EPA 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: Intranet Content Management System (IntraCMS)	
Preparer: Rodney Baylor/Lin Darlington	**Office: OMS/OIM/WCSD**
Date: January 6, 2021	**Phone: 202-566-2919**
Reason for Submittal: New PIA_X__ Revised PIA____ 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:

Intranet Content Management System (IntraCMS) is a content management system that will be utilized for EPA's internal facing intranet on intranet.epa.gov (not exposed to, or is accessed by the general public). This application, running on open source Drupal code, will be the Agency's standalone internal system for developing office or regional intranet content.

We also utilize Drupal CMS (DWCMS) for our public access website, www.epa.gov (available to general public) however this system will be separate from our IntraCMS and will become part of the AWS Cloud Hosting System. This internal facing portal will be the primary means by which stakeholders (Federal Employees, Contractors, SEE, Grantees) create and disseminate internal information, which is accessible solely via EPA LAN ID and password, SSL-encrypted, and restricted to EPA Intranet access to improve knowledge sharing and decrease email communication. IntraCMS also allows for the development of a social hub to connect with employees through company news, blogs, events calendar, videos and newsletters.

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?

The Intranet Content Management System, running on Drupal content management software, does not collect information. Our current pilot site; oneintranetpilot.epa.gov meets every policy outlined in Policies for Federal Agency Public Websites and Digital Services, OMB Memo M-17-06, including privacy protection (Privacy Act) and implementing information security (FISMA and OMB Circular A-130). Federal Information Security Modernization Act of 2014 44 USC 3531-3538 (Pub. L. 113-283) 128 STAT. 3073

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?

No. This is new system and in the early stages of development and deployment.

ATT expires November 2020.

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. The IntraCMS will be hosted on-premise at the National Computer Center, RTP, NC.

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).

IntraCMS will collect public and internal information that consists of memos, agency announcements, organizational charts, agency forms and listings of EPA services.

Additionally, the use of forms will allow for collection of information such as first name, last name and email addresses.

The application does not collect or post Social Security numbers, Biometrics, or Dates of Birth.

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

Information will come from EPA program and regional offices, which will create and upload content to current pilot URL oneintranetpilot.epa.gov, as part of a unifying communication, productivity, and collaboration platform to better inform EPA staff and contractors.

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. All information comes from EPA staff and contractors.

2.4 Discuss how accuracy of the data is ensured.

EPA staff and contractors post information that has been peer-reviewed and is required as part of any federal regulation (Clean Air Act, Clean Water Act, etc.) that pertain to EPA activities and informational outreach.

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:

Risk of information integrity.

Mitigation:

System requires authenticated access to edit content. System tracks user edits and changes can be tracked by each user. Additionally, version tracking will be enabled to allow previous versions to be restored.

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?

Since this information is intended for internal communications, there are no access controls required. However, only users with sufficient privileges, as given by program office, can edit pages and content that belong to another office (e.g. Staff in the Office of Air and Radiation cannot modify Office of Water content).

Program and Regional offices designate users with specific roles for their web area topics. Users can have the following roles: web area webmasters, editors, approvers, or authors. These roles are in place only for that web area: users only have access to the information for that web area.

The system stores and tracks all system roles and user permissions (Member/Author/Admin). Admin policy is to assign a user with the least privilege role required to complete the task. Each permission is specifically granted to a user role. A user must be a member of a web area to perform any content management tasks. The only permission not associated with web areas is the creation of webforms. Creating webforms requires the Webform site role and only Admins can assign that role. Signed Rules of Behavior (ROB) are required for all admin account holders.

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

This new system is still in pilot stages and will soon be going to production environment. After the production environment is established, the policies and procedures for access controls will then be documented. Currently, the system is only accessible to system administrators. To obtain requirements to be considered a system administration, users must sign and consent to a rules of behavior agreement.

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

Yes. There will be multiple roles, ranging from author (very limited access) to administrator (can view all content and configuration settings). Each role has its own set of privileges, and each succeeding role inherits the privileges of the role below it.

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?

Users include EPA employees and contractors. For contractors, depending on their role, have access to some parts of the content in the system. Their contracts include the FAR clause.

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.

EPA Records Schedule 0742 and the related schedule is 1012. Disposal of records are to be disposed of at close of calendar year, or when superseded by a new iteration, or no longer needed. Destroy 7 years after file disclosure.

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:

The privacy risks related to retention would be site owners failed to update or refresh existing content that is no longer valid.

Mitigation:

Routine content review will ensure updated content, valid links, and quality of information. The system enforces a review of all content within one year. EPA program and regional offices must review every page they own annually

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing extern al 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. There is no external sharing.

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. There is no 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 as stated in Section 6.1?

IntraCMS will have auditing enabled to enable tracking/auditing of changes within the environment to ensure information is used for the purpose for collection.

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

IntraCMS is covered by the agency's mandatory training requirements, e.g., information security and privacy awareness training, ethic, and FOIA.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of improper audit.

Mitigation:

To mitigate risks regarding accountability, an audit trail will be implemented. This audit trail will accomplish security-related objectives, including individual accountability, reconstruction of events, and problem analysis.

Additionally, the implemented audit trails can be used to identify and provide information about users suspected of improper modification of data.

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.

Information posted on EPA's Intranet site will be used for internal communications and education. Information posted can include but not limited to; memos, agency forms, listings of EPA services, agency announcements and organizational charts.

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.*)

The system retrieves information via keywords, description, or links from page to page. It's a web site.

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?

Drupal CMS has an audit trail that maintains a system activity both by the system and by user activity of systems and applications. System will also utilize EPA authentication and that user information is stored outside of system in active directory.

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 information misuse.

Mitigation:

The system stores and tracks all system roles and user permissions (Member/Author/Admin). Admin policy is to assign a user with the least privilege role required to complete the task. Each permission is specifically granted to a user role. A user must be a member of a web area to perform any content management tasks. The only permission not associated with web areas is the creation of webforms. Creating webforms requires the Webform site role and only Admins can assign that role. Signed Rules of Behavior (ROB) are required for all admin account holders.

***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 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

<u>Mitigation</u>:

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 <u>Privacy Impact Analysis</u>: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

<u>Privacy Risk</u>:

<u>Mitigation</u>: