Affects Members Of the Public? ☒

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/0206.1-BOrder/view

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	January 25, 2021	
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)	
Exhibit Project UID	019-000000139	
New PIA □ **Update** ☒	ESPCE PIA	
	Name, Title	**Contact Information Phone, Email**
System Owner	Matthew Hess ESPCE System Owner	720-356-1573 matthew.hess@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 U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy (EERE) SharePoint Collaboration Environment (ESPCE) is a business collaboration platform that is used by EERE federal employees, contractors, business partners and members of the public that have been approved access to the environment. By leveraging SharePoint's capabilities, ESPCE provides access to a centralized repository of EERE-organizational information and applications on the DOE network. ESPCE has been configured to provide support for records management, information sharing, collaboration, automation of business processes and access to features such as document co-authoring and sharing, content management, custom branding, robust search capabilities, custom forms, task management systems, registration tools, advanced reporting, external database connections for legacy applications, custom workflows for EERE business processes, electronic signatures with automated approval processes, and using both local and online Microsoft Office productivity tools such as Word, Excel, Outlook, PowerPoint, Access, and Project.	
Type of Information Collected or Maintained by the System:	□ SSN Social Security number □ Medical & Health Information □ 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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Name, Phone, Address Specifically, first name, last name, office location/room number, business phone, business cell phone, and business email address. ☒ Other – Please Specify IRS 48C Advanced Energy Manufacturing Tax Credit documentation contains EIN and DUNS numbers. This information is no longer being collected, but previously submitted forms are still retained in the system.
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.*	The SharePoint system is scanned/crawled weekly for PII. The shared network drives are scanned/crawled bi-weekly for PII. Email is scanned/crawled daily for PII.
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 I – PRIVACY NEEDS ASSESSMENT

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?**	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.

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)?**	Within ESPCE, there are various business sites/modules that require contact information such as name and e-mail address. An individual does have the right to decline to provide information but will forfeit their right to utilize that tool for that specific business need. PII provided via a custom form is required and handled by form validation and does not allow users to decline as it is needed to submit the form without error. Other PII (contact information for DOE employees and contractors) is sourced from OCIO's Active Directory and not by the individuals, therefore the user does not have the opportunity to decline providing business contact information in ESPCE. IRS 48C Advanced Energy Manufacturing Tax Credit documentation contains EIN and DUNS numbers – applicants voluntarily submitted the documentation and associated information in order to apply for and receive tax credits. This information is no longer being collected, but previously submitted forms are still retained in the 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 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.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The system contains PII business contact information (names, business phone numbers, and business e-mail addresses) and EIN and DUNS numbers (tax credit document no longer collected but retained by SharePoint). This information is low risk PII and the potential for privacy concerns is moderate if the system happened to be compromised.

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.**	Records can be retrieved using PII data elements (information that is tied to a user based on the user's SharePoint profile) using the system's search engine feature.
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. OPM/GOVT–1 – General Personnel Records OPM/GOVT-2 – Employee Performance File System Records OPM/GOVT-5 – Recruiting, Examining, and Placement Records DOE-2 – Personnel Supervisor Maintained Personnel Records DOE-18 – Financial Accounting System DOE-26 – Official Travel Records DOE-28 – General Training Records DOE-33 – Personnel Medical Records DOE-56 – Congressional Constituent Inquires DOE-57 – Congressional Profiles DOE-62 – Historical Files – Published Information Concerning Selected Persons in the Energy Field DOE 82 – Grant and Contract Records for Research Projects, Science Education and Related Activities Records and information maintained within the Record Center site will include copies of records from various systems across EERE for record keeping/tagging purposes. Please refer to the source system/application PIA for system details including SORN coverage.

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?	For external SharePoint sites, information about the individual is sourced directly from the individual. All other contact information about DOE employees and contractors is sourced from Active Directory and the EERE Data Center.
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 individuals information.
10. Are the data elements described in detail and documented?	No, a data dictionary or other documentation does not currently exist that describes the data elements in detail.
DATA USE	
11. How will the PII be used?	PII is used to communicate with individuals to provide them with project updates, contract information, press releases, or user requested information. E-mail addresses are also used as usernames for external users. Business contact information (e.g. phone, business address, etc.) are used for conference/event registration.
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. ESPCE does not derive meta data from the information collected.
13. With what other agencies or entities will an individual's information be shared?	ESPCE does not share data and has no interconnections with 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?	There are no reports produced about individuals from SharePoint. Only SharePoint system usage reports are generated on as needed basis.
15. What will be the use of these reports?	Statistical purposes to identify how many people are visiting the site.
16. Who will have access to these reports?	System Administrators only.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No
18. What kinds of information are collected as a function of the monitoring of individuals?	ESPCE does not have the capability to monitor individuals.
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.	DOE OCIO Active Directory will be automatically updated, and all other records will need to be maintained and kept current by the individual.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	ESPCE is only operated at one site, EERE Headquarters.
Records Management	

MODULE II – PII SYSTEMS & PROJECTS	
22. Identify the record(s).	**Customer Services Information** **Public Relations Information** **Congressional Liaison Operations Information** **Personal Identity and Authentication Information** **Travel Information** **Payments Information** **Staff Acquisition Information** **Benefits Management Information** **Employee Performance Management Information** **Training and Employment Information** **Medical Records – Telework/Leave Request**

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)* **Customer Services Information** • Technical and administrative help desk operational records. GRS 5.8, item 010 (DAA-GRS-2017-0001-0001) Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. **Public Relations Information** • Public affairs related routine operational records. GRS 6.4, item 010 (DAA-GRS-2016-0005-0001) Temporary. Destroy when 3 years old, or no longer needed, whichever is later. • Internal Publications DOE ADMIN 16:1.1.1.a (N1-434-01-8, item 1.1.1a) Permanent. Cutoff file annually. Transfer to NARA 20 years after cutoff. • Speeches DOE ADMIN 14:41.a (N1-434-98-17, item 41a) Permanent. Cutoff at end of fiscal year. Transfer to NARA when 25 years old. • News Media Materials DOE ADMIN 14:42.a (N1-434-98-17, item 42a) Permanent. Cut off at end of fiscal year. Transfer to NARA when 25 years old. **Congressional Liaison Operations Information** • Congressional Hearing Coordination Case files DOE ADMIN 14:55 (NCI-434-83-2(1)) Temporary. Destroy 5 years after close of calendar year in which testimony was given. **Personal Identity and Authentication** • Security/Clearance Access Authorization Case Records DOE ADMIN 18:22.a (DAA-0434-2015-0005(1)) Temporary. Cut off file upon termination of authorization processing, when access authorization is terminated, or when the contract relationship expires. Retire inactive records 5 years after cutoff. Destroy not later than 10 years after date the individual's authorization is terminated or upon notification of death of the individual, whichever is sooner. **Travel Information** • Financial management and reporting administrative records.

	GRS 1.1, item 001 (DAA-GRS-2016-0013-0001) Temporary. Destroy when 3 years old. • Foreign Travel Authorizations DOE ADMIN 9:1.1.a (N1-434-98-12, item 1.1a) Cut off at end of fiscal year. Destroy 7 years after cutoff. **Payments Information** • Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. GRS 1.1, item 010 (DAA-GRS-2013-0003-0001) Temporary. Destroy 6 years after final payment or cancellation. **Staff Acquisition Information** • Job vacancy case files. Records of one-time competitive and Senior Executive Service announcements/selections. GRS 2.1, item 050 (DAA-GRS-2017-0011-0001) Temporary. Under EPI hold. Destroy 2 years after selection certificate is closed or final settlement of any associated litigation; whichever is later. • Job vacancy case files. Records of standing register competitive files for multiple positions filled over a period of time. GRS 2.1, item 051 (DAA-GRS-2017-0011-0002) Temporary. Under EPI hold. Destroy 2 years after termination of register. **Benefits Management Information** • Notifications of personnel actions. GRS 2.2, item 050 (DAA-GRS-2017-0007-0006) Temporary. Destroy when 3 years old. • Employee incentive award records. GRS 2.2, item 030 (DAA-GRS-2017-0007-0003) Temporary. Destroy when 2 years old or 2 years after award is approved or disapproved, whichever is later. **Employee Performance Management Information** • Employee performance file system records. Acceptable performance appraisals of non-senior executive service employees. (Federal Only) GRS 2.2, item 070 (DAA-GRS-2017-0007-0008) Temporary. Destroy no sooner than 4 years after date of appraisal. • Employee performance file system records. Records of senior executive service employees. (Federal Only)

