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: Drupal WebCMS (DWCMS)	
Preparer: Michael Hessling	**Office:** OMS/OIM/WCSD
Date: 13 May 2020	**Phone:** 202-566-0419
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:

Drupal WebCMS is a content management system that helps EPA staff and contractors manage their public information content on www.epa.gov. This application, running on open source Drupal, is the primary method that EPA uses for communication with the public. This public web site and associated digital services is the primary means by which the public receives information from and interacts with the EPA. This web site provides information for the public to find grant applications, search for jobs, comply with Federal rules, obtain authoritative information, and much more. The EPA web site meets and maintains high standards of effectiveness and usability and provide quality information that is readily accessible to all.

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 DWCMS does not collect information. www.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).

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 SSP was first published in December 2012 and has been updated periodically since. The current ATO expires on 01 August 2022.

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?

The DWCMS is currently 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).

Public information content EPA staff creates and edits public information content on a variety of topics under EPA's regulatory purview. EPA staff and contractors create, edit, and upload this public content in HTML, PDF, images, and various other formats.

This 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?

The public information comes from EPA program and regional offices, which create and

upload content to www.epa.gov, as part of its public outreach and education. This application does not collect or post Social Security Numbers, Biometrics, or Dates of Birth.

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:

Because this information is public and is meant for public consumption, there is no privacy risk.

Mitigation:

N/A

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 meant for the general public, there are no access controls required. However, only users with sufficient privileges, as given by the 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 be: 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.

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

documented?

These access controls are documented in controls AC-2: Account management, AC-3: Access enforcement, AC-5: Separation of duties, and AC-6: Least privilege.

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

Yes. There are 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?

Contractors, depending on their role, have access to some parts of the content in the system. Their contracts comply with the FAR.

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 0090 and the related record schedule is 1021. The WEB Content is covered by EPA 0095.

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 concern is records that remain publicly available after its retention period is over.

Mitigation:

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 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.

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?

The application is a public web site; all information posted to the public web site is meant for educating and informing the public.

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

The DWCMS is covered by the agency's annual 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:

The concern is content that remains publicly available after its retention period is over.

Mitigation:

The system enforces an audit of all its public content within one year. EPA program and regional offices must review every page they own annually.

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.

This public information posted to the application is used by the public for their information and education. Information includes the list of disinfectants to kill viruses, grants for safe drinking water, regulatory history of various congressional acts, etc.

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?

None. No information about public users are captured or retrievable.

[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.]

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:

None. No information about public users are captured or retrievable.

Mitigation:

None.

*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 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?

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

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: