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	10/27/2022
Departmental Element & Site	BPA Headquarters 905 NE 11th Ave, Portland, OR
Name of Information System or IT Project	Data Integration and Reporting-Cloud Integration Services (DIR-CIS)
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 a new system

	Name, Title	Contact Information Phone, Email
Information System Owner	Yvette Gill Supervisory IT Specialist	503-230-3947 yrgill@bpa.gov
Information Owner	Rebecca Wilde Supervisory IT Specialist	503-230-4298 rlwilde@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Candice Palen Privacy Act Officer	503-230-5397 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Nick Choi IT Specialist	503-230-3680 hcchoi@bpa.gov
Person Completing this Document	Pankaj Pabla IT Specialist	503-230-4045 ppabla@bpa.gov
Purpose of Information System or IT Project	DIR-CIS integrates data between BPA databases, files and applications. The data remains on premise and applications are only connected after an Authority To Operate (ATO) process. This is a backend application with only Elevated Privlege User (EPU) accounts. The Integration service provides “pipes” to safely transport data; it does not examine or store the data being integrated. The only data stored in the cloud is the meta-data specific to the integration “jobs,” descriptive data that might include an assigned job name or number. The only PII is the user account ID for the approximately 10-15 people who work with CIS. No PII data is retrieved from the system.	
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 ☒ Name, Work Phone and work email address	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Other – EPU accounts names
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, the system stores PII
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?**	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.
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)?**	Individual consent is not requested. Users must access the system to perform job functions.
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, this is a SaaS and the relevant Privacy clauses are included in the contracts.

MODULE II – PII SYSTEMS & PROJECTS

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**		

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.

N/A

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

MODULE II – PII SYSTEMS & PROJECTS	
8. What are the sources of information about individuals in the information system or project?	Username assignments are created in the system since direct Active Directory Authentication is not supported. Data Fields: First name Last Name Job Title - set to N/A Phone Number - set to 503-230-0000 Email for sending alerts about jobs EPU SAML Account Name
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, documented in System Security Plan.
DATA USE	
11. How will the PII be used?	The PII is used to authenticate users to the system, and provide email communications of issues with the services or processes.
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?**	Only login/logout information is stored in the system. No personal records are stored in the system.
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?	System access audit report
15. What will be the use of these reports?	Validate system access

MODULE II – PII SYSTEMS & PROJECTS	
16. Who will have access to these reports?	System Administrators
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.	Quarterly audit with manual validation
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).	User Login/Logout information
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	CA-1125 - Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
24. Records Contact	IGLM@bpa.gov
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
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.
26. Who will have access to PII data?	RBAC limits access to administrators of the system.
27. How is access to PII data determined?	System administrators are the only ones capable of accessing PII data.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	None. The nature of the system is that control is at the platform level. The data stored is the metadata for the systems connected to CIS and therefore doesn't provide information associated to specific records.
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?	There is an existing ISA for the system between BPA and Informatica which has been approved. BPA System system administrators are the only ones capable of accessing PII data related to login activity to CIS.
30. Who is responsible for ensuring the authorized use of personal information?	System Administrators
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	YVETTE GILL **(Print Name)** Digitally signed by YVETTE GILL Date: 2023.02.13 15:01:30 -08'00' **(Signature)**	
Information Owner	Rebecca L. Wilde **(Print Name)** Digitally signed by Rebecca L. Wilde Date: 2023.02.22 09:58:33 -08'00' **(Signature)**	
Local Privacy Act Officer	Candice Palen **(Print Name)** Digitally signed by Candice Palen Date: 2023.02.22 10:51:25 -08'00' **(Signature)**	
DOE Chief Privacy Officer	William K. Hunt **(Print Name)** Digitally signed by William K. Hunt Date: 2023.02.10 10:42:15 -05'00' **(Signature)**	