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-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	May 30, 2024
Departmental Element & Site	Bonneville Power Administration (BPA) HQ, 905 NE 11th Ave, Portland, OR
Name of Information System or IT Project	Internal Services Support System (IS3) – Configuration Management System (CMS)
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 an existing system.

	Name, Title	Contact Information Phone, Email
System Owner	Peter Raschio, TTS Supervisory Electrical Engineer	360-418-2563 pjraschio@bpa.gov
Information Owner	Kim Hunter, TT Supervisory IT Specialist	360-619-6715 kahunter@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Candice Palen, CGI Privacy Act Officer	503-230-3602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Josh Perkins, TTS ISSO	360-418-1729 jiperkins@bpa.gov
Person Completing this Document	Josh Perkins, TTS ISSO	360-418-1729 jiperkins@bpa.gov
Purpose of Information System or IT Project	Internal Services Support System (IS3) – Configuration Management System (CMS) is a configuration management database supporting Control Center systems inventory and their periodic access review process. This is a custom application for managing configuration and access/permissions verification for Transmission Technology asset inventory management. It validates Active Directory user group memberships. The only part of the system that contains PII is the periodic access review component, which is active for ten days per quarter. This component maintains a list of Transmission personnel names, including the User IDs, manager's name, and email address for each person. These reports are generated for the purpose of managing access permissions. Reports are not retrieved by name, but rather by group or role to validate continued access requirements. This is required to comply with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards.	
Type of Information Collected or Maintained by the System:	☐ SSN ☐ Medical & Health Information ☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Criminal History ☒ Name, Email (work). ☒Other – Employee User IDs, Active Directory Group Memberships
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, the above non-sensitive PII is stored on the system during the periodic access review process.
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.

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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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. (Department of Energy Authorization Act) and 16 U.S.C. §§ 832a(f), 839f(a) (Bonneville Project Act)
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)?**	The information is drawn directly from Active Directory so there is no opportunity for consent.
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, the contract contains the necessary Privacy Act clauses.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The overall privacy risk is LOW – minimal non-sensitive PII is collected.

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

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.

No, information is retrieved based off of group or role identification. The reports pulled do contain lists of names associated with email addresses and BPA User Domain (BUD) IDs.

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*.

N/A – reports are not pulled by name or identifier.

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?	Database Infrastructure Systems, manual entry
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?	Yes, in the System Security Plan (SSP).
DATA USE	
11. How will the PII be used?	Managers use the data to verify appropriate cyber access for their employees and contractors.
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
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Group Membership logs for permissions validation.

MODULE II – PII SYSTEMS & PROJECTS	
15. What will be the use of these reports?	Verification of access privileges and revocations for cyber access.
16. Who will have access to these reports?	Managers, Security Privilege Coordinators
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	
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.	System updates from active data at time of permissions review.
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).	System Access additions and revocations for preceding yearly quarter. System Management Administrative Records

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 3.2, item 030 DM-1120 - Destroy when business use ceases. GRS 5.6, item 010 SR-1140. Temporary: destroy when 3 years old but longer retention is authorized if needed for business use
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?	Roles Based Access Controls and lawful government purpose to access the information.
26. Who will have access to PII data?	Managers only have access to information about their own employees, including name, BPA system user IDs, and cyber access privileges.
27. How is access to PII data determined?	Access is determined by Active Directory group membership.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No
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?	Information Owner and Resource Manager (System Administrator)
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) PETER RASCHIO Digitally signed by PETER RASCHIO Date: 2024.08.12 10:26:17 -07'00' (Signature)	
Information Owner	(Print Name) KIMBERLY HUNTER Digitally signed by KIMBERLY HUNTER Date: 2024.08.12 15:53:30 -07'00' (Signature)	
Local Privacy Act Officer	(Print Name) CANDICE PALEN Digitally signed by CANDICE PALEN Date: 2024.08.13 11:42:31 -07'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.08.12 11:07:31 -04'00' (Signature)	