Affects Members Of the Public?	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	11/30/2021
Departmental Element & Site	Department of Energy (DOE) Bonneville Power Administration (BPA) Portland, Oregon
Name of Information System or IT Project	Financial Management System (FMS) by PeopleSoft/Oracle
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.
New PIA ☐ **Update** X	This is an updated PIA for an existing system. This PIA further elaborates on how this system handles real-time visibility and transparency into the financial impact of "what-if" scenarios enabling optimal decision making that maximizes financial positions and positively impacts the bottom line.

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

MODULE I – PRIVACY NEEDS ASSESSMENT

Information Owner	Valerie Gonzales Darling	(503) 230-5018 vsgonzales@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.)	Nick Choi Information System Security Officer	503-230-5397 hcchoi@bpa.gov
Person Completing this Document	Valerie Gonzales Darling	(503) 230-5018 vsgonzales@bpa.gov
Purpose of Information System or IT Project	The Financials Management System (FMS) supports the overall financial planning, accounting, treasury, and financial reporting for the Federal Columbia River Power System (FCRPS) and the Bonneville Power Administration (BPA). Its mission includes the delivery of financial information in a consistent manner that is useful, relevant, reliable, verifiable and comparable to executives, managers and analysts throughout BPA. BPA managers and staff use FMS to make business decisions and respond to information requests. The system also supports real-time visibility and transparency into the financial impact of "what-if" scenarios enabling optimal decision making that maximizes financial positions and positively impacts the bottom line. The system includes: • Accounts Payable – voucher creation, payment processing, U.S. Treasury interface, ETS/2 interface, EET invoice processing, REP invoice processing, AS invoice processing; • Residential Exchange Program – REP customer and rates maintenance, RPSA integration, REP load and invoice approval processing; • Accounts Receivable – item maintenance, payment collection, customer aging, U.S. Treasury (Pay.Gov & CIR – Collections Information Repository) interfaces; • Asset Management - financial management of assets, including asset transactions, depreciation, and accounting;	

MODULE I – PRIVACY NEEDS ASSESSMENT

	• Billing – customer invoicing for reimbursable projects and miscellaneous goods/services. (Three types of bills: Customer Bills, Project Bills, Miscellaneous Bills.); • General Ledger – financial records, BPA reporting, Federal reporting; • Project Costing - asset costing, project setup, project transaction management. (Keeping Asset Suite and PeopleSoft project info in sync – Overall Project Dates, Project status, activities [dates and status], Project Manager); • Deal Management - capture Treasury bond and investment information and generate accounting entries; • Lease Administration - storing financial terms of lease agreements for 3rd party financing leases; • Purchasing – storing Supplier Contracts and Receiving data to support matching and payment of invoices (limited license); • Suppliers – supplier maintenance (including bank details for EFT, and address info for Check payments), support Accounts Payable, 1099 reporting; • Customers – store customer data (CDM – Customer Data Management interface), maintain customer bank details, support Billing and Accounts Receivable. (Keeping CDM and PeopleSoft in sync with Primary Address information, Tax ID info); • Customer Contracts – customer contracts maintenance for reimbursable projects, support Billing and Project Costing. • The system collects and stores financial information (including SSNs), names, and contact information for BPA personnel and members of the public.
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

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ 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, Phone, Address ☒ Other – Taxpayer Identification Numbers (TINs). In some instances, FMS collects and stores SSNs for business owners who are sole proprietors (in place of the TIN), and for employees who are paid as vendors of BPA.
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 above listed PII is known to exist in the system.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A - the system contains PII. Querying the tables within the supporting database demonstrates the existence of TIN/SSN, bank account numbers, first/last names and addresses.

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

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ 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?**	The Bonneville Power Project Act provides administrative authority to contract to fulfill Bonneville Power Administration's mission. The Financial Management System is essential to BPA's financial operations and to advance BPA's business mission. (See 16 U.S.C. 832a(f); 16 U.S.C. 839f(a). FMS is also authorized by the Debt Collection Improvement Act (31 U.S.C. 3701, et seq.).

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)?**	In order to make or receive payments to/from BPA, individuals must provide addresses, SSNs, and financial information to meet requirements for processing and reporting. Individuals consent through active participation when providing PII. Individuals who decline to provide information cannot make or receive payments.
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 Master Agreement with Contractors includes the following privacy Clause: "The contractor agrees to: (1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals. (2) Include this clause in all subcontracts awarded under this contract which required the design, development, or operation of such a system of records. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor and any employee of the Contractor are considered to be employees of BPA."

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The Privacy Impact is HIGH.

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.

Data regarding a vendor (employee or contractor, current or past) is accessed using the individual's name.

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-18 Financial Accounting System (74 FR 1020).

DOE-26 Official Travel Records (74 FR 1026).

MODULE II – PII SYSTEMS & PROJECTS	
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?	Individuals are entered into the system by data processors using information provided by the individuals. There are PII data from Peopledata web service and Customer Data Management (CDM) systems.
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 and documented in the System Security Plan (SSP)
DATA USE	
11. How will the PII be used?	The PII is used to ensure the accurate processing and recording of payments/invoices to individuals, and reporting of withholding data for 1099 purposes.
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?	The data will be shared, only as required by law or regulation, with the U.S. Department of Treasury for AP payment schedule files and the U.S. Department of Revenue Services for 1099 reporting.
Reports	

MODULE II – PII SYSTEMS & PROJECTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Queries have been built for users who have access to Vendor data to look up data for business purposes (contracting officers, vendor team). The banking and TIN data are not made available through these queries. Only the Vendor Maintenance team and the Business Analysts supporting the Vendor Maintenance team have access to the tables that have the banking and TIN data. There are queries built to look up the additional data and to pull it into a third-party software that the Vendor team uses to produce 1099 reports for each tax year. The Treasury file produced daily by Accounts Payable (AP) to schedule payments to vendors also includes PII (name, bank account) but this is available only to the individuals with a business responsibility of generating and transmit the file (through a dedicated line) to Treasury.
15. What will be the use of these reports?	Vendor Maintenance uses the reports to monitor and correct vendor setup (including PII data). The contracting office uses the reports to monitor vendor activity. The Treasury file is used to make standard payments to vendors.
16. Who will have access to these reports?	Only employees with a need to know will be given access to the reports. Supplier Processing Authority options must be enabled under User preferences configuration on top of application security roles for page access in order to add/update/inactivate vendor data in FMS. This is an added control.
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	

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.	Vendor information is collected from the vendors and manually entered into the system (there are no automated sources or other methods to collect vendor data in FMS). Online and batch edits are built into the system to prevent incomplete or incorrect data entry. Vouchers entered for vendors are also edited and flagged if corrections are needed prior to payment. Queries and reports within FMS are used to verify and validate information in the system quarterly. Vendor data is also verified and corrected annually as part of the 1099 reporting process.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The system is maintained and managed centrally at BPA Headquarters. Employees and managers access the system from the field and other locations on the BPA network. A vendor file will be downloaded at a secondary location for disaster recovery purposes; this file will provide the ability to make payments to the US treasury if an emergency or disaster precludes employees at Headquarters from performing this task. User training and guides are provided from an internal portal site and users can call a centralized Help Desk for future assistance.
Records Management	
22. Identify the record(s).	Financial transaction data

23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	This system records financial transactions and prepares a general ledger that meets Generally Accepted Accounting Principles (GAAP). (a) Input documents Automated data feeds and manual entry related to financial transact ions. Retention authority: N1-305-07-1-9/a Destroy when superseded, updated, replaced or no longer applicable. (b) System content (1) Journals and vouchers Retention authority: N1-305-07-1-9/b Retain for 6 years and then destroy (2) Billing invoices Retention authority: N1-305-07-1-9/c Retain for 10 years and then destroy (3) Project resources Retention authority: N1-305-07-1-9/d Retain for 10 years after the project is closed and then destroy. (4) Accounts receivables Retention authority: N1-305-07-1 -9/d Retain for 24 years and then destroy. (5) Asset accounting and lease administration Retention authority: N1-305-07-1-9/e/1 Retain for 25 years and then destroy. (6) Cost accounting

MODULE II – PII SYSTEMS & PROJECTS	
	Retention authority: N1-305-07-1-9/c Retain for 10 years and then destroy. (c) System output (1) Convenience and reference reports, periodic and on demand reports that are printed lo paper or digital media and used for Convenience, reference or distribution. Retention authority: N1-305-07-1-9/a Destroy when superseded, updated, replaced or no longer applicable.
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 Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with BPA's Cybersecurity Program Plan (CSPP) and DOE Directives.
26. Who will have access to PII data?	Only authorized personnel will have access to PII data with access privileges granted on a need-to-know basis. Within the application, security options must be enabled under "User Preferences" on top of application security roles for page access in order to add/update/inactivate vendor data in FMS.
27. How is access to PII data determined?	The access model employed in FMS is least-privilege; only an individual whose job function requires access to PII data would be granted this access. However, all users have access to query at least some of the data (name, employee ID) that are shared between the different modules of FMS (Projects Costing, Accounts Payable, Accounts Receivable, General Ledger).

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	The Department of the Treasury. Bureau of the Fiscal Services: Treasury Web Application Infrastructure (TWAI) Asset Suite: Supply Chain and Inventory Management System BPFAS: Planning and Forecasting Analysis System EPM: Data warehouse for reporting HRMIS: Human Resource Management Information System Concur: Travel System RPSA: Residential Purchase Sale and Agreement EE Tracker: Energy Efficiency Tracker Fieldglass: Supplement Labor Office
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?	We have Interconnection Security Agreements (ISAs) in place for external (outside the BPA network) systems
30. Who is responsible for ensuring the authorized use of personal information?	Information Owner
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	YVETTE GILL (Print Name) Digitally signed by YVETTE GILL Date: 2023.01.18 12:58:24 -08'00' (Signature)	
Information Owner	VALERIE GONZALES DARLING (Print Name) Digitally signed by VALERIE GONZALES DARLING Date: 2023.01.19 08:34:39 -08'00' (Signature)	
Local Privacy Act Officer	Candice Palen (Print Name) Digitally signed by Candice Palen Date: 2023.01.19 09:30:57 -08'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	William K. Hunt (Print Name) Digitally signed by William K. Hunt Date: 2023.01.18 10:51:33 -05'00' (Signature)	