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: Program & Peer Review Management Information System (P^2RMIS)	**System Owner:** Julie Wanslow
Preparer: Julie Wanslow	**Office:** Office of Science Advisor, Policy & Engagement (**OSAPE)**
Date: 3/10/2021	**Phone:** 202-564-6521
Reason for Submittal: New PIA__✓__ 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:

General Dynamics Information Technology, Inc's (GDIT) P^2RMIS System is a virtual online peer review system that assists in the evaluation and management of applications and proposals that are submitted to the EPA Office of Research and Development (ORD), office of Science Advisor, Policy & Engagement (OSAPE) as part of a competitive peer review process. These research applications are unique from other documents that are typically peer reviewed at EPA in that they are submitted by non-EPA entities; they are not EPA policy documents; they do not represent EPA policy positions; and they are submitted in high volumes and frequency. These applications are subjected to an

external peer review and internal relevance review managed by OSAPE. EPA will be using existing software owned by GDIT and GDIT will customize it for EPA use.

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 following citations for Statutory Authorities permit research grant awards:

- Safe Drinking Water Act, 42 U.S.C. 300j-1, Section 1442;
- Toxic Substances Control Act, 15 U.S.C. 2609, Section 10, as amended by P.L. 106-74;
- Federal Insecticide, Fungicide, and Rodenticide Act, 7 U.S.C. 136r, Section 20, as amended by P.L. 106-74;
- Clean Air Act, 42 U.S.C. 7403, Section 103(b)(3);
- Clean Water Act, 33 U.S.C. 1254, Section 104(b)(3);
- Solid Waste Disposal Act, 42 U.S.C. 6981, Section 8001];
- National Environmental Policy Act, Section 102(2)(F) (for international grant awards).

Additional applicable regulations include: *2 CFR Part 200, 2 CFR Part 1500, and 40 CFR Part 40* (Research and Demonstration Grants).

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?

This will be hosted in the current EPA AWS NHS managed cloud environment. This is managed as a shared service by OMS. There is an ADC in place and they said it will get an Authorize to Use on their system. AWS ECHS ATO Expiration: April 29th, 2023.

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. System and data will be located in the EPA AWS NHS managed cloud environment utilizing their Platform as a Service.

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).

Data extracted from each application includes names of the Principal Investigators (PI) and Co-Investigators (Co-PI), names of the PI and Co-PI institutions (e.g., universities), and collaborators.

For each peer reviewer, the system collects the peer reviewer name and other profile information, and a recent CV (if available). The other profile information that is collected is as follows: e-mail address, contact phone numbers, address including city/state, affiliation/company, and expertise). Although the system collects the names of the peer reviewers for each RFA, the names are not searchable.

Other information contained within the system includes applications submitted in response to Agency solicitations (aka Request for Applications or RFAs), application evaluations from peer reviewers, review records, other material related to evaluation of applications, and supporting data extracted from the applications, including Title of the Proposed Project, Abstracts, and Project Summaries. Other supporting data includes application identification and tracking numbers, RFA Titles, Solicitation Solicitation/Funding Opportunity Numbers, Topic/Subtopic Codes, and Topic/Subtopic Titles.

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

EPA staff (ORD SRO) will send an excel spreadsheet of reviewer names and the other profile information (described in Section 2.1 above) for each panel to GDIT, who will be the contractor managing the P2RMIS system. Then a GDIT script will import these entries into the P2RMIS system where the EPA staff will be able to view the reviewer names and other profile information for a particular panel. Also, the peer reviewers themselves can add or update their own profile information and upload a pdf of their CV (if available) into the system.

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 PII is supplied by ORD staff and/or the peer reviewers themselves and is not acquired externally at all.

2.4 Discuss how accuracy of the data is ensured.

It isn't. Its user supplied. In terms of data integrity, at rest and in transit data are encrypted. We rely on users to supply accurate data since it comes directly from them

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:

Low risk of entering inaccurate data.

Mitigation:

Only required data is entered. If the data is incorrectly entered it will then be corrected either by the contractors managing P2RMIS or by the panelist who access the system.

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. The system has role-based access and can view other user's data only if permissions assigned to their role permits it. All data is denied unless specifically allowed.

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

Roles & Permissions are defined by the P^2RMIS CCB (Change Control Board) and as identified in the Statement of Work for the EPA contract. These are documented in the EPA User guide.

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

Yes. The system has role-based access and can view other user's data only if permissions assigned to their role permits it. All data is denied unless specifically allowed.

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?

Access to the system will be required for EPA staff, contractors and external users as

required. FAR clause is included into their contract.

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.

Yes, EPA Records Schedule1004 and ten (10) years after the file closure. The records are kept for 10 years for auditing purposes.

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:

Risk is associated with keeping the data beyond when it is needed.

Mitigation:

Record retention schedule are followed.

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.

Yes, the information is shared outside of EPA only to authorized users (i.e., the panelists for that particular panel). Only documents related to grant proposals that may include the grantee information such as resumes or contact information are visible and can be downloaded by the panelists and EPA staff in P^2RMIS. Yes, there is an agreement in place.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

Only documents related to grant proposals that may include the grantee information such as resumes or contact information are visible and can be downloaded by the panelists and EPA staff in P^2RMIS to facilitate the review the proposals.

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?

Panel Member Agreements (PMA) that include Conflict of Interest and Confidentiality statements are signed by the reviewers. Security measures are in place to not grant access to the proposal documents prior to signing the PMA.

4.4 Does the agreement place limitations on re-dissemination?

Yes, the language within the Panel Member Agreement prohibits re-dissemination of information.

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:

Breach of PMA by sharing information.

Mitigation:

System records are received by panelists who are selected to evaluate the specific grant. The panelists do not have access to any other grants in the system. The system by design is able to track who receives the records and can track where the breach occurred. There is a log in the system that records who accessed the system.

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 purpose of collecting this information is to facilitate the review the grant proposals, to house reviewer contact information, and ensure reviewers are qualified to evaluate the grant proposals. This is the only reason for collection and use of this data. There is a log in the system that records who accessed the system. Any unauthorized use can be traced by the logs in the system.

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

- User Handbooks & internal Trainings define the privacy.
- Annual required Information Security and Privacy Awareness training is mandatory for all EPA staff.
- Privacy training is also included as part of reviewer orientation.

- Confidentiality agreement in Panel Member Agreement for reviewers where they agree to not disseminate information.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of untimely or improper review of the audit of the logs in the system.

Mitigation:

Scheduled timely review of audit logs will account for the data in the system.

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.

Peer Reviewer data, such as, expertise, CVs, and profile information (described in Section 2.1 above) are stored in the system and are used in making contact with the reviewers via e-mail or telephone, assessing whether the reviewers have the necessary expertise to be on the grant review panel, and in recruiting reviewers for future grant review panels.

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.*)

Information is retrieved by a computer-generated number.

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?

Data is restricted by the assigned permissions in user role. Reviewers cannot see other reviewers' profile. P2RMIS is a role-based system where permissions are defined by user roles. If a role does not have permission to view another user's profile, they will not have visibility to the user's profile. We will be defining these roles for EPA in our subsequent Fit Gap meetings. We do have authenticated access to pages in our application and no user who is not authorized to access a functionality in the system is allowed to do so.

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:

Low risk associated to the data misuse

Mitigation:

System logs permit tracking of information access by user to track misuse.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is requi*red. 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: