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	September 27, 2022
Departmental Element & Site	Bonneville Power Administration (BPA), Headquarters, Portland, OR
Name of Information System or IT Project	Microsoft SharePoint Services
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.
New PIA X **Update**	This is a new PIA for SharePoint Services

	Name, Title	Contact Information Phone, Email
Information System Owner	Yvette Gill, JL Supervisory IT Specialist	503-230-3947 yrgill@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Information Owner	Wilde, Rebecca Supervisory IT Specialist	503-230-4298 rlwilde@bpa.gov
Local Privacy Act Officer	Candice Palen, CGI FOIA/Privacy Act Officer	503-230-3602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Nick Choi, JLS IT Specialist	503-230-5397 hcchoi@bpa.gov
Person Completing this Document	Adrian Williams, JSI IT Specialist	503-230-4259 aewilliams@bpa.gov
Purpose of Information System or IT Project	Microsoft SharePoint (SharePoint) is a commercial off-the-shelf web-based application that integrates with Microsoft Office to provide enhanced communication and collaboration features in addition to document storage. This PIA includes SharePoint 2010, 2016, and 2019. SharePoint Services is a platform for multiple applications and it falls within a larger information system: the General Computing Environment General Support System (Data Center GSS). Both SharePoint and the Data Center are managed through BPA's Office of the Chief Information Officer (OCIO). SharePoint is used by offices, groups, and projects across BPA. SharePoint sites can be set up and tailored for individual BPA organizations and for business processes undertaken by those teams. SharePoint Services includes SharePoint as a platform as well as the feature of Microsoft Project Server, which runs as a service within the SharePoint farm. Project Server is used to manage projects and track the progress of requests. BPA governs information management on SharePoint through a governance team and governance standards. BPA has implemented standards that allow for all types of PII to be stored on SharePoint, with instructions for how to restrict permissions to sensitive PII. Social Securty Numbers are allowed on SharePoint in limited circumstances approved by the BPA Privacy Team. Further privacy analysis is required before collection and storage of SSNs.	
Type of Information Collected or Maintained by the System:	☒ SSN Social Security number ☒ Medical & Health Information e.g. blood test results, vaccination status, health surveys	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ 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 - SharePoint collects PII in unstructured format based on site content owner's discretion.
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.*	Yes, the PII indicated above is known to exist in the system.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Not applicable; system contains PII.

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?	☒ Federal Employees ☒ Contractor Employees

MODULE I – PRIVACY NEEDS ASSESSMENT

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

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	The Bonneville Power Project Act provides administrative authority to contract to fulfill Bonneville Power Administration's mission. SharePoint is essential to increase transparency and communication among BPA employees and contractors, allowing personnel to conduct their work with increased knowledge and efficiency to advance BPA's business mission. (See 16 U.S.C. § 832a(f); 16 U.S.C.§ 839f(a)).

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)?

PII collected for system administration is collected voluntarily from employees when they are onboarded for employment. Consent is onbtained at the source of collection for PII collected by the Site Content Owners for established business functions/purposes.

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 have been involved in both the design and maintenance of SharePoint. Personal information may be disclosed to these contractors in the performance of their contract duties. Contractors are require to safeguard all information in accordance with the Privacy Act and BPA and DOE Policy.

All employees and contractors must complete Cyber Security training prior to being granted network access and yearly thereafter. All employees and contractors are required to complete annual privacy training.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The impact to privacy is high due to the sensitive nature of PII and the volume of data stored in SharePoint.

Confidentiality Factors	Low	Moderate	High
Identifiability			X
Quantity of PII		X	
Date Field Sensitivity		X	
Context of Use		X	
Obligation to Protect Confidentiality			X
Access to and Location of PII		X	
Overall PII Confidentiality Level			X

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.**	There are numerous ways data can be retrieved. SharePoint has built-in searching capabilities which can be queried based on keyword, author, and other relevant information. Documents may be accessed through keyword search of any text or field contained in the document. SharePoint may support specific business processes that require regular retrieval of PII by identifier, including name and BPA identification number ("HRMIS number"). The records generated by those business processes are covered by SORNs. The rule change to permit sensitive PII on SharePoint is recent, some SORNS might be used in the future as teams adapt to this new rule. Some relevant SORNs may include DOE-28 (training records), DOE-77 (physical fitness test records), DOE-26 (travel records), and DOE-11 (emergency call list)
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*.**	No, SharePoint is not covered by a published SORN. Because SharePoint supports many business processes, it can contain PII covered by a number of DOE SORNs. SORNS include OPM/GOVT-1, DOE-2 (personnel records) and DOE-18 (financial records).
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?	Active directory is the only automated source of information. The system receives data directly from active directory. Individual users are also information sources as they upload and store data in SharePoint. This information may occasionally pertain to individuals.
9. Will the information system derive new or meta data about an individual from the information collected?	No

MODULE II – PII SYSTEMS & PROJECTS	
10. Are the data elements described in detail and documented?	Data elements are described in detail in the SSP.
DATA USE	
11. How will the PII be used?	Non-sensitive PII is stored to administrate the system. Sensitive PII is stored to support BPA business processes as needed by Site Content Owners.
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?	None; no individual information will be shared with other agencies or entities.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	The system will be capable of creating an audit report of which pages are accessed most frequently, who contributes most frequently, and other similar data points (i.e. who has access to certain sites). Reports about individuals can be obtained by Site Content Owner at their discretion. Sites with sensitive information MUST have restricted access.
15. What will be the use of these reports?	To verify if sites are still active and to determine if sites have the proper security controls.
16. Who will have access to these reports?	Site Content Owners SharePoint Support Personnel
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?	Not Applicable
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Not Applicable
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.	Administrative PII is kept accurate through automatic updates between Active Directory and HRMIS. Business PII is kept accurate by the Site Content Owners. Content retention and disposal is enforced through the SharePoint Governance document.
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
Records Management	
22. Identify the record(s).	SharePoint does not constitute a Structured Electronic Information System under BPA Policy 236-13, "Overview of Electronic Information Systems." Because almost any kind of unstructured federal record data can be stored on SharePoint, BPA schedules these records according to each organization's individual information asset plan.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Since almost any type of federal record may be stored on SharePoint, there are no specific disposition authorities. The entire BPA Agency File Plan and General Records schedules may be applicable.
24. Records Contact	Information Governance & Lifecycle Management iglm@bpa.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The BPA SharePoint system has been implemented with role-base security process that is applied to each user account. A user must be granted permission to view document by Group. The account structure that implements BPA SharePoint system has been designed to limit access to a site or site module by Group and/or through a direct account.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	All system users are BPA users. Access is strictly controlled based on user group, job responsibility and function. User name and password are required to access data as authorized by the SharePoint Site Content Owner.
27. How is access to PII data determined?	Users manage these access controls to grant permissions and limit sharing of their documents to an individual user or a group based on need-to-know basis as authorized by the Site Content Owner.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	N/A
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
30. Who is responsible for ensuring the authorized use of personal information?	Access is determined through account access procedures. The SharePoint administrator and Site Content Owner are ultimately responsible for ensuring the authorized access to PII.
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	**Yvette Gill** **(Print Name)** YVETTE GILL Digitally signed by YVETTE GILL Date: 2022.11.07 10:49:58 -08'00' **(Signature)**	
Information Owner	**Rebecca Wilde** **(Print Name)** Rebecca L. Wilde Digitally signed by Rebecca L. Wilde Date: 2022.11.07 11:34:29 -08'00' **(Signature)**	
Local Privacy Act Officer	**Candice Palen** **(Print Name)** CANDICE PALEN Digitally signed by CANDICE PALEN Date: 2022.11.07 12:45:27 -08'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2022.11.03 12:14:28 -04'00' **(Signature)**	