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: https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file

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	July 26, 2023	
Departmental Element & Site	Office of Energy Efficiency and Renewable Energy (EERE) System is located at DOE Headquarters 1000 Independence Ave SW, Washington, DC 20585	
Name of Information System or IT Project	Project Management Center (PMC)	
Exhibit Project UID	019-000000142	
New PIA □ **Update** ☒	Annual review and update. Some specific changes include the removal of TIN collection. When PMC was initially developed, it was used as a pseudo-procurement system by Golden acquisition staff. Since that time, the system is no longer used in that manner and TIN field is no longer generally used in our business process.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Brandy Brooks PMC System Owner	202-287-1868 brandy.brooks@ee.doe.gov
Local Privacy Act Officer	Shaida Beklik 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 Cyber Security Program Manager	(202) 586-4769 Shaida.Beklik@ee.doe.gov
Person Completing this Document	Adam Giannini EERE HQ Cybersecurity support	571-406-5940 adam.giannini@ee.doe.gov
Purpose of Information System or IT Project	The Project Management Center (PMC) is a DOE Office of Energy Efficiency and Renewable Energy (EERE) web-based application that operates as a “virtual hub" of project management information and resources for EERE customers, stakeholders, staff, and contractors. Users must log into to the PMC to access or upload information. Information on PMC is not publicly available. Generally, the PMC has two types of users: external/public user (Applicants, Grant Recipients, and Vendors) and internal DOE employee users, which may include contractors working on behalf of EERE. Public users use the PMC to: ▪ Locate and track funding opportunities; ▪ Access federal forms, regulations, and circulars; ▪ Obtain instructions on preparing and submitting unsolicited proposals; ▪ Obtain informational links for small businesses and inventors and related links to the informative Web sites; ▪ Obtain links for financial assistance recipients for submitting reporting requirements ▪ Submit state master file documents; ▪ Collaborate and share files; ▪ Manage documents and award information; ▪ Upload Federal Energy Management Program (FEMP) documents; ▪ Track and submit National Environmental Policy Act (NEPA) compliance submissions, questionnaires, and determinations; ▪ Obtain information regarding *EERE Network News*, which covers national and international energy efficiency and renewable energy news and events; and ▪ Submit FOIA requests. Internal DOE users use the PMC to: ▪ Track Congressionally-directed projects (“earmarks"), as needed; ▪ Upload and download of project reports and information updates; ▪ Maintain Block Grant Program Environmental Reviews and document uploads; and

MODULE I – PRIVACY NEEDS ASSESSMENT

	▪ Manage Energy Service Company's (ESCO's) contract deliverable repository, including housing a database for DOE to review and retrieve information on the Old and New Energy Savings Performance Contracting (ESPC) IDIQ Contracts for the FEMP Program.
Type of Information Collected or Maintained by the System:	☐ SSN Social Security Number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☒ Other – Please Specify (current employer, role, and title; e-mail address; business and technical points of contact associated with a reward; business and company contact information such as phone and address noted above; and DOE internal users and points of contact). Grant recipients can also provide optional demographic data (e.g., gender, ethnicity, race, and disability status).
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, as PII is knowingly collected.

MODULE I – PRIVACY NEEDS ASSESSMENT

If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

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

If the answer to **<u>all</u>** 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 Organization Act, Title I, Declaration of Findings and Purposes, section 102. 42 U.S.C. 7101 et seq.; 50 U.S.C. 2401 et seq. Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons
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 (individuals and businesses who are members of the public) of the PMC provide information voluntarily if they wish to receive financial assistance from DOE or enter into contracts with DOE or wish to submit FOIA requests electronically. Contact and personal information is only used for the purpose of managing proposals and awards and providing information that non-DOE users have requested. Contact information for DOE contracting officers and their representatives or DOE technical project managers is provided as required by their official roles. If individuals decline to provide their information, they are not allowed to access or use PMC.
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 contracts.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed PMC as a moderate-risk system according to the criteria set forth in Federal Information Processing Standard 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity, or availability be compromised. PMC 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 • System reviews The unauthorized disclosure of information is expected to have adverse effect on organizational operations, organization assets, or individuals. The potential impact on an individual's privacy is minimal, as the PII provided is not considered highly sensitive.
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.**	Information collected from the PMC is only retrievable by project title, award number, and characteristics, such as the funding organization. PII is not retrievable by a name or a personal identifier.
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*.**	N/A. A SORN is not required for PMC, see #5 above.

MODULE II – PII SYSTEMS & PROJECTS	
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Information on individuals is provided voluntarily via online form by the individuals.
9. Will the information system derive new or meta data about an individual from the information collected?	No
10. Are the data elements described in detail and documented?	Yes. Data elements are described in detail in database schema reports.
DATA USE	
11. How will the PII be used?	In general, PII will be used to authorize and validate access to specific information in the system (proposal, project, and funding details; specific FOIA requests; etc.); and to communicate with project participants, project managers, and FOIA requestors.
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
13. With what other agencies or entities will an individual's information be shared?	No information will be shared with other agencies or third-parties. Limited DOE points of contact information (business contact information) will be available to the external project partners for the project(s) in which the awardees/partners are involved.

MODULE II – PII SYSTEMS & PROJECTS

Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Project-tracking and project-funding reports may include points of contact business contact information, which includes name, phone number, email address, and fax number. Optional demographic data (i.e., gender, ethnicity, race, and disability status) collected from grant recipients will also be included in reports after this data has been collected. FOIA reports will contain a list of FOIA requests. The report will also include points of contact information, which includes name, phone number, email address, and fax number. Listings of projects assigned to contracting officers and project managers will contain business contact information for those individuals.
15. What will be the use of these reports?	The reports will be used to facilitate effective project and program management, and to ensure responsiveness to FOIA requests.
16. Who will have access to these reports?	The reports will be available to those individuals who have an assigned role as participants or managers of the projects or who have an oversight or program management role that covers the information being reported.
Monitoring	
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?	None. 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 PMC have implemented security controls to prevent unauthorized users from monitoring or accessing any of the PII on the system (e.g., Access Controls). See the PMC System Security Plan for more details.

MODULE II – PII SYSTEMS & PROJECTS

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 about individuals is supplied voluntarily by those individuals, who will have the capability to update it as necessary by logging in and changing their information.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A – PMC is only operated at one site, DOE Headquarters.
Records Management	
22. Identify the record(s).	The system includes: ▪ Project award and management information, which falls under NARA's GRS 1.2 – *Grant and Cooperative Agreement Records*, items 010, 020, and 030; ▪ FOIA requests, which fall under GRS 4.2 – *Information Access and Protection Records*, item 020; and ▪ NEPA categorical exclusion (CX) filings and their background documents (DOE Environmental Records 2.f.(3)(a) and (c)); NEPA Support Documentation and related determinations (DOE Environmental Records 2.f.(4)). ○ (*The system does NOT contain Environmental Assessments (EAs) or Environmental Impact Statements (EISs) – if needed, those are done outside of the PMC workflow and database.*)

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 ☒ Scheduled *(cite NARA authority(ies) below)* GRS 1.2, item 010 – DAA-GRS-2013-0008-0007 GRS 1.2, item 020 – DAA-GRS-2013-0008-0001 GRS 1.2, item 030 – DAA-GRS-2013-0008-0003 GRS 4.2, item 020 – DAA-GRS-2016-0002-0001 DOE Environmental Records: ▪ 2.f.(3)(a) – N1-434-98-28 ▪ 2.f.(3)(c) – N1-434-98-28 ▪ 2.f.(4) – N1-434-98-28
24. Records Contact	Tia Alexander 202-586-3135 tia.alexander@ee.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	PMC has physical and logical controls in place to prevent unauthorized access, modification, and use. Security assessments are performed on PMC on an annual basis per the methodology in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. 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 PMC System Security Plan for more information.
26. Who will have access to PII data?	PII data will be available to those individuals who have an assigned role as participants or managers of the projects associated with that PII, or who have an oversight or program management role that covers the projects. Limited DOE points of contact business information will be available to the external project partners for the project(s) they are involved.
27. How is access to PII data determined?	PII is made available only to users who are authorized to see information about specific projects. For example, DOE project managers can see awardee information about those projects for which they are responsible, but not about projects managed by others. The system implements role-based access controls.

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	PMC has existing connections with EERE's Corporate Planning System (CPS) and the EERE Data Center (EDC) for reporting purposes. Each connection is a one-way connection where CPS/EDC pulls data directly from the PMC database. The data collected on the PMC site is stored within three databases that reside within the EERE Data Center (EDC). The information is available for reporting or aggregation through Cognos or other EDC tools, subject to role-based access controls. The CPS, EDC, and PMC are all housed within the EERE HQ LAN system.
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?	No ISA is necessary because the connected systems are all within the EERE data center and have the same Authorizing Official and the same security control requirements.
30. Who is responsible for ensuring the authorized use of personal information?	System Owner
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) Brandy T. Brooks Digitally signed by Brandy T. Brooks Date: 2023.11.07 12:29:39 -05'00' **(Signature)**	
Local Privacy Act Officer	(Print Name) Shaida Beklik Digitally signed by Shaida Beklik Date: 2023.11.17 13:10:51 -05'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.11.03 10:25:00 -04'00' **(Signature)**	