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: Small Business Innovation Research Electronic Handbook / SBIR-EHB	
Preparer: April Richards	**Office: ORD/OSAPE**
Date: 9/30/2021	**Phone: 202-564-6462**
Reason for Submittal: New PIA_ _ Revised PIA____ Annual Review_X___ 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:

Commercial Off the Shelf (COTS) software specialized and customized to support the EPA business processes of the Agency's Small Business Innovation Research (SBIR) Program. Technical proposals from small businesses for the SBIR Program are received from outside vendors and uploaded to the system. Users of the system will review the proposals and enter their evaluation. EPA reviewers will access the system, complete a review form and enter a score for each proposal. Reports are created for internal use.

The system will be used to review and score proposals being considered for funding. Users will input answers to multiple questions related to the technical quality and relevancy of the proposal to specified criteria and will score the proposal from 1-100.

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 SBIR program was established under the Small Business Innovation Development Act of 1982 (P.L. 97-219), 15 U.S. Code § 638 (e)(4) Research and development, with the purpose of strengthening the role of innovative small business concerns in Federally funded research and development (R&D).

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. It comes under the ORD Enterprise General Support System (ORD GSS). The ATO expires 11/1/2022.

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?

No, data will be stored in the ORD servers.

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).

Uploaded PDF proposals contain Confidential Business Information and are nonFOIA.

Proposals uploaded in the system will contain the following data: Principal Investigator Name, Business Representative Name, Company Team Names and relative previous employer company names.

Fields entered by the EPA SBIR Program Manager from the proposal (PDF file), table format to save space.			
Year	Phase (status)	Solicitation #	Topic Code

Topic Description	Proposal Title	Company Name	Company Address
Organization Type(LLC, INC, etc.)	Number of Employees	Dollars Requested	Website
Taxpayer ID	DUNS#	Small Business Concerns ID#	Technical Plan
Principal Investigator Position Title	Principal Investigator business phone	Principal Investigator business email	Commercialization Plan
Business Representative business phone	Business Representative business email	Certification / Authorizations (eligibility / characterization) of small business	

Data entered in the system:
Data is entered in fields taken from the proposal information listed above.

Additional data entry includes EPA Reviewer Name

Fields entered by the EPA Reviewer, table format to save space.			
Evaluation score	EPA Reviewer email	EPA Reviewer Organization	Evaluation text
EPA Review Conflict of Interest signed form uploaded in application			

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

Outside small business vendors email PDF files to SBIR Program Manager, applying for EPA grants.

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. System contains data provided by the small business vendor applying for EPA grant.

2.4 Discuss how accuracy of the data is ensured.

The Program Manager enters the data from the small business vendor supplied PDF file and verifies 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:

Data shared with selected EPA internal reviewers. Access controlled by system.

Mitigation:

The system logs show who all logged into the system and when. We can make sure who made the mistake and correct it as needed.

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 three levels of access as described below:

•Program Coordinator (system owner) enters data, uploads PDF file, and assigns Reviewers.

•Reviewer enters review remarks for proposals assigned to them.

•Readers, on a limited basis as needed, have read access for proposal assigned to them.

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

The access control will be documented in the SOP. Refer to 3.1 for the 3 access controls for the system.

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

No

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 EPA employees granted access will be able to access the system initially. May allow EPA contractors access in future. If any EPA Contractors are granted access, the CO will ensure there is

appropriate FAR clause for the contractor(s).

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.

Records retention is for 6 years, and we store the data in one place for historic reference. Currently data is not being purged as we don't have the system yet. EPA Records Schedule is covered by 1004(b).

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:

Information could be retained longer than needed, 6 years. This is a possible risk.

Mitigation:

Record Retention Schedule properly implemented and reviewed.

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.

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:

No risk since the information is not shared with external parties.

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 SBIR Program Manager / Coordinator ensures the PDF file and data required is loaded in the system. We follow the process, and the data is used for evaluating the proposals and nothing else. The system logs show who all logged into the system and when to ensure information is used solely for the intended purposes of collection. We can make sure who made the mistake and correct it as needed.

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

Nothing other than the annually required Information Security and Privacy Awareness Training. First time users will be trained on the new system.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

If routine audits are not conducted, it could lead to unaccounted data.

Mitigation:

There is a proper annual audit in place.

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.

Program Coordinator receives PDF via email. Program Coordinator enter data from the PDF file into separate fields in the system. Program Coordinator assigns a Reviewer. Reviewer reviews the record, enters comments. Program Coordinator completes the record.

The system collects the data and tracks the status of the process.

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.*)

It is retrieved by proposal number (computer generated number) or vendor name.

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?

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:

Information may be misused.

Mitigation:

SBIR Program Manager can review access to ensure appropriate use of data.

*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: