



PRIVACY IMPACT ASSESSMENT: PSRF – RPSA
PIA Template Version 5 – August 2017

Affects Members Of the Public?	<input checked="" type="checkbox"/>
--------------------------------	-------------------------------------

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	September 24, 2024	
Departmental Element & Site	Bonneville Power Administration (BPA) HQ, 905 NE 11 th Ave, Portland, OR	
Name of Information System or IT Project	Residential Purchase and Sales Agreements (RPSA)	
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.	
New PIA Update	<input type="checkbox"/> <input checked="" type="checkbox"/>	Update – 2010 draft assessed that no PII was collected. In reviewing the system in 2024 it was determined that some non-sensitive PII is collected. The update shifted to PIA as a consequence.
	Name, Title	Contact Information Phone, Email
Information System Owner	Yvette Gill, JL Supervisory IT Specialist	503-230-3947 yrgill@bpa.gov
Information Owner	Scott Winner, PSRF Supervisory Public Utilities Specialist	503-230-3378 swwinner@bpa.gov



MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Rachel Hull, CGI Privacy Act Officer	503-230-5241 rlhull@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Nick Choi, JLS ISSO	503-230-5397 hcchoi@bpa.gov
Person Completing this Document	Oliver Rose Jr., JLSI IT Specialist	503-230-3616 oxrose@bpa.gov
Purpose of Information System or IT Project	<p>Regional Purchase and Sales Agreements (RPSA) tracks the purchase and sales transactions for BPA’s utility customers (e.g. Portland General Electric (PGE) that participate in the Residential Exchange Program (REP). The REP originates from a congressionally brokered compromise to address disparate resource costs between public and private utilities in the Pacific Northwest and level the playing field between preference customers and residential and small farm customers. Bonneville pays the utilities the difference between the utility’s average system cost and Bonneville’s Priority Firm Exchange rate to ensure that regardless of whether a household or farm is served by a public utility or an investor-owned utility the rates should be the same.</p> <p>RPSA collects invoices from utilities showing the average system cost. The utilities submit the invoices for reimbursement under the Residential Exchange Program. This information includes invoices between BPA and its utility customers which contain the amount of energy for exchange, estimated benefit, and calculated benefit. The invoices do not contain PII. This data collection supports annual and monthly business processes and provides stakeholders with a venue for the discussion of rates and submission of monthly utility load information.</p> <p>More information about the Residential Exchange Program can be found on BPA’s public webpage, Residential Exchange Program - Bonneville Power Administration (bpa.gov).</p> <p>Users are representatives from utilities who register themselves for accounts and provide non-sensitive PII (name, work email address, organization affiliated with (e.g. PGE), and work phone number) to allow for access vetting.</p> <p>AIM ID 696.</p>	
Type of Information Collected or Maintained by the System:	<input type="checkbox"/> SSN <input type="checkbox"/> Medical & Health Information	



MODULE I – PRIVACY NEEDS ASSESSMENT

- Financial Information
- Clearance Information
- Biometric Information
- Mother's Maiden Name
- DoB, Place of Birth
- Employment Information
- Criminal History
- Name, Work Phone Number, Work email Address
- Other – Please Specify

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 identified non-sensitive PII is in 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

- Federal Employees
- Contractor Employees



MODULE I – PRIVACY NEEDS ASSESSMENT

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?

16 U.S.C. § 832 et.seq. – The Bonneville Project Act



MODULE II – PII SYSTEMS & PROJECTS

<p>2. CONSENT</p> <p>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)?</p>	<p>Consent is implied when the individual requests to register.</p>																																
<p>3. CONTRACTS</p> <p>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?</p>	<p>Yes, supplemental labor contractors (CFTE) access the system and data in the course of their regular jobs. All supplemental labor CFTE operate under master agreements with Privacy Act clauses and non-disclosure attestations.</p> <p>The relevant Privacy Act clauses were included in the Master Agreements.</p>																																
<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>The overall privacy impact is LOW due to the limited number of accounts and limited amount of work related PII collected.</p> <table border="1" data-bbox="625 1087 1243 1642"> <thead> <tr> <th>Confidentiality Factors</th> <th>Low</th> <th>Moderate</th> <th>High</th> </tr> </thead> <tbody> <tr> <td>Identifiability</td> <td>X</td> <td></td> <td></td> </tr> <tr> <td>Quantity of PII</td> <td>X</td> <td></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></td> <td>X</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></td> <td>X</td> <td></td> </tr> <tr> <td>Overall Privacy Risk</td> <td>X</td> <td></td> <td></td> </tr> </tbody> </table>	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		
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

<p>5. SORNs</p> <p>How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?</p> <p>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>Yes, information can be retrieved by name or email address.</p>
<p>6. SORNs</p> <p>Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>?</p> <p>If "Yes," provide name of SORN and location in the <i>Federal Register</i>.</p>	<p>DOE-18 Financial Accounting System</p>
<p>7. SORNs</p> <p>If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>NO</p>
<p>DATA SOURCES</p>	
<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>Individual provided and updated information.</p>
<p>9. Will the information system derive new or meta data about an individual from the information collected?</p>	<p>NO</p>
<p>10. Are the data elements described in detail and documented?</p>	<p>Yes, in the System Security Plan.</p>
<p>DATA USE</p>	



MODULE II – PII SYSTEMS & PROJECTS

11. How will the PII be used?	Information is collected for account access and operational contact.
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?	NO
13. With what other agencies or entities will an individual's information be shared?	N/A
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?	N/A
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

<p>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.</p>	<p>Users will be able to update their own records. Account administrators can disable accounts.</p>
<p>21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?</p>	<p>N/A</p>
<p>Records Management</p>	
<p>22. Identify the record(s).</p>	<p>System data consists of Residential Exchange Invoice data submitted by electrical utility customers to be reimbursed as defined by the Residential Exchange Agreement.</p>
<p>23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.</p>	<p>Check appropriately and cite as required.</p> <p><input type="checkbox"/> Unscheduled <input checked="" type="checkbox"/> Scheduled (<i>cite NARA authority(ies) below</i>)</p> <p>N1-305-07-001-2c</p> <p>PT-1300 Destroy 10 years after the records are closed.</p>
<p>24. Records Contact</p>	<p>IGLM@bpa.gov</p>
<p>ACCESS, SAFEGUARDS & SECURITY</p>	
<p>25. What controls are in place to protect the data from unauthorized access, modification or use?</p>	<p>Roles Based Access Controls, user verification prior to account creation.</p>
<p>26. Who will have access to PII data?</p>	<p>Account Administrators</p>
<p>27. How is access to PII data determined?</p>	<p>Roles Based Access Controls, outlined in the System Security Plan.</p>



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	<hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
Information Owner	<hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
Local Privacy Act Officer	<hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
Ken Hunt Chief Privacy Officer	<hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>