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 1, 2024
Departmental Element & Site	Bonneville Power Administration (BPA) HQ, 905 NE 11th Ave, Portland, OR
Name of Information System or IT Project	BPA Application Analytics (Analytics)
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 internal application.

	Name, Title	Contact Information Phone, Email
System Owner	Yvette Gill, JL Supervisory IT Specialist	503-230-3904 yrgill@bpa.gov
Information Owner	Justin Steel, JLSC Supervisor IT Specialist	503-230-3854 jasteel@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.)	Nick Choi, ISSO	503-230-5397 hcchoi@BPA.gov
Person Completing this Document	Steven Cupp, IT Specialist	503-230-3761 sdcupp@bpa.gov
Purpose of Information System or IT Project	BPA Analytics tracks usage of approximately 10 of BPA's internal applications (e.g. Rates Analysis Module (RAM), Service Point Profile (SPP)) in the Agency Commercial System portfolio by logging activity to a centralized location. BPA Analytics logs access including username to the following applications: Catalog Search, Commercial Business Support Application (CBSA), Customer Contracts Management (CCM), Customer Data Management (CDM), Foreign and Joint Owned Ratings Data (FJORD), Hazardous Waste Tracking (HazTrac), Rates Analysis Model (RAM), Asset Suite (PassPort) Shipping Bolt On Shipping, Service Point Profile (SPP), Transmission Asset Portfolio Management (TAPM), and Tower Steel System (TSS). This is data concerning the usage of websites that are connected to Analytics, such as: pageviews, user names, timestamps, browser version, IP addresses, Operating System and monitor's screen resolution. For the previously identified applications BPA Application Analytics displays the site usage data including pageviews, user names, timestamps, browser version, IP addresses, Operating System and monitor's screen resolution. This mimics what Google Analytics collects regarding website visits. At this time the only information leveraged is the pageviews to ensure that the applications are being used. Usernames are only collected if the application is individually configured to send the user names.That information is then graphed for ease of consumption and visualization. Graphing of site activity is consistent with Google Analytics and can provide web designers and administrators with information to improve the accessibility of the site. However, since the applications are all internal to BPA and used internally to BPA the primary use of the graphing is to develop a trend of the site's use over time. This type of data is particularly useful in tracking how applications are being used. For example, is the cadence of use seasonal, monthly or infrequent? Who are the highest value users and what pages are they frequenting? This information can also help identify an application for retirement. PII collected is BPA employee and contractor usernames.	

MODULE I – PRIVACY NEEDS ASSESSMENT

	(BPA internal note: AIM ID is 1246)
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 ☐ Criminal History ☐ Name, Phone, Address ☒ Other –BPA User IDs
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 – system contains non-sensitive PII identified above.
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

MODULE I – PRIVACY NEEDS ASSESSMENT

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.

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?**	Department of Energy Authorization Act, Title 42 United States Code (U.S.C.) Section 7101, et seq. The Bonneville Power Project: *Administrative Authority to Contract*, Title 16 U.S.C. § 832a(f), 839f(a) grants BPA authority to procure contracts to advance the agency's mission.

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)?

Consent is derived through use of the monitored websites by all BPA application users. All BPA system users are warned of monitoring at log-in, and consent is assumed when the network is accessed.

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?

The contract contains the necessary Privacy Act clauses.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The overall privacy risk is LOW – minimal PII is collected related to a small number of applications.

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.**	N/A – information is not retrieved by identifier in the normal 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?	BUD User IDs from Active Directory, no internal accounts for the 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
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	BPA Applications Analytics logs BPA User ID for authentication purposes. Application Analytics doesn't use the PII collected, it merely logs it for site usage analysis, looking at the number of visitors rather than the specifics of individual visitors for the purpose of determining whether to continue maintaining specific software applications or retiring them.
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?	System usage reports for limited applications
15. What will be the use of these reports?	Identification of system for retirement or ensuring the appropriate amount of licenses are applied.
16. Who will have access to these reports?	Administrators of the system
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes
18. What kinds of information are collected as a function of the monitoring of individuals?	Data concerning the usage of websites that are connected to Analytics, such as: pageviews, user names, timestamps, browser version, IP addresses, Operating System and monitor's screen resolution.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes, RBAC for administrators and limited set of applications are monitored.

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.	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).	Analytics data is information about views of web sites, including pageview counts, user names, timestamps, browser configurations, IP addresses, and any other types of usage information the website owner chooses to send. This captures how many people are using a web site and what pages they are viewing.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. ☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* GRS 3.1, DM-1260 destroy 5 years after the project/activity/transaction is completed or superceded.
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 system uses Active Directory and authorized access is controlled through BUD ID. Furthermore, access is turned off by default and granted only for those with a lawful government purpose.
26. Who will have access to PII data?	Applications Analytics Administrators
27. How is access to PII data determined?	Based on lawful government purpose

MODULE II – PII SYSTEMS & PROJECTS	
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
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) YVETTE GILL Digitally signed by YVETTE GILL Date: 2024.08.13 10:11:48 -07'00' (Signature)	
Information Owner	(Print Name) JUSTIN STEEL Digitally signed by JUSTIN STEEL Date: 2024.08.13 10:40:22 -07'00' (Signature)	
Local Privacy Act Officer	(Print Name) CANDICE PALEN Digitally signed by CANDICE PALEN Date: 2024.08.13 11:18:18 -07'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.08.12 11:00:27 -04'00' (Signature)	