United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

System Name: Drupal WebCMS (DWCMS)	
Preparer: Michael Hessling	**Office: OEI/OIM**
Date: 12 October 2018	**Phone: 202-566-0419**
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: 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 main way EPA communicates 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 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 agreements permit and define the collection of information by the system in question?

I do not know. 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?

Yes. The SSP was first published in December 2012 and has been updated periodically since.

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.

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 on a variety of topics under EPA's regulatory purview. EPA staff and contractors create, edit, and upload public content in HTML, PDF, images, and various other formats. Many topics-based web areas include a "contact us" form, where the public can contact EPA with a question or a comment. These forms include optional fields for name and email. The results of these forms are saved in the DWCMS database, but are not publicly available. After 180 days, this data is deleted from the DWCMS database.

In addition, the system connects to EPA's Identity Management system to authenticate user accounts. EPA staff log into the system to manage their content using their Agency-wide account credentials.

This application does not collect 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. Information from the "contact us" forms are voluntarily given to EPA for the purposes of communicating with EPA staff and subject matter experts. This contact information is deleted after 180 days. EPA staff and contractor information is provided from OAM to the DWCMS for authentication purposes. This application does not collect 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

2.4 Discuss how accuracy of the data is ensured.

N/A

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:

All EPA staff – federal employees and contractors with access to EPA Virtual Private Network – have access to the information via the DWCMS application. While there is PII – personally identifiable information, it is not exposed to the public and it is deleted after 180 days.

Mitigation:

All PII is deleted after 180 days, adequate time for EPA staff to respond to the public. In addition, the DWCMS has a "sweep" function that will scan every page for SSN and credit card numbers, alerting system administrators when found.

Section 3.0 Uses of the Information

The following questions require a clear description of the system's use of information.

3.1 Describe how and why the system uses the information.

The PII from "contact us" forms are used for correspondence. EPA has no way of responding to the public if we do not know the email address to respond to.

3.2 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.*)

We have no identifiers linked to specific individuals, unless they are Agency staff or contractors, since we use their account information for authentication purposes—only Agency staff or contractors are allowed to log into the system. Agency staff details are not exposed to the internet.

3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?

N/A. No information about public users are retrieved.

3.4 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

None.

3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.

No.

3.6 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. Name and email are voluntarily given and are optional.

Mitigation:

All PII is deleted after 180 days, adequate time for EPA staff to respond to the public. In addition, the DWCMS has a "sweep" function that will scan every page for SSN and credit card numbers, alerting system administrators when found.

Section 4.0 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.

4.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

A link to EPA's Privacy topic, https://www.epa.gov/privacy, and EPA's Privacy and Security Notice, https://www.epa.gov/privacy/privacy-and-security-notice, are included on every www.epa.gov page.

4.2 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?

All contact forms are optional. The public can submit information without identifying themselves or providing a way for EPA to respond.

4.3 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:

None

Mitigation:

N/A

Section 5.0 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.

5.1 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. Only users with sufficient privileges, as given by the program office, can view the results of contact us form for their specific web areas. Only system administrators—there are less than three—can view results of contact us form for the entire site. All "contact us" form results are deleted from the system after 180 days.

5.2 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.

5.3 Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

Contractors, depending on their role, have access to some parts of the "contact form" results. Their contracts comply with the FAR.

5.4 What procedures are in place to determine which users may access the information and how does the system determine who has access?

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.

5.5 Explain how long and for what reason the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

The information is retained for 180 days.

5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes

5.7 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 with the stated purpose and mission of the system.

Privacy Risk:

None.

Mitigation:

N/A

Section 6.0 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.

6.1 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.

6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

N/A

6.3 Does the agreement place limitations on re-dissemination?

N/A

6.4 Describe how the system maintains a record of any disclosures outside of the Agency.

N/A

6.5 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

6.6 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.

Mitigation:

N/A

Section 7.0 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.

7.1 What are the procedures that allow individuals to access their information?

No one from the public has ever asked to access the information they've submitted via a "contact us" from. If someone asks, and it is less than 180 days, the information may be retrievable by querying the database of the DWCMS to send to the requestor.

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

Since the information is submitted by the public, any errors are their own. Since these "contact form" submissions are typically questions to the Agency, the correspondence between the public and the Agency affords an opportunity to correct any errors.

7.3 How does the system notify individuals about the procedures for correcting their information?

N/A

7.4 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:

None.

Mitigation:

N/A

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the system ensure that the information is used in accordance

with stated practices in this PIA?

Periodically, we sweep all pages to ensure that no SSNs or credit card numbers are publicly posted. System Admins also check quarterly that "contact us" form results are deleted. In addition, accounts from users that have left the Agency are deleted monthly.

8.2 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., security awareness, ethic, and FOIA.

8.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

None.

Mitigation:

N/A