MODULE II – PII SYSTEMS & PROJECTS

	GRS 2.2, item 072 (DAA-GRS-2017-0007-0010) Temporary. Destroy no sooner than 5 years after date of appraisal. • Supervisors' personnel files. GRS 2.2, item 080 (DAA-GRS-2017-0007-0012) Temporary. Review annually and destroy superseded documents. Destroy remaining documents 1 year after employee separation or transfer. **Training and Employment Information** • Non-mission employee training program records. GRS 2.6, item 010 (DAA-GRS-2016-0014-0001) Temporary. Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate. • Individual Employee Administrative and Ethics Training Records (excludes Mission Related Training) - Federal Employees. DOE 2.6, item 015 (DAA-GRS-2016-0014-0003 and DAA-GRS-2016-0014-0002) Temporary. Destroy when 10 years old. • Individual Employee Administrative and Ethics Training Records (excludes Mission Related Training) - Contractor Employees. DOE 2.6, item 16 DAA-GRS-2016-0014-0003 and DAA-GRS-2016-0014-0002) Temporary. Under EPI hold. Destroy 10 years after employee separation OR contract completion (final payment), whichever is later. **Medical Records – Telework/Leave Request** • Telework/alternate worksite program case files. GRS 2.3, item 040 (DAA-GRS-2018-0002-0004) Temporary. Destroy when superseded or obsolete or 1 year after end of employee's participation in program, whichever is sooner. • Reasonable accommodation employee case files. GRS 2.3, item 020 (DAA-GRS-2018-0002-0002) Temporary. Destroy 3 years after employee separation from the agency or all appeals are concluded whichever is later.
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.
26. Who will have access to PII data?	Anyone with DOE network access can access the ESPCE homepage and will have access to PII (contact information maintained in Active Directory). However, individuals who need access beyond the ESPCE homepage will require additional privileges and access. Access to data submitted via custom forms/applications is only available to the "Admins" of that application. For external users, each individual will have access to their own PII data only.
27. How is access to PII data determined?	Anyone with DOE network access can access the ESPCE homepage and will have access to PII (contact information maintained in Active Directory). However, individuals who need access beyond the ESPCE homepage will require additional privileges and access. Internal access is managed by permission groups. The DOE Site Owners and administrators of that site manage access for each SharePoint site. Access to data submitted via forms/applications is only available to the "Admins" of that application.
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 data from SharePoint for reporting purposes, such as system usage report. There is no PII being transferred/pulled from SharePoint.
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.
30. Who is responsible for ensuring the authorized use of personal information?	ESPCE System Owner in conjunction with the SharePoint site owners.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	**(Print Name)**______**Matthew Hess**___ Matthew Hess Digitally signed by Matthew Hess Date: 2022.07.13 08:15:43 -06'00' **(Signature)**	________________
Local Privacy Act Officer	**(Print Name)** Shaida Beklik Digitally signed by Shaida Beklik Date: 2022.08.01 11:31:08 -04'00' **(Signature)**	________________
Ken Hunt **Chief Privacy Officer**	**(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2022.07.01 08:28:47 -04'00' **(Signature)**	________________