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	04/04/2022
Departmental Element & Site	Bonneville Power Administration Dittmer and Munro facilities
Name of Information System or IT Project	Internal Services Support System (IS3) – Quarterly Access Verification (QAV)
Exhibit Project UID	IS3-QAV
New PIA [X] **Update** [ ]	This is a new PIA for an existing system.

	Name, Title	Contact Information Phone, Email
System Owner	Peter Raschio Information System Owner (ISO)	360-418-2563 pjraschio@bpa.gov
Information Owner	Kim Hunter Director, Transmission Technology, TT	360-619-6715 kahunter@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

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.)	Josh Perkins Information System Security Engineer (ISSE)	jiperkins@bpa.gov
Person Completing this Document	Patricia Cordova	pmtrapani-cordova@bpa.gov
Purpose of Information System or IT Project	Quarterly Access Verification (QAV) is a web application that provides Transmission managers with a quarterly report of which cyber and physical assets can be accessed by each of their direct reports. The purpose of QAV is to capture changes and revocations in access, and to inform the Security Privilege Coordinators of these changes. The previous quarter's privileges are copied to a historical QAV table. For compliance tracking purposes, QAV maintains a list of managers who have completed the current quarter-year reviews. The system is only active for a ten-day period per quarter. QAV maintains a list of Transmission personnel names with their User IDs and manager name. It also maintains Tranmission manager email addresses for the purpose of notification that the quarterly check is required.	
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 ☐ Employment Information ☐ Criminal History	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Name, Email (work). ☒Other – Employee UserIDs, 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.*	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	

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?**	Federal Power Act of June 10, 1920, as amended by Energy Policy Act of 1992 Act of Oct. 24, 1992, and as amended by Energy Policy Act of 2005 Act of Aug. 8, 2005.
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)?**	For BPA and BPA contract resources, there is no opportunity to consent to specific uses or decline to provide information. Information within the system is based on access requests submitted by the employees.

MODULE II – PII SYSTEMS & PROJECTS

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?

QAV is only used internally within the Transmission organization; there is no contract for the system and all internal contractors have Privacy Act clauses in their contracts.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The Privacy Impact is LOW.

	Impact Level		
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		

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.

Yes, information is accessed by name and user ID.

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*.**	DOE-51 – Employee and Visitor Access Control Records
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	No
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, see the SSP.
11. How will the PII be used?	Managers use the data to verify appropriate cyber/physical access for their employees and contractors.

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?**	n/a
13. With what other agencies or entities will an individual's information be shared?	None
14. What kinds of reports are produced about individuals or contain an individual's data?	Managers have access to reports concerning their own employees by Name and User IDs and system access.
15. What will be the use of these reports?	Verification of access privileges and revocations for cyber and physical access
16. Who will have access to these reports?	Managers, Security Privilege Coordinators
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?	No
19. Are controls implemented to prevent unauthorized monitoring of individuals?	No

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.	As the system is active for less than two weeks per quarter, each generation of records is pulled from active data. Stored compliance information is considered historical.
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
22. Identify the record(s).	System Access additions and revocations for preceeding yearly quarter. System Management Adminstrative Records
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?	The Internal Services Support System has an implemented and assessed System Security Plan that documents all appropriate baseline security controls as dictated by its assessed FIPS impact rating, DOE Directives, and Organizational security policies. These controls were assessed and the Authority to Operate granted by the BPA CIO on May 18, 2021.
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/physical access privileges.

MODULE II – PII SYSTEMS & PROJECTS	
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?	Resource Manager (System Administrator)
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	PETER RASCHIO (Print Name) Digitally signed by PETER RASCHIO Date: 2022.12.15 14:26:41 -08'00' (Signature)	
Information Owner	Kimberly A. Hunter (Print Name) Digitally signed by Kimberly A. Hunter Date: 2022.12.21 10:57:53 -08'00' (Signature)	
Local Privacy Act Officer	Candice Palen (Print Name) Digitally signed by Candice Palen Date: 2022.12.28 11:56:30 -08'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	William K. Hunt (Print Name) Digitally signed by William K. Hunt Date: 2022.12.15 14:44:48 -05'00' (Signature)	