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	05/19/2022	
Departmental Element & Site	BPA, Bonneville Power Administration, HQ	
Name of Information System or IT Project	File Servers	
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions	
New PIA ☒ **Update** □	This is a new PIA for an existing system	
	Name, Title	**Contact Information Phone, Email**
Information System Owner	Paul Dickson, JN Infrastructure Service Manager	(503) 230-4075 prdickson@bpa.gov
Information Owner	Benjamin Berry, L	503-230-4072 blberry@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

	Chief Information Officer	
Local Privacy Act Officer	Candice Palen Privacy Act Officer	503-230-5602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Earl Evans Information Systems Security Engineer	503-230-3019 erevans@bpa.gov
Person Completing this Document	Earl Evans and Paul Carr	503-230-3019 erevans@bpa.gov
Purpose of Information System or IT Project	A file server is a computer or dedicated system that holds files available to all users connected to a local-are network (LAN). There are currently fifteen file servers in use. File servers are responsible for the storage and management of data files so that other computers on the same network can access the files. File servers support the BPA mission by allowing for storing, securing and sharing files in the organization. All files are unstructured data, and as such, collection of PII is broad. There is no structured data or structured systems stored on the file servers.	
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 (Potential on HR tickets) ☒ Employment Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Criminal History ☒ Name and work contact information (phone and email) ☒ Other – HRMIS ID and BUD ID
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 known to exist 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?	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?**	The Bonneville Power Project: *Administrative Authority to Contract* (16 U.S.C. §§ 832a(f), 839f(a)) grants the Bonneville Power Administration authority to procure contracts to advance the agency's mission. All PII on the system is approved for collection by the source system authority.
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)?**	Consent for collection of information is sought at the time of collection. Users do not have the opportunity to decline storage of information on the file servers.

MODULE II – PII SYSTEMS & PROJECTS

<table>
<tr><td><b>3. CONTRACTS</b>
<b>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?</b></td><td>Yes. Every CFTE signs a non-disclosure agreement and attestation, and the Privacy Act clauses are included in the contracts.</td></tr>
<tr><td><b>4. IMPACT ANALYSIS:</b>
<b>How does this project or information system impact privacy?</b></td><td>The Privacy Impact is HIGH. File Servers 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
• Encryption
<table>
<tr><th>Confidentiality Factors</th><th>Low</th><th>Moderate</th><th>High</th></tr>
<tr><td>Identifiability</td><td></td><td></td><td>X</td></tr>
<tr><td>Quantity of PII</td><td></td><td>X</td><td></td></tr>
<tr><td>Date Field Sensitivity</td><td></td><td></td><td>X</td></tr>
<tr><td>Context of Use</td><td></td><td>X</td><td></td></tr>
<tr><td>Obligation to Protect Confidentiality</td><td></td><td></td><td>X</td></tr>
<tr><td>Access to and Location of PII</td><td></td><td>X</td><td></td></tr>
<tr><td>Overall PII Confidentiality Level</td><td></td><td></td><td>X</td></tr>
</table>
</td></tr>
<tr><td><b>5. SORNs</b>
<b>How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?</b>
<b>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</b></td><td>The PII is not retreived by identifier in the regular course of business. Files can be searched by identifier, but only identifiers used in the name of the file will be returned in the search. Additionally, access to the servers is controlled by roles, which further limits the access an individual has to files with identifiers.</td></tr>
</table>

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*.**	No, FileServer is not covered by a published SORN. Because FileServer 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?	Users place files onto file servers. The information source varies depending on the needs/purpose of the user and the file share. It can include work from individual or team efforts and/or information extracted from another information system.
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?	An export of the fields of information available can be provided. Portions of the SSP contain types, but not relationships between the data elements.
DATA USE	
11. How will the PII be used?	The use of the information varies depending on the intended purpose by the users or of the individual file share. Authority and purpose for use is determined by the source system/collection.

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?**	Metadata stored with files consists of: • Author of the file • The user who last modified the file in the file share • The time/date of last update and last access • Any special attributes of the file (e.g., read-only) • Other metadata as determined by the application which generated the file.
13. With what other agencies or entities will an individual's information be shared?	None
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	None identified.
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
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A
19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A
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.	Individual users who deposit and use files in file shares as records are responsible for these records to be accurate, relevant, and complete, and for following information handling procedures as documented in the Information Governance series of policies (236-) in the BPA Policy Library.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Files in a file share will exist only in that file share. They can be copied between file shares, but once a copy is created, the new file is managed independently.
Records Management	
22. Identify the record(s).	The File Servers do 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 here, BPA schedules these records according to each organization’s 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 here, there are no specific disposition authorities. The entire BPA Agency File Plan may be applicable.
24. Records Contact	IGLM@bpa.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Access to data in the system is controlled through Role Based Access Control (RBAC) security. Access controls will be tested as implemented. To access data, users must be on a BPA workstation logged on with BPA credentials. File servers are not exposed to the Internet. Data is encrypted in transit. On some file servers (those hosted on the Storage Area Network system), data is also encrypted at rest.

MODULE II – PII SYSTEMS & PROJECTS

26. Who will have access to PII data?	Personal files shares, known as personal drives or H drives, are control by the individual user. Organization file shares, known as Workgroup file shares, have a designated IO who authorizes access to these locations through the use of Role Based Access Controls.
27. How is access to PII data determined?	Access to file shares is determined via role-based access control for the particular file share and purpose.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	File share contents may be backed up via standard backup processes.
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 – file shares are not accessible by external parties or vendors.
30. Who is responsible for ensuring the authorized use of personal information?	Individual users who deposit and use files in file shares are responsible for safeguarding the privacy and security of the information, including PII, in accordance with information handling policies are procedures as documented in BPA Policy 433-1, Information Security and the Information Governance series of policies (236-) in the BPA Policy Library.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) PAUL DICKSON Digitally signed by PAUL DICKSON Date: 2023.03.20 07:08:02 -07'00' (Signature)	
Information Owner	(Print Name) Benjamin L Berry Digitally signed by Benjamin L Berry Date: 2023.04.03 14:55:02 -07'00' (Signature)	
Local Privacy Act Officer	(Print Name) Candice Palen Digitally signed by Candice Palen Date: 2023.04.05 06:59:07 -07'00' (Signature)	
DOE **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.03.17 10:57:31 -04'00' (Signature)	