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	10/14/2021	
Departmental Element & Site	Bonneville Power Administration Portland, Oregon	
Name of Information System or IT Project	Customer Contracts Management (CCM) BAE-GSS	
Exhibit Project UID	BPA is a Non-Appropriated Federal agency and is exempt from Exhibit 300 submissions.	
New PIA □ **Update** ☒	This is an update to an existing PIA	
	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	Jamie Sims, KSC-4 Supervisory Public Utilities Specialist	(503) 230-3886 jtsims@bpa.gov
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, JLS Information System Security Officer	(503) 230-5397 hcchoi@bpa.gov
Person Completing this Document	Alex Singharaj, JSC IT Specialist	(503) 230-4322 asingharaj@bpa.gov
Purpose of Information System or IT Project	Customer Contracts Management (CCM) is an internally hosted tool used by BPA to facilitate contract lifecycle business processes, including qualifying, negotiating, drafting, review/approval, offer, execution, implementation, administration, and closing out contracts. CCM is also the source of record for BPA's delegations of authority, including contracting and operational functions. The systems collects a limited amount of PII. Internal individual PII includes name, organizational code, login information, and business contact information, role (customer account team assignment), delegation of authority (if applicable), contract administration task completion comments and data, contract review/approval comments and data.. PII on members of the public includes name and contact information. Customer information is included in CCM by virtue of the information being in the contract. It is not in a structured format in the system, only in an unstructured format in the documents uploaded into 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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name and business contact information (job title, phone, email, and address) ☒ Other - auto-login based on BUD ID for internal personnel
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.*	Yes, 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)	Direct review of database and system information during the system upgrade and migration.

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 ☒ 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 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?**	The Bonneville Power Project Act provides administrative authority to contract to fulfill Bonneville Power Administration's mission. (See 16 U.S.C. § 832a(f); 16 U.S.C.§ 839f(a)).

<table>
<tr><th colspan="2">MODULE II – PII SYSTEMS & PROJECTS</th></tr>
<tr><td><b>2. CONSENT</b>
<b>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)?</b></td><td>None. The customer’s information is included in CCM because it is in the contract that is uploaded.
Employees are not given the opportunity to consent.</td></tr>
<tr><td><b>3. CONTRACTS</b>
<b>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?</b></td><td>Yes, contractors are involved with the project and system development.
Yes, all BPA’s supplemental labor contracts involving contractor access to BPA records contain a clause that requires contractors to comply with the Privacy Act per BPA Purchasing Instructions Clause 23-4.</td></tr>
<tr><td><b>4. IMPACT ANALYSIS:</b>
<b>How does this project or information system impact privacy?</b></td><td>
<table>
<tr><th>Confidentiality Factors</th><th>Low</th><th>Moderate</th><th>High</th></tr>
<tr><td>Identifiability</td><td>X</td><td></td><td></td></tr>
<tr><td>Quantity of PII</td><td></td><td>X</td><td></td></tr>
<tr><td>Data Field Sensitivity</td><td>X</td><td></td><td></td></tr>
<tr><td>Context of Use</td><td>X</td><td></td><td></td></tr>
<tr><td>Obligation to Protect Confidentiality</td><td>X</td><td></td><td></td></tr>
<tr><td>Access to and Location of PII</td><td>X</td><td></td><td></td></tr>
<tr><td>Overall Privacy Risk</td><td>X</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

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.**	Data is retrieved in the regular course of business by some attribute of the contract (e.g., contract number or contract type) or by utility or organization customer name, not by personal identifier.
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?	External PII data is provided by customers with whom BPA has a contract. Internal PII data is fed by Active Directory, Customer Data Management System, or directly inputted into the system.
9. Will the information system derive new or meta data about an individual from the information collected?	No new forms of metadata are derived.
10. Are the data elements described in detail and documented?	Yes, they are described in the data schema and software application documentation.

MODULE II – PII SYSTEMS & PROJECTS	
DATA USE	
11. How will the PII be used?	External name and contact information are used to contact the individual contract representative as needed. Internal names are used as an internal control (e.g., only individuals with delegated authority can sign contracts), for contract development and administration purposes (e.g., individuals on the team and in specific roles draft the contract, can view a draft contract, complete review/approval tasks, complete contract administration tasks, etc.).
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?	Contract maintenance information and reports may contain individual PII (e.g., the name of the individual who is on a contract team or who participated in a review of a contract).
15. What will be the use of these reports?	CCM generates reports about contracts, their assignment to BPA teams, and dates when contracts need to be reviewed/updated.
16. Who will have access to these reports?	BPA's legal department, CCM system users
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.

MODULE II – PII SYSTEMS & PROJECTS

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.	The external PII is sourced directly from the external counterparties. Updates are made as needed. Internal PII data is fed by Active Directory, Customer Data Management System, or directly inputted into the system.
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 information is stored in a database that is updated in realtime across all CCM users, regardless of site location.
Records Management	
22. Identify the record(s).	Customer contracts, delegations of authority, other misc. contract documents. The contracts are stored as Microsoft Word and PDF documents and are used for legal and billing reasons. A delegation of authority is a specific transfer from one official to another to bind BPA to a third party.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Contracts: N1-305-07-001-2c; Options: N1-305-07-001-2e2 and Delegations of Authority: N1-305-07-001-5c Contracts: PT-1300 Retain for 10 years after the records are closed. Options: PT-1600 - Transfer textual records to NARA 25 years after the records are closed. Transfer electronic records to NARA transfer to NARA in 5 year blocks when the most recent record in the block has been closed for 5 years. Delegations of Authority: MP-1300 - Destroy 10 years after the records are closed.
24. Records Contact	IGLM@bpa.gov

MODULE II – PII SYSTEMS & PROJECTS

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 the BPA Cybersecurity Program Plan (CSPP) and DOE Directives.
26. Who will have access to PII data?	Information Owner Delegates maintain access to CCM for users based on a need-to-know basis. IT maintains access to the overall system via Active Directory role groups.
27. How is access to PII data determined?	IO and IO delegates will approve access to non-sensitive PII on a need to know basis.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	CCM allows limited access to customers about their contracts by way of the Customer Portal.
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 Owners and Information Owner Delegates

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) YVETTE GILL Digitally signed by YVETTE GILL Date: 2022.12.14 13:34:55 -08'00' **(Signature)**	
Information Owner	(Print Name) JAMIE SIMS Digitally signed by JAMIE SIMS Date: 2022.12.15 08:14:57 -08'00' **(Signature)**	
Local Privacy Act Officer	(Print Name) Candice Palen Digitally signed by Candice Palen Date: 2022.12.15 11:52:57 -08'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2022.12.07 08:46:54 -05'00' **(Signature)**	