Affects Members Of the Public?	X

Department of Energy
Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, *Department of Energy Privacy Program,* Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	September 29, 2022
Departmental Element & Site	Office of Energy Efficiency and Renewable Energy (EERE) System is operated and managed from DOE Headquarters 1000 Independence Ave SW, Washington, DC 20585
Name of Information System or IT Project	EPIC (EERE Program Information Center)
Exhibit Project UID	019-000001331 00-20-01-12-01-00
New PIA ☐ **Update** X	This PIA is updated as part of the system's annual risk assessment. There have been no changes to the collection and use of PII since the last review in August 2021 and CPO approved PIA in November 2020. The only update is in item #23, where the disposition schedules are added. There are no changes to disposition authorities.

	Name, Title	Contact Information Phone, Email
System Owner	Christine Smith, EPIC System Owner	(202) 586-3556 Christine.smith@ee.doe.gov
Local Privacy Act Officer	Shaida Beklik EERE HQ Cyber Security Program Manager	202-586-4769 Shaida.beklik@ee.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Shaida Beklik EERE HQ Cyber Security Program Manager	202-586-4769 Shaida.beklik@ee.doe.gov
Person Completing this Document	Quyen Tran EERE HQ Cybersecurity support	703-371-9299 Quyen.tran@ee.doe.gov
Purpose of Information System or IT Project	The EERE Program Information Center (EPIC) is a web-based system that supports planning and publication of Funding Opportunity Announcements (FOAs), Notices of Technical Assistance (NOTAs), Lab Calls, Notices of Intent (NOIs), and Requests for Information (RFIs); merit review and selection of awards; negotiation, monitoring, and closeout of financial assistance and lab projects; and budget planning and execution. The purpose of EPIC is to improve EERE's operational effectiveness and efficiency through a single integrated system by providing an information system supporting improved execution of EERE's business processes for managing programs, projects, and data. This will be achieved through the development of a system that automates the day-to-day activities required to develop and maintain EERE's project portfolio while also streamlining the associated business processes to be automated and the data integration points that will be captured between processes.	
	☐ SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number (Taxpayer Identification Number (TIN)) ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☒ Employment Information [Employment History-Resume] ☐ Criminal History	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Name, Phone, Address [Business Contact Information]
	• **Applicant Information (**Name, Phone, Organization, Email Address)
	• **Reviewer Information (**Name, Phone, Email Address, Education, Employer Information, Areas of Expertise)
	
	☒ Other – Please Specify
	• **Organization Information** (Name, Government Business POC, DUNS/UEI, Address, e-mail, and Phone Number)
	• **Project Financial Information**
	  ○ Application Proposed Project Budget & Project Actuals (post-award)
	  ○ EERE Budget Execution Information (planned AFP, costs, obligations)

Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	No; PII is knowingly collected.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	PII will be collected from the application and stored within the system.

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES
3. Is the information about individual Members of the Public?	YES
4. Is the information about DOE or contractor employees?	YES ☒ Federal Employees ☒ Contractor Employees

MODULE I – PRIVACY NEEDS ASSESSMENT

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. seq. 2 Code of Federal Regulations (C.F.R.) 200, as amended by 2 C.F.R. Section 910

MODULE II – PII SYSTEMS & PROJECTS	
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	Non-DOE users (public individuals and organizations) provide information voluntarily if they wish to receive financial assistance from DOE or enter into contracts with DOE. Individuals can choose not to apply or decline to provide information (contact information); however, in doing so they would also decline access to the EPIC system.
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	Yes, contractors are involved with the design, development and maintenance of the system; Privacy Act clauses are included in their contract.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	EPIC does not collect/maintain sensitive PII, like SSN or date of birth, which limits the privacy impact. If the system or data is breached, the impact to the individual's privacy would be low since the PII maintained in the system is business contact (possibly personal contact information in situations in which the Applicant is a sole proprietor) by users who wish to enter into a financial relationship with DOE. EPIC is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls: • Strict access control enforcement based on need-to-know • Security scans
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	PII will be retrieved by the Applicant's first name, last name, and email address.

MODULE II – PII SYSTEMS & PROJECTS	
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	SORN DOE-82- Grant and Contract Records for Research Projects, Science Education, and Related Activities
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A - SORN amendments and revisions are not required.
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	• Information about individuals is provided voluntarily by the individuals (non-organization users). • EPIC also obtains data (i.e., email, name, business name and physical address) from the General Services Administration's (GSA) System for Award Management (SAM); this data is pulled from SAM.gov via search feature when an applicant is registering as an Authorized Organizational Representative. • EPIC also obtains internal DOE employees/contractor information from DOE OCIO Active Directory.
9. Will the information system derive new or meta data about an individual from the information collected?	No. The system will not derive new or meta data about an individual from the information collected.
10. Are the data elements described in detail and documented?	Yes. Data elements are described in the EPIC data dictionary.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	PII is included in submission of applications and will be used as part of the management of awards and to communicate updates to project awardees.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	N/A. No meta-data is derived by the system.
13. With what other agencies or entities will an individual's information be shared?	No information will be shared with other agencies, entities, or third-parties.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	• Reviewers by expertise • Applications including POCs received by Announcement • Applications Reviewed per Reviewer • Projects by Technical lead • Ad hoc reports that contain Business POC
15. What will be the use of these reports?	• Identify highly qualified reviewers • Manage workload of reviewers • Project-tracking and project-funding reports may include point-of-contact business contact information. • Listings of projects assigned to contracting officers and project managers will contain business contact information for those individuals. • Review applications
16. Who will have access to these reports?	The reports will be available to those internal EERE users who have an assigned role such as the Announcement Manager, EERE Project Lead, Technology Officer Director, or a delegate.
Monitoring	

MODULE II – PII SYSTEMS & PROJECTS	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. The system does not have the capability to identify, locate, and monitor individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A. No information is collected as a function of monitoring individuals.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. Although the site/system does not have monitoring capability, EERE and EPIC has implemented security controls to prevent unauthorized users from monitoring or accessing any of the PII on the system (e.g., Access Controls). See the EPIC System Security Plan for more details.
DATA MANAGEMENT & MAINTENANCE	
20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	Information is provided and updated directly from the individuals (non-organizational). The system will prompt applicants to verify contact information at submission of initial or new applications. Registered users always have access to update profile. Data pulled from GSA's SAM system is business organization related and this system is owned/managed by the GSA which has their own completeness system validation process/rules. However, EPIC has in place a nightly job to synchronize the information (i.e. email address to validate the EPIC AOR role) pulled from SAM.gov. EPIC also synchronizes with DOE Active Directory via a nightly job to keep internal data (DOE employees & contractors) current.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	EPIC is only operated at one site, DOE Headquarters at 1000 Independence Ave SW, Washington, DC 20585.
Records Management	
22. Identify the record(s).	Funding Opportunity Announcements: Funding Opportunity Announcements, Notices of Intent, Notices of Technical Assistance, Requests for Information, Lab Calls (DOE National Laboratory Funding Announcements), Funding Opportunity Coversheets. Application submissions: Letters of Intent, Concept Papers, Full Applications, application review comments.

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. ☐ Unscheduled X Scheduled *(cite NARA authority(ies) below)* Grant and Cooperative Agreement Program Management Records GRS 1.2, item 010 (DAA-GRS-2013-0008-0007) Temporary. Destroy 3 years after final action is taken on the file. Grant Cooperative Agreement Case Files GRS 1.2, item 020 (DAA-GRS-2013-0008-001) Temporary. Destroy 10 years after final action is taken on file.
24. Records Contact	Tia Alexander Tia.Alexander@ee.doe.gov 202-586-3135
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	System access is (granted) based on role and upon approval. The System Owner implemented required baseline security controls as appropriate to its FIPS categorization to prevent unauthorized access, modification, and use, in accordance with DOE Directives and the Office of the Under Secretary of Energy Implementation Plan for the Department's Risk Management Approach (Energy Programs RMA IP). In addition, security assessments are conducted on an annual basis using the NIST SP 800-53 methodology. These assessments involve the evaluation of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. Reference the EPIC System Security Plan for more information.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	Based on EPIC system's permissions model and access level, designated DOE internal users and System Administrators will have access to all or part of PII data to perform their duties. Applicants will have access to their own PII that they voluntarily entered into the external facing EPIC site to receive funding from DOE. Applicants can search other external users to share their application and/or add other external users as Technical POC, Business POC and by searching the users by Name or email and will have access to part of PII (First Name, Last Name, email address, association with organization). Authorized Organizational Representatives for any organization/lab will have access to PII of all the users associated with their organization/lab.
27. How is access to PII data determined?	DOE user's access is restricted to the business functions inherent in their roles. Based on the user role, the user may be granted access to one or more modules within EPIC, most likely announcements or project management. Applicants will be required to register in the system to gain access to the announcements module. Within the system, applicants will only be able to see information related to their personal account and organization. Selectees will have access to the project management module and will be limited to their personal account information and projects where they are listed as part of the project team. Internal EERE users will have read-only access to all major modules in the system and access will be single-sign on based on their network credentials.

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	EPIC shares data with the following EERE applications: • EERE Data Center (EDC): This is a one-way data transfer on a periodic basis for reporting purposes. • DOE network Active Directory – This is a one-way data transferred/pulled for account registration purpose and daily data synchronization. • DOE eXCHANGE – This is a two-way connection for sharing announcement data. EPIC also retrieves business/organization data (i.e. name, DUNS number, business email and address) from SAM.gov (System for Award Management) that's owned/managed by the GSA. This is a site that all vendors, grantees, receivers of federal financial assistance, and other entities doing business with the Federal government must register prior to receiving an award. EPIC has a search functionality to pull the existing business/organization data from SAM.gov to support the account registration and approval/validation process. This data pull is via the GSA API gateway and not a direct connection.
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	EDC and DOE Active Directory connections to are internal EERE systems. Therefore, does not require an ISA. The ISA for the EPIC-eXCHANGE interconnection is in place. Data obtained from GSA SAM.gov is via the GSA's API gateway and not a direct connection.
30. Who is responsible for ensuring the authorized use of personal information?	EPIC System Owner
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	**Christine Smith** (Print Name) CHRISTINE SMITH Digitally signed by CHRISTINE SMITH Date: 2022.12.15 13:31:27 -06'00' (Signature)	
Local Privacy Act Officer	**Shaida Beklik** (Print Name) Shaida Beklik Digitally signed by Shaida Beklik Date: 2023.01.10 11:31:48 -05'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2022.12.02 09:06:48 -05'00' (Signature)	