The system has an ATO and is due to start a CMA Y1 on October 1, 2018. The current ATO will be renewed upon completion of this assessment.

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?

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).

CMS captures metadata which consists of, name, address, email, and telephone, relating to internally and externally generated Agency correspondence; draft responses (including versions); scanned (.pdf) copies of incoming correspondence, outgoing responses and final documents; and electronic versions of supporting documents. The application also captures information relating to workflows, including which Agency employees created, modified, reviewed, or concurred on the documents in the application and when they did it.

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

Correspondence is generated by EPA employees, members of the public, stakeholders, industry, academia, Congress, the White House, and state, local, tribal, and international governments. Information may be received in hard copy or electronic format (most commonly e-mail).

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.

The CMS users is responsible for ensuring that the information from the recipient is correct.

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:

Collection of and quality of the information ensuring the response is sent to the correct person.

Mitigation:

Make sure that the address of the recipient(s) is correct.

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?

There are two distinct levels of access in CMS, Coordinator and Author with the former being the higher. All actions/workflows are associated with corresponding Access Control Lists (ACL) to determine who has access to information.

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

Only EPA employees and contractors may request access to the system, which means they 1.) have passed a background check appropriate to their responsibilities; and 2.) receive periodic Privacy Act and Records Management Training.

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

Each program or regional office (groups) in CMS decides who needs access as a part of the job responsibilities.

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 external parties have access to this application. The FAR clauses are included in the CMS maintenance contract. Only EPA employees or authorized contractors have access to the data/information in CMS. Access is limited according to the individual's office and his or her assigned role. In general, an individual may only access a control (the CMS term for the virtual folder containing the scanned images, files, and metadata for each piece of correspondence tracked using the application) if she or he created the control, modified the control, edited the control, or was granted viewing authority by the creator of the control. In this way, access to CMS records mirrors access to hard-copy records.

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.

A records schedule is under development for the system, No. 77. Electronic data is disposable and will be kept for the length of time required by the applicable records schedule. (CMS is not certified as an electronic system of record, so EPA creates and manages hard copy records that correspond to the information contained in CMS. Each of these hard copy records are maintained in accordance with their associated records schedules.)

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:

Answer is based on the records schedule(s) that is assigned to the correspondence.

Mitigation:

CMS users must consult with their RLOs to make sure that they are selecting the correct records schedules.

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.

Yes, the following General Routine Uses of EPA Systems of Records apply to this application:

A, B, C, D, E, F, G, H, I, J, K

Records may also be disclosed to a federal, state, or local governmental agency when it is determined that a response by that agency is more appropriate than a response by the U.S. Environmental Protection Agency.

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

The external sharing is compatible with the purposes of the original collection. The records are collected for correspondence management.

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?

The Information Sharing Agreements (ISAs) and MOUs are reviewed by the system owner and the Information Security officer before being approved. These agreements are signed by the ISO and SIO of both parties and reviewed during the annual CMA. Uses of the

information is explained in both documents. There is no access to the system by organizations outside of EPA.

4.4 Does the agreement place limitations on re-dissemination?

Yes.

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?

The Rules of Behavior state the use of the system and users are instructed to only enter correspondence related information.

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

Yes, the end user training provided by the CMS support staff along with the annual security and privacy training (ISPAT) that is provided by Agency.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Information is not shared electronically outside of the Agency, except what is stated in the SORN.

Mitigation:

None

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 data is used to facilitate the dissemination of information to the public, stakeholders, and government officials. It is also used to facilitate searches of Agency records responsive to Freedom of Information Act and legal discovery requests, as well as Congressional inquiries. The information is used to track, route, and store incoming and outgoing Agency correspondence from and to members of the public, private, and governmental sectors.

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.)

All CMS records are full-text indexed and are retrieved by name or control number.

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

EPA-22 Correspondence Management System (CMS)

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:

If the system is ever breached, the information collected has a potential to be misused.

Mitigation:

The system is housed within the EPA firewall and use is exclusive to EPA personnel and contractors. IT security requirements are in place and levels of access and ACLs (access controls listsN) are inherent to the system which prevent the misuse of information.

*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, or his or her duly authorized representative, who (1) is desirous of knowing if information of any kind about him or her is maintained in the Correspondence Management System, should make his or her request in writing to the System Manager(s).

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?

Anyone writing to the U.S. Environmental Protection Agency voluntarily shares the content of their letter, their name, and whatever contact information they provide. CMS does nothing more than capture this information in an electronic format for internal tracking, workflow control, and retrieval purposes.

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:

None

Mitigation:

None

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?

At a minimum, requestors will be required to provide adequate identification (e.g., driver license, military identification card, employee badge or identification card) and, if necessary, proof of authority. Additional identity verification procedures may be required as warranted. Copies of records that are responsive to the individual's request will be mailed or delivered by reasonable alternate means, if requested. Fees may be incurred if copies are made and mailed in accordance with 16.4 of current regulations.

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

Individuals requesting correction of or amendment to records must reasonably and accurately identify the record in question, specify the information they are contesting, and detail the corrective action sought. Complete U.S. Environmental Protection Agency Privacy Act procedures are set out in 40 CFR Part 16.

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

N/A

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:

None

Mitigation:

None