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: Center for Environmental Measurement and Modeling (CEMM) IO Document Tracker	**System Owner: Jim Owens**
Preparer: Jim Owens	**Office: ORD/CEMM/IO**
Date: 7/8/2021	**Phone: (513) 569-7235**
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 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:

The CEMM IO Document Tracker application manages requests for the creation of MOUs, Outside Activity Requests, and FTTA agreements: Cooperative Research and Development Agreements (CRADAs), Materials CRADA (MCRADAs), Materials Transfer Agreement (MTAs) and Non-Disclosure Agreement (NDAs). For each agreement the system tracks general request information for CEMM. The system also tracks the status and workflows of each document creation/review/final signature.

The database may be used to track requests for License and Patent information.

The platform is SharePoint.

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?

Congressionally mandated, EPA Agency-wide program facilitated by ORD to track FTTA and ethic related documentation originating in the CEMM IO.

Congressionally mandated, EPA Agency-wide program facilitated by ORD

15 USC 3710, Utilization of Federal Technology.

15 U.S.C. 3710a. Cooperative Research and Development Agreements.

35 U.S.C. Ch. 18 (Patent Rights in Inventions Made with Federal Assistance), 37 CFR parts 401, 404, and 501

Memorandum of Understanding

- Sections 103(a) and (g) of the Clean Air Act, 42 U.S.C. 7403(a) and (g)
- Sections 104(a) and (b) of the Clean Water Act, 33 U.S.C. 1254(a) and (b)
- Section 8001(a) of the Solid Waste Disposal Act, 42 U.S.C. 6981(a)
- Section 203(a) of the Marine Protection, Research and Sanctuaries Act, 33 U.S.C. 1443(a)
- Section 1442(a) of the Safe Drinking Water Act, 42 U.S.C. 300j-1
- Section 305(a) of the Toxic Substances Control Act, 14 U.S.C. 2665(a)

Outside Activity Request

- 5 CFR 6401 - Supplemental Standards of Ethical Conduct for Employees of the Environmental Protection Agency §6401.103 Prior approval for outside employment

Requests to Collaborate in Research Projects Funded by Another Federal Agency*

- Sectiion 103 of the Clean Air Act (CAA), 42 USC 7403
- Section 104 of the Federal Water Pollution Control Act (FWPCA) (also referred to as the Cleain Water Act), 33 USC 1254
- EPA Ethics Advisory 07-04, EPA Collaboration with Parties Seeking Scientific Research Grants from Other Federal Agencies
- ORD Policies and Procedures Manual 4.C.1, Interaction between ORD Researchers and EPA Grant and Cooperative Agreement Applicants/Recipients

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?

SharePoint platform authorized by OSM/OEI for agency use. The ATO expires October 2021.

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 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?

Yes, the data will be stored in the Agency SharePoint environment. EPA O365 / My Workplace data is physically stored in Microsoft's Global Foundation Services (cloud infrastructure) within continental US data centers and in O365 government cloud community-specific racks for O365. O365 is a SaaS FedRamp approved cloud platform provided by Microsoft.

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).

EPA Staff and supervisor information will be pulled from the Microsoft Global Address List (GAL). The attached documents will contain outside partner organization name, partner technical point of contact, partner signatory, business email address, business telephone number, work address.

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

CEMM Staff employee completes a request form and attached document template. Once document information is reviewed by CEMM IO staff, the review cycle is started. ORD/ORM (FTTA personnel) will review FTTA documents. Office of General Counsel (OGC) may be a reviewer of the documents as well.

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.

Data accuracy is checked at the time the document is submitted. The data is maintained and not modified once signed. A new document would be required to amend the original document to update the data if the data changes.

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:

A potential to access a business partner's personal email or phone number, if they do not have a functional business number.

Mitigation:

No partner information is collected except in the signed document that is attached. We do not enter this content into our database.

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 – SharePoint controls access. The SharePoint environment uses all the extensive access controls, including user and group profiles, permission sets, record-level permissions access controls.

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

We will create user guides to help identify user access. Users consist of the CEMM, ORM and OGC staff.

The SharePoint admins also provides level of access based on guidance from the CEMM IO staff Access is determined through assignment of SharePoint permission sets.

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

CEMM Staff employee completes a request form and attached document template. Once document information is reviewed by CEMM IO staff, the review cycle is started.

ORD/ORM will review documents. Office of General Counsel (OGC) may be a reviewer of the documents as well. Users have different roles/responsibilities and the SharePoint admins provide different level of access as needed.

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?

Only internal access. No contractor will have access to the CEMM IO Tracker.

Privacy Risk:

There is a low risk of over keeping the data longer than needed.

Mitigation:

Will follow the Records Controls by Law to ensure we adhere to all requirements as per 0089, Information Tracking Systems.

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. Information is not shared externally.

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. Information is not externally shared.

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 system allows admin users to assign the document request to users who need to update or sign the document.

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

None other than the annually required Information Security and Privacy Awareness Training. First time users are also trained on CEMM IO Document Application.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

The risk exists that applications being in SharePoint could have inadequate application access controls at the application level. Application owners are accountable to mitigate risks to define role of customer in application.

Mitigation:

CEMM IO Doc Tracker application administrators will manage all risks associated with application access by determining each user's role / access.

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.

The CEMM IO Document Tracker application tracks document requests for the creation of MOUs, Outside Activity Requests, and FTTA agreements: Cooperative Research and Development Agreements (CRADAs), Materials CRADA (MCRADAs), Materials Transfer Agreement (MTAs) and Non-Disclosure Agreement (NDAs). For each agreement the system tracks general request information for CEMM. The system also tracks the status and workflows of each document creation/review/final signature.

The database may be used to track requests for License and Patent information.

The document requestor enters a document request with an attachment of the document template. The request and document are routed throughout CEMM as needed to gather information to complete the document prior to signature. This application provides the status of documents with the updated document attached.

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 has list views that can be filtered, depending on user preference, to present data.The data in the list view(dashboard) is taken from the data in the application: EPA Staff, supervisor information, date of request, date due, request status. The columns in the list view/dashboard can be sorted in ascending / descending order.

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?

There are controls in place to protect PII in the system.
ORD CEMM IO Application Admins have elevated privileges to access system, send requests for review / signature, ad-hoc reporting dashboard.
ORD CEMM IO staff can enter requests, attach documents, review documents and add comments.
ORD/ORM team can modify document, review document and add comments.
OGC team can modify document, review document and add comments.

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 low risk associated to data misuse

Mitigation:

The CEMM IO Document Tracker application will be accessed by authorized users only. Privacy risk mitigation is a function of both the source systems and the SharePoint security plan.

***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: