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	February 5, 2024
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, EERE Server Room, 1000 Independence Avenue, Washington D.C. 20585.
Name of Information System or IT Project	EERE SharePoint Collaboration Environment (ESPCE) - Customer Service Center (CSC) System
Exhibit Project UID	019-000000139
New PIA [X] **Update** [ ]	

	Name, Title	Contact Information Phone, Email
System Owner	Kyle Fox ESPCE System Owner	240-562-1348 kyle.fox@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 Cybersecurity Support	703-894-6417 Quyen.tran@ee.doe.gov
Purpose of Information System or IT Project	EERE's Customer Service Center (CSC) portal is hosted within EERE's SharePoint environment and used to automate and manage the onboarding process for all new EERE federal employees and contractors. This includes tracking the badging process, tracking provisioning new IT equipment, and tracking of setting up office spaces (via a Dashboard). All data is securely stored within the ESPCE environment and badging forms include additional security restrictions, limiting access to the team responsible for processing. The CSC system is owned by EERE's Workforce Management Office (WMO). They're responsible for processing all onboard, offboard and transfer requests for employees. Onboard requests for new contractors require the upload of badging forms. Upon upload, the badging forms are password-protected and moved to a secure location in SharePoint. The password is automatically emailed to the WMO Security Officer. They may open the badge forms by entering the password. No one else, including system administrators, has access to the passwords. The WMO Security Officer uses the information within the badge forms to enter new employees into USAccess, a system external to EERE. The information will be used to identity proof and register Applicants as part of the Personal Identity Verification process. Failure to submit this information will result in denial of a DOE security badge.	
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, Phone, Address ☐ Other – Please Specify
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 stored on 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?	☒ 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

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; Public Law 95–91; and Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons. Privacy Notice: 42 U.S.C. 7101, 50 U.S.C. 2401 and Public Law 93-579 permit collection of the data requested on form DOE F 206.4. The Office of Personnel Management is authorized to request this information under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U. S. Code. Section 1104 of title 5 allows the Office of Personnel Management to delegate personnel management functions to other Federal agencies. If necessary, and usually in conjunction with another form or forms, this form may be used in conducting an investigation to determine your suitability or your ability to hold a security clearance, and it may be disclosed to authorized officials making similar, subsequent determinations. Your Social Security Number (SSN) is needed to keep our records accurate, because other people may have the same name and birth date. Public Law 104-134 (April 26, 1996) asks Federal agencies to use this number to help identify individuals in agency records.
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)?**	Employees are aware this information is collected during the Onboarding process. Privacy Notices (42 U.S.C. 7101) are included on all forms where employee information in collected. Providing this information is voluntary; however, failure to submit this information will result in denial of a DOE security badge.
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 maintenance of the system. All contractors are required to sign the EERE HQ LAN Rules of Behavior. Privacy Act clauses are included in their contract.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The system contains DOE onboarding information, including sensitive PII (e.g. SSN, employment information, military service, etc.,). This information is high risk PII and the potential for privacy concerns is high if the system happened to be compromised.
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 is stored within the badging forms; these forms are retrievable by the employee's name, so yes, this is an 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*.**	OPM/GOVT-1
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	OPM/GOVT-1
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	The information is sourced directly from the individual.
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 individual's information.

MODULE II – PII SYSTEMS & PROJECTS	
10. Are the data elements described in detail and documented?	N/A. PII is provided via onboarding forms.
DATA USE	
11. How will the PII be used?	PII is used by the Workforce Management Office (WMO) to enter into the USAccess (GSA database) to determine suitability for the issuance of a DOE security badge. The information will be used to identity proof and register Applicants as part of the Personal Identity Verification process. Failure to submit this information may result in denial of a DOE security badge.
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 new or meta data is derived from the PII collected.
13. With what other agencies or entities will an individual's information be shared?	None. There are no sharing with other agencies.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	None
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No

MODULE II – PII SYSTEMS & PROJECTS	
18. What kinds of information are collected as a function of the monitoring of individuals?	None
19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A
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.	PII is provided by the individuals via onboarding forms. These forms will only be stored temporary (60 days). The badge forms are considered Intermediary (temporary) Records and are deleted from the system after 60 days and cannot be retrieved.
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. ESPCE system is only operated at one site, EERE Headquarters.
Records Management	
22. Identify the record(s).	Onboarding information used to determine suitability for the issuance of a DOE security badge.
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)* **Intermediary Records** • Electronic input source records. GRS 5.2, item 020 (DAA-GRS-2017-0003-0002) Temporary. Destroy when 60 days old.
24. Records Contact	Tia Alexander Tia.Alexander@ee.doe.gov 202-586-3135
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	DOE physical, logical access and network security controls protect all data from unauthorized access, modification, or use. Reference the ESPCE System Security Plan (SSP) for more information. Additionally, password protection is implemented on files containing sensitive data.
26. Who will have access to PII data?	Access to PII files with sensitive information is limited to the appropriate/authorized WMO and ITSO Team Members who have the appropriate permissions in the USAccess system.
27. How is access to PII data determined?	Access is restricted to only the authorized WMO team. 1. The user has to be authenticated using DOE Active Directory otherwise they don't get access to the site containing PII 2. To add additional level of security, only individuals granted access to the SharePoint security group based on their role can only enter the SharePoint site and access the library containing encrypted documents. Access control is maintained and administered by the WMO team. 3. Each document has a different password. To view the contents of the document, the user will need access to unique 13-character long password (exclusively held by the WMO team).
28. Do other information systems share data or have access to the data in the system? If yes, explain.	There is an internal connection with the EERE Data Center (EDC). The connection is a one-way interface – where EDC pulls/push the data from and to ESPCE for reporting purposes, such as system usage report. EDC does not have access to or pull PII from the badging documents.
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 required since EDC is part of the EERE HQ LAN system boundary and has the same Authorizing Official and System Owner as ESPCE/CSC.
30. Who is responsible for ensuring the authorized use of personal information?	ESPCE System Owner in conjunction with the CSC portal/site owner.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) KYLE FOX Digitally signed by KYLE FOX Date: 2024.05.23 07:50:00 -06'00' (Signature)	
Local Privacy Act Officer	(Print Name) SHAIDA BEKLIK Digitally signed by SHAIDA BEKLIK Date: 2024.05.23 09:25:53 -04'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2024.05.23 09:02:26 -04'00' (Signature)	