Department of Energy

Affects Members Of the Public?	**X**

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	4/1/2024
Departmental Element & Site	Office of State and Community Energy Programs, SCEP-10
Name of Information System or IT Project	Performance and Accountability for Grants in Energy (PAGE)
Exhibit Project UID	019-000002824
New PIA ☐ **Update** ☒	This is an updated PIA that documents the use of the EITS Azure Government to host the PAGE System. The last PIA was updated and signed on 8/3/2022

	Name, Title	Contact Information Phone, Email
System Owner	Jay Nathwani Performance and Accountability for Grants in energy (PAGE) SCEP-10	202-510-0854 jay.nathwani@hq.doe.gov

PRIVACY PROGRAM

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Brooke Dickson Director of Privacy Management and Compliance Office of the Chief Information Officer, IM-42	202-287-5786 Brooke.Dickson@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Bright Boateng ISSO Security & Compliance Office, IM-63	347-725-9837 Bright.Boateng@hq.doe.gov
Person Completing this Document	Bright Boateng ISSO Security & Compliance Office, IM-63	347-725-9837 Bright.Boateng@hq.doe.gov
Purpose of Information System or IT Project	Performance and Accountability for Grants in Energy (PAGE) is a web-based Federal information system that is used to collect, organize, distribute, and report information relating to financial assistance awards originating from Energy Efficiency and Conservation Block Grant (EECBG) Program, Weatherization Assistance Program (WAP), and the State Energy Program (SEP) which includes SEP special projects. With the passage of the Bipartisan Infrastructure Law and the Inflation Reduction Act, PAGE now processes Home Energy Rebates, Energy Efficiency and Conservation Block Grant Bipartisan Infrastructure Law (EECBG BIL), Training for Residential Energy Contractors (TREC), WAP Enhancement an Innovation (E&I), SEP Energy Efficiency Revolving Loan Fund (EE RLF), and Codes grants. The application allows DOE to track the performance and accountability for SCEP awarded grants. PAGE has three types of users, Federal, Support users and Grantees. Federal users are federal employees from U.S. Department of Energy HQ and Golden Field Office. Federal users are primarily responsible for reviewing and approving grant plans, Federal Financial Reports and Program Performance Reports, and other reports for Grantees. Support users are system administrators and lastly Grantees are State, territorial, local government and tribal external users that have applied for and received federal grants and as a result are required to submit grant related planning information and report on the status of grants such as costs, milestones, metrics, and qualitative descriptions that collectively provide a view on activity progression. PAGE is not accessible to the public; it requires login, and the system access request is by invitation only.	

PRIVACY PROGRAM

MODULE I – PRIVACY NEEDS ASSESSMENT

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. fingerprint, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☐ Name, Phone, Address ☒ Other – Please Specify Name and Work information (e.g., organizational name, work address, user work phone, alternate work phone, fax number, and user work email address)
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
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

MODULE I – PRIVACY NEEDS ASSESSMENT

2. Is the information in identifiable form?	No
3. Is the information about individual Members of the Public?	YES - "State Territorial, Local and Tribal employees and Contractors"
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.

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

MODULE II – PII SYSTEMS & PROJECTS

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.*; 50 U.S.C § 2401 *et seq.*.**;** 42 U.S.C. § 17152 through 17158; 42 U.S.C. § 6321 *et seq.*; and 42 U.S.C. § 6861 through 6872
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)?**	Grantee contact information is required for all state, local, and tribal entities that seek a grant from DOE/SCEP. Grantees can decline to provide work contact information; however, in doing so the Grantee would also decline the opportunity to obtain a grant from SCEP and to obtain a PAGE account needed to manage their grant. The information is voluntarily provided, as the contact information is provided to SCEP (via the PAGE system) directly from the Grantee. User fields (contact information) are also required for DOE employees and contractors, but individuals can provide organization-level contact information, rather than their individual work contact information. For question submissions via the PAGE Communication Portal, individuals are not required to provide organizational information (e.g., phone number and address), only name and email address would be required. Users can decline to provide name and email address; however, in doing so, the individual would decline the ability to submit a question through the portal.
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 current maintenance life cycle phase of the system and were involved in the design and development of the system. Some PAGE Administrators are DOE contractors. All contractors are required to sign the EITS Rules of Behavior, which covers the security and safeguarding of personal information. Affected contracts include the appropriate Federal Acquisition Regulation (FAR) privacy contract clauses. Privacy Act clauses are included in contractors' contracts.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The system contains the username, user work address, user work phone, and user work email address. The work contact information maintained in PAGE is low risk.

MODULE II – PII SYSTEMS & PROJECTS

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 is retrieved based on a system-generated unique ID for each user profile. From the Contact Management screen, the Administrator can select the desired user which would display the username, user work address, user work telephone, and user work email address. From the User Management module, PAGE Administrators can retrieve user information by login name, first name, last name, grant number, company, email address and/or phone number. Local System Administrators may only retrieve user information for users from their organization.
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*.**	YES. 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?**	Not Applicable. SORN amendments/revisions are not required.

DATA SOURCES

MODULE II – PII SYSTEMS & PROJECTS

8. What are the sources of information about individuals in the information system or project?	Individual-provided. • PAGE Users (Grantees and Federal users) input their work contact information directly into PAGE. New users are sent an email invitation to create a user account on the external public facing side of the PAGE system. Using the link provided in the email, the user enters their work contact information (username, user work address, user work phone, and user work email address) to complete their user profile. SCEP obtains the Grantee's work email address used to send the initial invitation from grant applications, documents, and forms submitted directly to SCEP by the Grantee. • Users submitting questions via the PAGE Communication Portal are required to provide name and email address (entering other contact information, e.g., organizational name and phone number is optional).
9. Will the information system derive new or meta data about an individual from the information collected?	No new or meta data is derived from the system.
10. Are the data elements described in detail and documented?	PAGE has a data dictionary that describes each data element maintained in the system.
DATA USE	
11. How will the PII be used?	The PII is used to serve as an audit trail (who submitted and when) and to identify who to contact for issues or questions.
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	

MODULE II – PII SYSTEMS & PROJECTS

14. What kinds of reports are produced about individuals or contain an individual's data?	PAGE collects and generates: 1. The reports contain username, user work address, user work phone, and user work email address. 2. Monthly Email address archive reports.
15. What will be the use of these reports?	The quarterly reports will be used in managing SCEP's grant programs. These reports are used to track spending of funds and progress of programmatic impacts. The contact information is used to serve as an audit trail (who submitted and when) and to identify who to contact for issues or questions. The monthly email address archive reports are for system disaster recovery purposes only, to contact user in the event the system is not available for an extended period.
16. Who will have access to these reports?	The quarterly, programmatic, and financial reports are available to DOE Project Officers and Grantees. Email address archive reports are available to the PAGE support staff.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system does not identify, locate, and 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, Security assessments are performed on PAGE on an annual basis using the NIST SP 800-53 methodology, which would identify any unauthorized monitoring of individuals.
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.	The data collected is solely through users input and is verified for completeness by DOE officials in the approving process after the information has been submitted. All information is current. Grantees submit grant status reports on a quarterly basis that would include either corrected or accurate, up-to-date, and current contact information. Additionally, annual email reminders are sent to PAGE Local System Administrators to review/update grants and grantees contact 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?	The system is only operated at one site, EITS Azure Government. Therefore, the consistent use of information is assured.

Records Management

22. Identify the record(s).	State, local, and tribal grant applications, records of grant awards, financial data, reports, and records that track the spending of funds and progress of programmatic impacts.
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)* GRS 1.2, item 020 – DAA-GRS-2013-0008-0001
24. Records Contact	Jay Nathwani SCEP-10 U.S. Department of Energy 202-510-0854 jay.nathwani@hq.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?	The PAGE system has controls in place to prevent unauthorized access, modification, and use. Security assessments are performed on PAGE 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. For a detailed description of logical access controls in place, please reference the most recent PAGE System Security Plan (SSP).
26. Who will have access to PII data?	PAGE users will have access to their user profiles, and to view report submission history information for their grants. DOE PAGE users have access to view report submission history for all grants.

The User Management Module is only accessible by PAGE Administrators. Local System Administrators (LSAs) may only view users from their own organization, and the Contact Management function presents the Administrators with a list of the Grantee and DOE Point of Contacts (POCs). |
| **27. How is access to PII data determined?** | Access to the PAGE system is by email invitations only and approved privileges are role-based.

Email invitations are generated (by either a Grantee LSA, Federal LSA, or Web System Administrator (WSA) for new users with a link to setup their account. Local System Administrators would verify/grant access based on role for users (grantees) across their organization only. Grantee users will have access to their user profiles, and to view report submission history information for their grants.

For Federal users, the PAGE Administrator/Helpdesk would create a ticket upon receiving a request and would validate the request and role(s) with the DOE program manager. Once approved, the PAGE Administrator WSA or Federal LSA creates an invitation to be sent to the new user to create an account. DOE PAGE users have access to view report submission history for all grants. |

MODULE II – PII SYSTEMS & PROJECTS

28. Do other information systems share data or have access to the data in the system? If yes, explain.	PAGE has access to data from the DOE Standard Accounting and Reporting System (STARS) and the Strategic Integrated Procurement Enterprise System (STRIPES) through an interface with the I-Manage Data Warehouse (IDW). IDW is the DOE corporate system used to share information with other DOE systems. For the PAGE interface, IDW has a set of views that were setup specifically for PAGE with grant data from STRIPES and vendor payment information from STARS; no PII data is exchanged. It is a one-way interface, with PAGE receiving data from IDW.
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?	There is an ISA for the PAGE IDW connection. The agreement was signed by both parties in May 2022. The ISA will be revised to address EITS Azure Government to hosting the PAGE System.
30. Who is responsible for ensuring the authorized use of personal information?	PAGE System Owner Jay Nathwani 202-510-0854 Jay.nathwani@hq.doe.gov

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	_____ **(Print Name)** _____ **(Signature)**	_____
Local Privacy Act Officer	_____ **(Print Name)** _____ **(Signature)**	_____
Chief Privacy Officer	_____ **(Print Name)** _____ **(Signature)**	_____