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 Roster.docx

System Name: Drupal Web Content Management System (DWCMS)		**System Owner: Michael Hessling**	
Preparer: Michael Hessling		**Office: Office of Mission Support / Office of Information Management**	
Date: 1/5/2024		**Phone: 202-566-0419**	
Reason for Submittal:			
New: ☐	Revised:☐	Annual Review: ☒	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: ☒	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:

Environment Protection Agency (EPA) Office of Mission Support manages the EPA Drupal Web Content Management System (DWCMS), which is a customized open-source software for creating and managing content on websites. EPA uses DWCMS to publish on www.epa.gov and manage content on www.epa.gov to provide information on the Agency's mission, vision, history, and to also engage with the public. EPA DWCMS offers features such as a responsive web design to enhance user engagement

across multiple devices, multilingual support for translating content, or for 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.

DWCMS permits authorized EPA employees/contacting staff to electronically administer the content of the Agency's flagship site, www.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 www.epa.gov and DWCMS follows applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. The site, www.epa.gov, has a variety of forms and other documents supporting program offices, regional offices, and activities. Data owners are responsible for working with their program office and regional office Liaison Privacy Officer (LPO) to identify, assess, and manage privacy risks related to their use of DWCMS and www.epa.gov, including conducting privacy impact assessments (PIAs) and providing privacy notice as appropriate and required.

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?

43 U.S.C. 1451, Establishment; Presidential Memorandum to the Heads of Executive Departments and Agencies on Transparency and Open Government, January 21, 2009; OMB M-10-06, Open Government Directive, December 8, 2009; OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, June 25, 2010; OMB M-10-23, Guidance for Agency Use of Third-Party Web sites and Applications, June 25, 2010; OMB M23-22, Delivering a Digital-first Public Experience.

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 in September 2025.

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

Section 2. 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).

DWCMS collects EPA Employees' names, phone numbers, email addresses. Additionally, DWCMS collects names and email addresses from members of the public.

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, and members of the public are able to voluntarily fill out web forms and provide comments on www.epa.gov.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

DWCMS does not use information from commercial sources or publicly available data.

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. Each EPA regional/ program office content owner is responsible for managing their information and verifying its accuracy.

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:

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

Mitigation:

The program officials and data owners are responsible for ensuring 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 meant for the 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 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?

The access controls (AC) 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?

Each program and regional offices designate staff to manage their program/regional content. Each office can assign staff to various roles, but roles are only assigned to individuals within their program and regional offices.

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:

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule.

Mitigation:

DWCMS maintains all records with PII in accordance with applicable records retention or disposition schedules approved by NARA or based on the need and relevancy of the data in the support of the OMS mission. Some records are maintained as permanent records due to their continuing historical value; all other temporary records are disposed of in accordance with approved records.

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 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.

Not Applicable.

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?

Not Applicable.

4.4 Does the agreement place limitations on re-dissemination?

Not Applicable.

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:

Not Applicable.

Mitigation:

Not Applicable.

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?

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.

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.

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:

OMS employees may misuse and inappropriately disseminate information.

Mitigation:

EPA require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions in the DWCMS are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. EPA employee 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.

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.

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: ☒ 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 is not designed to retrieve information by a personal identifier.

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.

The information within DWCMS is not maintained in a system of records.

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:

There is a risk that a user may access information on DWCMS that he or she does not have a need to know.

Mitigation:

To protect the privacy of the users and the information transmitted by DWCMS, EPA implemented a series of technical, administrative and physical controls, including encryption to secure transmissions to prevent interception or altercation. Each Data Owner is responsible for ensuring only personnel with the business need-to-know are authorized to access and process DWCMS. In addition, each program official and data owner is responsible for ensuring all staff complete EPA's annual security, privacy, record and role-based training and sign the EPA Rules of Behavior (ROB) prior to accessing www.epa.gov and DWCMS.

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:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.

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:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.