MODULE I – PRIVACY NEEDS ASSESSMENT

Date	07/20/2022
Departmental Element & Site	Bonneville Power Administration (BPA) Portland, OR
Name of Information System or IT Project	Transmission Asset Portfolio Management (TAPM)
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
Information System Owner	Yvette Gill Supervisory IT Specialist	503-230-3947 YRGill@bpa.gov
Information Owner	Paula Willhite TPW Supervisor	360-619-6229 plwillhite@bpa.gov
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.)	Jeffrey Gilmour Supervisory IT Specialist	503-230-3425 jbgilmour@bpa.gov
Person Completing this Document	Melinda M. Werner (Mindi) TPW Lead Management & Program Analyst	(360) 418-2396 mmwerner@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Purpose of Information System or IT Project	Transmission Asset Portfolio Management (TAPM) is designed to provide a centralized, 10-year horizon of Transmission (T) Asset Plan Item (API) information from strategy, delivery, and to operationalization of Transmission Assets. The intent of TAPM is for the purpose of planning, project execution preparation, performance tracking, evaluation, and improvement to Transmission assets and associated asset lifecycle. TAPM helps provide API information for planning purposes including past, current and future work. The TAPM Application has five permissioned roles, all managed through a formal request and approval process based on business need. The five permissioned roles "build" on each other (e.g., a Program Planner can do what the View Only & Submitter may do, plus additional features based on business role & need). Each of the five permissioned roles are as follows: • View Only - Any BFTE or CFTE employee, *with the exception of Power Services Marketing Function Employees*, may **request** and may be given read-only permissions for business purposes to the content of TAPM. Specifically, read-only access allows the viewer to reference individual approved APIs, reports and audit logs. • Submitter: Create, edit, and submit API Candidates for acceptance into an Asset Plan by the Lead Program Planner. • Program Planner: Create Candidates, submit Candidates and edit APIs. This user group is primarily made up of Program Managers, Program Planners and Program Coordinators. • Lead Program Planner: Approve/accept and reject API Candidates within their program. This user is primarily a Program Manager. • Project Planner: Edit APIs on Launch tab. This user group is primarily made up of Schedulers.
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"

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name - BPA authorized network account users who specifically have TAPM permissions and/or fulfill various T Asset Lifecycle Program/Project roles are captured for tracking & awareness purposes. ☒ Other – Login Credentials (BUD ID; network Account 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.*	The above-listed PII is known to exist in TAPM.
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

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ 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.

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 Administration Project Act provides the administrative authority to contract out in order to fulfill the BPA mission. TAPM is essential to Transmission's work and information availability associated to the T Assets and Asset Lifecycles. The information provided in TAPM allows BPA-authorized personnel who have specific TAPM permissions to conduct their work with increased efficiency and effectiveness to advance BPA's mission and business at hand. Please see 16 U.S.C. §832a(f).

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)?

Individuals may withhold consent and opt-out of using TAPM – unless it is a job requirement to use the tool for work assignments. If use of TAPM is a tool required by a BPA business role to fulfill the duties and work activities required, the individuals do not have an opportunity to decline to provide their information or limit the use of their information therein. TAPM collects and stores the above-mentioned data elements for both TAPM users and non-TAPM users who are identified as stakeholders on a Project.

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 – All supplemental labor contract employees that are involved with the development and application maintenance, as well as usage – past, current, and future - must sign a confidentiality and non-disclosure agreement before their assignment begins. The applicable Privacy Act clauses are included.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The Privacy Impact rating is LOW.

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**		

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.**	No. PII is not retrieved by name in the regular course of business.
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
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?	The application receives the name from the BPA Active Directory as the source 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?	Yes, the data elements are described in the System Security Plan.

MODULE II – PII SYSTEMS & PROJECTS

DATA USE	
11. How will the PII be used?	The PII is used to administer the system.
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. This is an internal BPA Use Only Application. TAPM is stored on BPA Servers; accessed by BPA only network authorized personnel that have additional approved TAPM specific access.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	The network account information is used by internal BPA-approved reporting mechanisms only (e.g. PowerBI, Excel, Print Screen & Paste) These reports indicate only the name of specific stakeholders on projects not information about the stakeholders themself.
15. What will be the use of these reports?	Reports are used for business processes and management decisions for resource allocation.
16. Who will have access to these reports?	All BPA has access to the reports.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	N/A, the system cannot locate or monitor individuals.
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

MODULE II – PII SYSTEMS & PROJECTS

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.	The records about individuals are generally pulled from other systems, and therefore accuracy, relevance, and completeness are maintained in the source system (BUD active directory).
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).	TAPM provides a centralized, 10-year horizon of asset program information from strategy through delivery to execution for the purpose of planning and project execution preparation.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	N1-305-07-001-11c FE-1300 - Destroy 10 years after the records are closed.
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?	TAPM has role-based access: Administrator, User, Viewer. Access is determined by role and need to know.
26. Who will have access to PII data?	Administrators (name and BUD ID) Users (name only) Viewer (name only) All users of the system can see the name only of persons who are stakeholders on a project but no other information about the stakeholder.

MODULE II – PII SYSTEMS & PROJECTS	
27. How is access to PII data determined?	The PII data captured in TAPM is BPA Personnel with authorized use of the application; support team; business and IT Technical personnel.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. TAPM is on the BPA internal platform and the information stored/accessed/used in TAPM available within the "BPA cube" whereby authorized BPA NT Account Users may leverage the TAPM data for BPA Only, Authorized user for internal reporting.
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?	Yes.
30. Who is responsible for ensuring the authorized use of personal information?	The Information Owner
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	YVETTE GILL **(Print Name)** Digitally signed by YVETTE GILL Date: 2023.02.13 09:53:56 -08'00' **(Signature)**	
Information Owner	Paula Willhite **(Print Name)** Digitally signed by PAULA WILLHITE Date: 2023.02.16 10:28:52 -08'00' **(Signature)**	
Local Privacy Act Officer	Candice Palen **(Print Name)** Digitally signed by Candice Palen Date: 2023.02.16 12:57:24 -08'00' **(Signature)**	
DOE Chief Privacy Officer	William K. Hunt **(Print Name)** Digitally signed by William K. Hunt Date: 2023.02.10 10:45:57 -05'00' **(Signature)**	