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: Enterprise Content Management System	
Preparer: Shah Khan/ Nannette Willis/ Titi Taiwo	**Office:** OMS/OEIP/ERMD
Date: 11/17/2021	**Phone:** 202-566-1226/ 202-566-0658/ 443-889-7402
Reason for Submittal: New PIA____ Revised PIA_X___ Annual Review __ 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:

The Enterprise Content Management System (ECMS) is an EPA Major Application (MA), developed in 2006 and operational since April 2007.

ECMS is an agency-wide content management services infrastructure that is providing standard records management services for Office 365 e-mail, desktop files, content management services, scanning capability, agency information search and retrieval and other planned services. ECMS supports workflow services for regional and program business processes. Currently, ECMS provides a set of core functional services that EPA users utilizes for their daily business operations. These services are referred to as ECMS Foundation Services and consist of the following:

- Content Management Services,
- Content Ingestion Services,
- Search Capability across EPA-wide applications,
- Scanning Capability/Services, and
- Records Retention Policy Management Services.

And a new component of existing Enterprise Content Management System (ECMS), the Agency Records Management System (ARMS Application), is being developed to upgrade the ECMS in 2022. That will result in a modernized records management technology solution hosted in the AWS Cloud of EPA. The Records Management Technology Modernization effort undertaken by Enterprise Records Management Division aims to upgrade the underlying records management technology from Documentum to Nuxeo and also focus on 3rd party application integration. This upgrade will include switching to a cloud native, API centric, low code application architecture and significantly improving search capability. Migration from the current on-premise Documentum repository to the ARMS repository will continue in conjunction with the technology upgrade. Nuxeo will handle records retention, search, litigation hold and user management. Nuxeo will also provide a simple-to-use content ingestion endpoint that allows records to be easily transfer into the repository with the required NARA metadata and record schedule information.

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?

CIO Memo 2135.0 Section 5 contains a list of specific legal authorities that permit and define the collection of information by ECMS. http://intranet.epa.gov/ecms/policy/cio21350.pdf

- E-Government Act of 2002 (P.L. 107-347). Designed to enhance the management and promotion of electronic Government services and processes.

- Information Technology Management Reform Act (Clinger-Cohen Act). Public Law 104-106, 1996. – Provides the Agency's CIO responsibility for "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency" (Sec. 5125(b)(2)) and "promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency" (Sec. 5125(b)(3)).

- The Government Paperwork Elimination Act. Public Law 105-277, 1998. – Requires agencies to allow the public to interact with the federal government electronically, and to maintain records electronically when practicable. In addition, requires the establishment of strategic planning and performance measurement in the Federal Government.

- OMB Circular No. A-11, Part 7 on Planning, Budgeting, Acquisition and Management of

Capital Assets – Encourages the use of enterprise-wide content management systems with capability to read records into the future to alleviate the need to maintain outdated software.

- OMB Circular No. A-130 – Management of Federal Information Resources

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 ATO Expires July 16, 2023.

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, Amazon AWS, SaaS

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 following minimum mandatory metadata elements may be collected as specified in the Enterprise Information Management (EIM) Minimum Metadata Standards (http://intranet.epa.gov/ecms/policy/EIM_Metadata_Standards.pdf):

- Title
- Creator
- Publisher

- Date [and Date Type]
- Retention

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

The sources of the information are either EPA emails or EPA desktop records. The information is collected through EZemail and EZdesktop. Both are components of ECMS.

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.

Each individual employee is responsible for the content of their records. The role of the ECMS is to collect those records and not disseminate the content.

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:

In section 2.1, we identified which fields we collect. Of those fields, none of these have an impact on the characterization of ECMS.

Mitigation:

As ECMS does not disseminate collected information neither does it mitigate information collected because of the lack of effects of characterization these fields have an impact on for ECMS.

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, access control levels are in place within ECMS to prevent unauthorized access to records. ECMS requires user accounts to be established in the system prior to a user being able to access the system for saving emails, searching emails or using any of the ECMS application management tools. All current EPA employees and contractors with email accounts have been set up with regular user accounts in the system. ECMS system does not use guest/anonymous or temporary accounts. Membership in the regular user account allows a user to access the ERMA records classification screen to save an email record to their organization's records-keeping file plan. Any regular user can also save an email record to the Superfund record schedule. They can also access the ERMA search screen to search for and view email records saved within their organization's records-keeping file plans. They can view records that they have saved as "sensitive" or private records.

See the following table for a list of all ECMS custom group and roles

Name	Class	Members	Usage
iss_org_base_group	Group	organization (organization office acronym)	All organizations created in the system must be added to the base group.
Staffs	Group	EPA employees	All EPA employees are members of the Staff Group. EPA Contractors are not members of this group. EPA Contractors are restricted to viewing only the records they have personally saved into the system
organization (office acronym)	Group	End users who wish to save and search records in ECMS must be a member of an organization group	Organization Group defined by office acronym. Members assigned to an organization group have access to that organization's file plan for records saving and searching.
ecms_username (username group)	Group	By default the individual user "custodian"	A user's personal or sensitive group. A user must be a member of this group to view their own sensitive (private) records.
epa_all	Group	special users	Special group for members of the Office of General Council (OGC).
rlo_organization (super level organization office acronym)	Group	Records Liaison Officers (RLOs)	Organization Group(s) to which Records Liaison Officers are assigned for the purpose of accessing and managing that organization's records. (e.g., rlo_OEI)

Name	Class	Members	Usage
rlo_officers	Group	rlo_organization (super level organization office acronym)	Records Liaison Officers Group. Membership in this group is required for access to the ECMS file plan and records management tools.
ecmsr_recordcontributor	Group	All active users from the OID (Users are added to this group via the LDAP sync job)	Records Contributor Group. All users must be members of this group in order to save records to records repository formal records file plan.
ecmsr_recordmanager	Group	rlo_officers and admingroup	This group is the owner of all records in ECMS. Membership in this group is required to access the Records Management Administrator privileges
Admingroup	Group	Special users that require extended privileges and records management audit reporting. (example:- system admininstrators and PMO admin users)	Admin Group. Membership in this group is required for access to ECMS Records management audit reporting.
org_adm_officers	Group	org_adm_(super level organization office acronym)	Application Administrator Group. Controls access to Organization Admin and People Admin Tools.
ecmsr_rloadmin	Role	rlo_officers and file plan admins	Administrator Role. Controls access to File Plan Admin and Records Admin Tools.
org_adm_(super level organization office acronym)	Group	Organizational administrators and people administrators	Organization Groups to which Org Admins and People Admins are assigned for the purpose of accessing and editing that organization's descriptive information and people (e.g., org_adm_oei)

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

The ECMS People Administration Tool (PAT) allows an organizational administrator the ability to easily reassign ECMS organizational access permissions to groups of people who have changed their organizational affiliation due to re-organizations. The users of the People Administration Tool will be limited to approximately 50 organizational administrators designated by the Information Management Officials (IMO) for each Program Office and Region who will be responsible for keeping their organizations' information current in

ECMS. Generally, there will be two of these administrators per headquarters Program Office or Region. Each of these users will be trained specifically in the use of this tool.

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

No, ECMS requires user accounts to be established in the system prior to a user being able to access the system for saving records, searching records or using any of the ECMS application management tools.

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?

All current EPA employees and contractors with email accounts have been set up with regular user accounts in the system. FAR 4.703 specifies that all federal contractors must retain certain project records for audit and inspection purposes. Section c provides express provision which allow contractor so "[duplicate or store] original records in electronic format."

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.

Records are retained until scheduled disposition of records from the system based on pre-defined records retention schedules.

Schedule: 742 - Enterprise Content Management System (ECMS)

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:

Records must be retained based on their pre-defined records retention schedules. Removal of records prior to the pre-defined records retention schedule is a potential privacy risk.

Mitigation:

Removal events are audited on a weekly basis by reports generated from the ECMS system. All deletions from the system are audited. The addition of records to the system is audited through weekly transaction reports and daily records transmission reports. The reports are maintained by the NCC ECMS system administrator and the EPA ECMS Program Management Office.

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.

External access and sharing of records stored within ECMS is not allowed.

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?

Periodic review of ISA and related documents. MOUs are not applicable as external access or information sharing is not allowed for ECMS.

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:

N/A

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 as stated in Section 6.1?

All transactions are tracked within ECMS through auditable events. The system does not alter the original content or time ordering of audit records. The system handles audit reduction and report generation capability by auditing functions within the database. The database creates customized reports based on the audit events in the system. These audit logs are reviewed to ensure that information is used in accordance with stated practices outlined in this PIA.

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

Only EPA employees and approved contractors may request access to this system, which means they have completed and passed annual Information Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Audit logs could be inadvertently lost.

Mitigation:

Database audit logs are kept for 90 days, some of that time on the instance and some of the time archived on a separate instance. Anything older than 90 days is deleted daily. In general they are on the DB server for about 24 hours then moved to the backup appliance. Audit records generated today would stay on the database for the rest of the day, then be moved to the separate database and kept for 90 days. The last backup of the separate database would be kept for another 90 days. That adds up to approximately 180 days' retention, 170 days to allow for the usual "expected" unexpected.

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.

In support of the authorities mentioned in section 1.1, ECMS performs the role of repository for EPA records and make them retrievable by EPA employees.

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.)

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.]

N/A. ECMS does not have SORN

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:

N/A

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.

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?

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?

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:

Mitigation: