EPA United States
Environmental Protection
Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Federal Facilities Environmental Stewardship & Compliance Assistance Center (FedCenter)

Preparer: Stephen Luzzi **EPA Grantee, US Army Corps of Engineers**	**Office: OECA**
Date: 5/13/2019	**Phone: 217-390-0492**

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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f)</u>.

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A)</u> (pgs. 44-45).

Provide a general description/overview and purpose of the system:

FedCenter, located at fedcenter.gov, is a web-based compliance assistance center designed to help federal agencies meet their environmental regulatory compliance needs and improve their environmental performance. The majority of information contained at FedCenter is publicly available to all (non-authenticated), providing program area information and guidance, implementation tools, best practices, etc. across a variety of environmental topics.

FedCenter offers additional services exclusively to federal agencies via membership (login/password authentication.) Those services include private workgroup areas for agency collaboration and document sharing, environmental reporting and tracking utilities, daily newsletter subscription, conference and meeting registration activities, and e-mail list management services.

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?

48 CFR § 17.502-2 - The Economy Act

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 current ATO expires 20 May 2019.

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.

N/A, information collected is not subject to PRA.

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?

Data is stored according to the policies of EPA's National Computer Center (NCC). The NCC determines where data is stored by all systems in the NCC. FedCenter data is currently being stored physically on the host web server, not in a cloud environment.

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).

The system collects a member's name, and business email, address and phone number.

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

The source of the information comes from the prospective member themselves. Information is collected via online membership application, which requests a user's name, agency, agency address, agency phone, and a place for user comments if desired. A privacy statement and link to FedCenter's *Privacy and Security Notice* is on the application form.

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.

When issuing member accounts, the user's business email address is used for identity and communication purposes – thus FedCenter relies on the accuracy of Federal email accounts.

2.5 <u>Privacy Impact Analysis</u>: 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:

A user's name is the only PII collected and it is kept secure from the public via system security controls in compliance with NIST and EPA policies.

Mitigation:

PII is collected via Secure Sockets Layer (SSL) protocols between a user's web browser and the FedCenter web server, which encrypts the contents and provides non-repudiation by the sender. Member accounts are then established by trained staff. The information is then stored in a protected database hosted by the NCC at RTP.

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?

Yes, there are member roles and access controls built into the system that are managed by the system manager. Role assignment is performed by the system manager and trained user managers.

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

FedCenter user policy defines who can be granted access to the private areas of the system and what access control groups a user should be given.

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

No. There are only management accounts (i.e. system manager, user manager, content manager, folder manager, style manager) and user accounts which have assigned roles and responsibilities.

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?

The system manager and user managers are the only ones with access to the user account information in the system. There are no federal contractors with access to this data.

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.

The FedCenter system is categorized under RCS #1044 (B,C,D as applicable), per Catherine Lucas, EPA Records Liaison, FFEO. The information is retained for as long as it is useful for its intended purpose. For example, account information is retained for identification and security purposes for as long as the user's account is in good standing.

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:

None.

Mitigation:

N/A

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:

N/A

Mitigation:

N/A

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 in accordance

with stated practices in this PIA?

FedCenter implements and is in compliance with EPA Privacy Policy CIO 2151.1, and uses NIST privacy controls for privacy protections. The information is collected, handled, maintained, stored and disposed of according this EPA policy and all the NIST controls, including the privacy control family, as stated in the FedCenter System Security Plan (SSP) which is stored and maintained in Xacta. The FedCenter system manager and user managers are the only management personnel with access to PII that is collected by the system (a user's name only), and, the user managers are trained annually by the FedCenter system manager to ensure that the PII information is properly used in accordance with the policies listed above. FedCenter staff may be subject to disciplinary action for failure to take appropriate action upon discovering a breach or for failure to take required steps to prevent a breach from occurring or re-occurring. Users are instructed when receiving a membership account not to provide any personally identifying information in their contact information other than their name, and again are reminded with a posted notice in their profile page as to such requirements.

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

As federal employees of the US Army Corps of Engineers, all personnel is trained annually on the collection, access, use, handling, storage, dissemination and protection of PII. The FedCenter employees are also training annually (required) for *Information Assurance*, *OPSEC*, *Cyber Awareness*, and the *US Army Threat Awareness and Reporting Program*.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

None.

Mitigation:

N/A

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.

FedCenter uses a member's name, along with their business email address, for identification of that individual, to determine if they are eligible to receive a FedCenter user account. User accounts are issued upon request to federal agencies for the purpose of accessing private (subscription) information contained with FedCenter, for private online collaboration purposes, and to receive the FedCenter daily e-newsletter delivery.

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.)

No PII identifier is collected from the user. The user's business email address is the unique identifier used for authentication purposes.

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

None.

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.

Mitigation:

N/A

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

8.4 <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>: