United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – 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 Roster.docx

System Name: Intranet Content Management System (IntraCMS)		**System Owner:** Michael Martinez	
Preparer: Michael Martinez		**Office:** OFA/SIMD/MOB	
Date: 3/3/2026		**Phone: 202-566-2912**	
Reason for Submittal:			
New: ☐	Revised: ☐	Annual Review: X	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: X	Rescindment/Decommission: ☐		

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 work.epa.gov (not exposed to or is accessed by the public). This application, running on open-source Drupal code, will be the Agency's standalone internal system for developing office or regional intranet content.

The IntraCMS offers features such as a responsive web design to enhance user engagement across multiple devices, building audience specific content, customizable workflow for content administration to meet publishing standards, security compliance with standards such as Federal Information Security and

Modernization Act (FISMA), built-in accessibility with Section 508 of the Rehabilitation Act of 1973 and Web Content Accessibility Guidelines (WCAG) 2.0 standards compliance, and key functions like custom promotions, drag-and drop layout, custom web forms, press releases, blogs and directories.

IntraCMS permits authorized EPA employees/contacting staff to electronically administer the content of the Agency's internal site, work.epa.gov, explicitly maintain the functional independence of content management on individual sites. Each EPA program office and regional office are responsible for their website content development and management activities in addition to complying with EPA Privacy Policy, Federal laws, and policies to protect individual privacy. Each EPA program office and regional office are responsible for ensuring their use of work.epa.gov and IntraCMS follow applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. The site, work.epa.gov, has a variety of forms and other documents supporting program offices, regional offices, and activities

Section 1. 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 site; work.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, the IntranetCMS does not currently have an SSP, or ATO/ATU.

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 information collection request 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?

The IntranetCMS is currently hosted in the Agency's Amazon Web Services (AWS) Enterprise Cloud Hosting System (ECHS).

Section 2. Characterization of 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).

IntranetCMS 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 work.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.

Some of EPA program/ regional offices epa.gov sub-page webforms may collect more PII than is needed.

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

The program officials and data owners are responsible for ensuring that only minimum PII needed is collection and that collection is authorized to support a mission or business need in accordance with the Privacy Act, other Federal law and policy, and EPA privacy policy.

Section 3. 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). Users know not to post any PII documents such as resumes unless the page is accessed for need-to-know purposes only.

Program and Regional offices designate users with specific roles for their web area topics. Users can have the following roles: member, editor or admin. 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 privileged 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 staff members, events and webforms. Staff Members and Events can be created and modified by any authenticated user. Creating webforms requires the Webform site role and only Site Admins can assign that role.

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

The procedures and standards can be found at work.epa.gov/intranet-guide.

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. The system roles we have include anonymous (still require access to VPN), authenticated, webform, system editor and administrator.

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, they 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 is to be disposed of at close of calendar year, or when superseded by a new iteration, or no longer needed.

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. Editors-in-Chiefs (EICs) are responsible for maintaining content within their respective web areas. EICs are given administrative access to their web areas to ensure they have the means of updating content as needed. Every Web Area is required to always have an EIC. Intranet Council members are notified whenever there is a change in an EIC for a web area that is owned by their region or office for transparency's sake.

Section 4. 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 governments, 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:

There is no external sharing.

Mitigation:

None.

Section 5. 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?

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

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

EPA employees and contractors are required to complete annual Privacy and Computer Security Awareness Training to ensure their understanding of proper handling and securing of PII. Privacy training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). Leadership at each OMS is responsible for ensuring that all federal employees and contractors receive the required annual Computer Security Awareness Training and Privacy Training. Other related and mandatory training requirements that cover the IntranetCMS are ethics and FOIA training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

EPA require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. All user actions in the Intra-CMS are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. EPA employees assigned to maintain the EPA systems have job duties that require them to design, develop, and optimize the system within the security accreditation environment. Furthermore, each employee is required to undergo annual security awareness training that addresses his or her duties and responsibilities to protect the data.

Mitigation:

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

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?

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.

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 privileged 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 National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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?

Click or tap here to enter text.

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. 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 Freedom of Information Act (FOIA).

Privacy Risk:

Mitigation:

I attest as the Agency Privacy Officer that **Intranet Content Management System (IntraCMS)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully, ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.07.10 12:59:45 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA