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	2/10/2023	
Departmental Element & Site	Bonneville Power Administration HQ, Portland OR	
Name of Information System or IT Project	Outage Management System (OMS) BAE-GSS	
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 a new system. It may replace DART and SCOUT.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Peter Raschio Information System Owner (ISO)	360-418-2563 pjraschio@bpa.gov
Information Owner	Michelle Cathcart Vice President, Transmission System Operations, TO	360-418-8775 mmcathcart@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.)	Daniel Akzinor Information System Security Officer (ISSO)	360-418-8669 DLAkzinor@bpa.gov
Person Completing this Document	Jeffery Gilmour	503-230-3425 jbgilmour@bpa.gov
Purpose of Information System or IT Project	The Outage Management System (OMS) standardizes and automates outage submission, tracking, and coordination for any generator in the Balancing Authority (BA) or transmission within the Transmission Operators Authority. It integrates with the Reliability Coordinator's outage system and other applications including Outage Tracking System, and for a defined period of time, the Daily Activity Record Tracking (DART). It supports advanced reporting requirements and facilitates analytics for outage management. It also positions BPA to integrate with the Western Energy Imbalance Market (EIM)/CAISO. Further it integrates an Operations Logging System with the Outage Management System that can be used by all operators (generation logging pending further investigation) managing the BA functions to log their relevant events, activities, and decisions throughout the day. For the purposes of dispatching personnel for outages, the system collects name and contact information for members of the public. It collects name, contact information, and employee ID for BPA personnel.	
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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address, Email (work and personal). ☒ Other – Employee 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.*	N/A—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?	YES
4. Is the information about DOE or contractor employees?	YES or NO (If Yes, select with an "X" in the boxes below) ☒ Federal Employees ☒ Contractor Employees

If the answer to **<u>all</u>** 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 I – PRIVACY NEEDS ASSESSMENT

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?**	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.

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)?

For BPA and BPA contract resources, there is no opportunity to consent to specific uses or decline to provide information. For resources and points of contact from other utilities or companies with which BPA does business, the consent is granted when points of contact information are requested by BPA. PII is manually entered after being collected over the phone or by email.

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 system support team at BPA consists of a mix of BPA and contracted supplemental labor. The contract with the vendor contains the information protection and assurance clauses.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

There is a low impact to privacy.

	Impact Level		
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 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.**	BPA emergency contact information will be retrieved by name consistent with SORN DOE-11 Emergency Operations Notification Call List in the Federal Register. Non-BPA point of contact information will not be retrieved by personal identifier 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*.**	Yes. SORN DOE-11 Emergency Operations Notification Call List in the Federal Register.
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	No
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Data sources limited to Peopledata (Active directory domain), or sourced from external entities through direct request.
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 System security plan describes the data types involved with authorizations, tagging and the station callout and contact book features of the OMS.

MODULE II – PII SYSTEMS & PROJECTS

DATA USE	
11. How will the PII be used?	The information is used by real time dispatchers and BPA personnel to support two main functions. The first function is the authorization and tagging process which is used to assign individuals to responsibilities in support of equipment outages. The second purpose is to provide real-time dispatchers and other control center personnel the ability to quickly contact field or other support resources during emergencies or in the course of daily operations. The PII is not used for system authentication. OMS is single-sign on.
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?	Information is not shared with other agencies or entities through normal course of business.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	None
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	RT Dispatchers, Outage Office, and field office personnel who maintain the data have access to the data, but there are no formal reports. Exports are available via the application user interface.
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?	N/A – the data is not used to monitor individuals
19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A – the data is not used to monitor individuals
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). However, there will be internal unique PII data collected by request that will be reviewed annually for accuracy by field support staff.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	While the system will be accessible from multiple locations, there will only be one production database where record updates occur. There will be a backup database to ensure business continuity in case of a main database failure. Application administration will occur within the Outage Management System and comprehensive training will be provided to ensure consistent data entry and capture.
Records Management	
22. Identify the record(s).	System of Record for SLIMs, Outage and Dispatch log information. Record types: ppt, pptx, bmp, doc, docx, pdf, rtf, xls, xlsx, zip, gif, jpg, png
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	N1-305-07-001-4d TL-1400 - Destroy 30 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?	Access controls are defined in the system security plan, but essentially only those within specific application roles can view the data and a different role(s) to modify the data.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	Data in the system is restricted using a role-based authorization model, but essentially real time dispatchers, outage office, senior dispatchers, field personnel and system adminstators will have access to the PII data.
27. How is access to PII data determined?	Data in the system is restricted using a role-based authorization model. Membership to the roles is authorized by the information owner (and delegates) or the information system owner (and delegates) and tracked through CRM requests for role membership.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes, there are several information systems that exchange information from the Outage Management System including Outage Tracking System, Integrated Curtailment and Redispatch System (iCRS), Daily Activity Record Tracking (DART), California Independent System Operator's (CAISO) Web Outage Management System (WebOMS), Outage Analysis and Reporting System (OARS) and Outage Tracking System (OTS)
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?	No
30. Who is responsible for ensuring the authorized use of personal information?	Information Owner
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) PETER RASCHIO Digitally signed by PETER RASCHIO Date: 2023.03.09 10:57:26 -08'00' **(Signature)**	
Information Owner	(Print Name) MICHELLE CATHCART Digitally signed by MICHELLE CATHCART Date: 2023.03.10 16:58:31 -08'00' **(Signature)**	
Local Privacy Act Officer	(Print Name) Candice Palen Digitally signed by Candice Palen Date: 2023.03.13 08:34:06 -07'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.03.08 09:19:35 -05'00' **(Signature)**	