Affects Members Of the Public? Mark if Applicable w/ an 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	April 5, 2022
Departmental Element & Site	U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy (EERE). This system is located at the US Department of Energy Headquarters, 1000 Independence Avenue, EERE Server Room, Washington D.C. 20585
Name of Information System or IT Project	Federal Energy Management Program (FEMP) Project Tracking System (PTS), part of the EERE Centralized Web Hosting Environment (ECWHE)
Exhibit Project UID	019-60-02-00-01-5000-04
New PIA [ ] **Update** [X]	This update is part of the annual review process. The last time this PIA was signed by the CPO was 10/17/2018. There are no changes to the collection and use of PII since the last review (May 2021).

	Name, Title	Contact Information Phone, Email
System Owner	Chris Tremper, Program Analyst FEMP	(202) 586-7632 Chris.Tremper@ee.doe.gov
Local Privacy Act Officer	Shaida Beklik, Cyber Security Program Manager (CSPM)	(202) 586-4769 Shaida.Beklik@ee.doe.gov
Cyber Security Expert reviewing this	Shaida Beklik, CSPM	(202) 586-4769 Shaida.Beklik@ee.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

document (e.g. ISSM, CSSM, ISSO, etc.)		
Person Completing this Document	Chris Tremper	(202) 586-7632 Chris.Tremper@ee.doe.gov
Purpose of Information System or IT Project	The Project Tracking System (PTS) provides FEMP staff the ability to actively manage and track their technical and financial assistance, as it relates to the planning and implementation of renewable energy and energy efficiency projects at Federal sites. PTS only maintains personally identifiable information (PII) about Federal employees and contractors working on renewable energy and energy efficiency projects at Federal sites. The PTS will enable technical and financial assistance data to be collected, stored, and reported from a centralized data store. The system is designed to facilitate the coordination of work between people in various practice areas and reporting the status of those projects to upper management. PTS data collected relates to facility energy and water efficiency projects and data related to FEMP funding initiatives, assistance, and research for Federal agencies, including name, email address, and phone number (phone numbers are optional to provide). Some of the funding data is considered procurement sensitive and must remain private and secure. It includes information on all phases of projects including funding breakdowns, facility energy data, workflow milestone dates, agency and facility information (name, location), partner company names, as well as other information related to the assistance process. PTS tracks email addresses of key POC's within its projects.	
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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Employment Information ☐ Criminal History ☒ Name ☒ Other – Email address and work phone number (optional)
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 by the application and stored within the system.
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?	NO
4. Is the information about DOE or contractor employees?	YES ☒ Federal Employees ☒ Contractor Employees

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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	42 U.S.C. § 7101 *et seq*.
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)?**	A valid email address is required to log into the system to perform their assigned job task/function within the system. The first and last names of the system users are saved with the user account. Work phone number is optional to provide. An individual does have the opportunity to decline to provide PII, but he/she will not be able to log into the system to use PTS.

MODULE II – PII SYSTEMS & PROJECTS	
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.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	Names, email addresses, and work phone numbers (work phone numbers are optional) maintained in PTS are low risk and non-sensitive PII. This data is only available to system administrators or individuals designated by the system owner who have oversight responsibility of the project information. PTS 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 • Annual Security assessments • Regularly scheduled security scans • Access Controls If the system was compromised, the potential for privacy concerns is low, as the information is not personal and generally available to the public.
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.**	The username list that contains names and email addresses may be sorted or filtered by the email address or first or last name. However, PII data is not retrieved by the system via a unique identifier. Access to the username list is limited to the PTS system administrator or PTS users designated by the system owner who have oversight responsibility of this data.

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*.**	N/A
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?	The information is provided either directly by the individual (system user) or organizational administrator.
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 a data dictionary and database schema.
DATA USE	
11. How will the PII be used?	Name, work email address, and work phone number are used for system login and to provide the FEMP and agency contact for project information.

MODULE II – PII SYSTEMS & PROJECTS	
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 – The system does not derive meta data.
13. With what other agencies or entities will an individual's information be shared?	The individual's information within the system will not be shared with any other agencies or entities.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Internal reports that list project records associated with a point of contact.
15. What will be the use of these reports?	The reports generated are used to manage and track data related to FEMP's technical and financial assistance as it relates to Federal energy efficiency projects.
16. Who will have access to these reports?	System Administrators and individuals designated by the System Owner who have oversight responsibility of this data will have access to these reports.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system does not identify, locate, and/or monitor individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A – The system does not collect information as a function of monitoring individuals.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes – Although the application does not have monitoring capabilities, EERE and PTS have implemented security controls to prevent unauthorized users from monitoring or accessing any of the PII on the system (e.g., Access Controls).
DATA MANAGEMENT & MAINTENANCE	

MODULE II – PII SYSTEMS & PROJECTS	
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.	Users or PTS Service Area administrators are responsible for updating the email address and/or phone number (phone number is optional to provide) if it changes.
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 – The system is only operated at **one** site which is in the EERE Server Room at DOE's Headquarters location.
Records Management	
22. Identify the record(s).	PTS collects and tracks data related to FEMP's technical assistance as it relates to Federal energy efficiency projects. The type of data includes: High level project and agency information (agency name, POC, project name, project location, project completion status, etc.); and project planning and acquisition information (funding information, project initiation/award dates, efficiency project type, potential energy savings, cost savings, etc.).
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Financial Management and Reporting Records GRS 1.1, item 010 (DAA-GRS-2013-0003-0001) Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.
24. Records Contact	Tia Alexander 202-586-3135 Tia.Alexander@ee.doe.gov
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	PTS has physical and logical security controls in place to prevent unauthorized access, modification, and use. The System Owner has implemented and tested the baseline security controls appropriate to its FIPS categorization, 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). Access controls (username/password, role-based access privileges) are in place to protect the confidentiality and integrity of the PTS data. Access to all PTS content requires identification and authentication. Regularly scheduled security scans are also performed on PTS. In addition, security assessments are conducted on an annual basis using the NIST SP 800-53 methodology.
26. Who will have access to PII data?	PTS System Administrators and PTS users designated by the System Owner who have oversight responsibility of this data have access to PII data.
27. How is access to PII data determined?	The system implements role-based access controls and PII data is made available only to individuals designated by the System Owner who have oversight responsibility of this data.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No – The PTS is a stand-alone application and does not share or access data electronically from any other systems.
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?	N/A – PTS is a stand-alone application and is not connected to any other system. Therefore, an agreement or ISA is not required.
30. Who is responsible for ensuring the authorized use of personal information?	PTS System Owner
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	___Christopher L. Tremper_____ **(Print Name)**  _____ **(Signature)**	**04/11/2022** _____
Local Privacy Act Officer	_____ **(Print Name)** Shaida Beklik Digitally signed by Shaida Beklik Date: 2022.09.29 09:49:03 -04'00' _____ **(Signature)**	_____
W. Ken Hunt **Chief Privacy Officer**	_____ **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2022.09.27 15:31:48 -04'00' _____ **(Signature)**	_____