



PRIVACY IMPACT ASSESSMENT: JLSC - BILS
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	2/15/2023	
Departmental Element & Site	Bonneville Power Administration Headquarters, 905 NE 11 th Ave, Portland OR	
Name of Information System or IT Project	Billing Invoice Lookup System (BILS)	
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.	
New PIA <input checked="" type="checkbox"/>	New	
Update <input type="checkbox"/>		
	Name, Title	Contact Information Phone, Email
Information System Owner	Yvette Gill Supervisory IT Specialist	503-230-3904 yrgill@bpa.gov
Information Owner	Henry Tieu Supervisory Public Utilities Specialist	503-230-5535 httieu@bpa.gov



PRIVACY IMPACT ASSESSMENT: JLSC - BILS
PIA Template Version 5 – August 2017

MODULE I – PRIVACY NEEDS ASSESSMENT

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 ISSM	503-230-5397 hcchoi@bpa.gov
Person Completing this Document	Justin Steel Supervisory IT Specialist	503-230-3854 jasteel@bpa.gov
Purpose of Information System or IT Project	<p>The Billing Invoice Lookup System (BILS) is a fully integrated web-based computer system on a common IT platform that manages Power and Transmission billing and backup documents, and associated customer attributes.</p> <p>The system collects business contact information for Power and Transmission customers and the business contact information for Revenue Analysts as well as user ID for authentication and logging purposes.</p>	
Type of Information Collected or Maintained by the System:	<input type="checkbox"/> SSN Social Security number <input type="checkbox"/> Medical & Health Information e.g. blood test results <input type="checkbox"/> Financial Information e.g. credit card number <input type="checkbox"/> Clearance Information e.g. "Q" <input type="checkbox"/> Biometric Information e.g. finger print, retinal scan <input type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> DoB, Place of Birth <input type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input checked="" type="checkbox"/> Name, Phone, Address (BPAs customers' business mailing addresses and billing contacts' email addresses, and BPAs Revenue Analyst's (RA) work email addresses) <input checked="" type="checkbox"/> Other – Please Specify (BUD ID for login, logging and audit purposes)	



MODULE I – PRIVACY NEEDS ASSESSMENT

<p>Has there been any attempt to verify PII does not exist on the system?</p> <p><i>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.</i></p>	<p>N/A, PII is known to exist in the system.</p>
<p>If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)</p>	<p>N/A</p>

Threshold Questions

<p>1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?</p>	<p>Yes</p>
<p>2. Is the information in identifiable form?</p>	<p>Yes</p>
<p>3. Is the information about individual Members of the Public?</p>	<p>Yes</p>
<p>4. Is the information about DOE or contractor employees?</p>	<p>Yes</p> <p><input checked="" type="checkbox"/> Federal Employees</p> <p><input checked="" type="checkbox"/> Contractor Employees</p>

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.



MODULE I – PRIVACY NEEDS ASSESSMENT

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

<p>1. AUTHORITY</p> <p>What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?</p>	<p>Department of Energy Authorization Act, Title 42 United States Code (U.S.C.) Section 7101, et seq.</p> <p>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.</p>
<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>For customers, the PII is required if the user wants to complete these business transactions with BPA. All contact information is related to the business, not to the individual.</p> <p>For BPA users, consent is assumed when they enter their BUD IDs to login to BILS. Revenue Analysts work email addresses are required for customer service work, and consent is provided via the assumption of the role.</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, all of 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.</p>



MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

BILS is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls:

- Strict access control enforcement based on need-to-know
- System Owner Testing
- Audit Reports

While BILS contains some PII, the ensuing risk to the privacy of individuals is generally low as the focus of BILS is to manage Power and Transmission billing and backup documents, and associated customer attributes.

The overall privacy impact is LOW (affects approximately 600 customers associated with BPA).

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.

No. Data is retrieved through the regular course of business by customer information (customer business name or account number, which corresponds to a business, not an individual) and not by personal identifier.



MODULE II – PII SYSTEMS & PROJECTS

<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>N/A</p>
<p>7. SORNs</p> <p>If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>N/A</p>
<p>DATA SOURCES</p>	
<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>Two systems provide the source information to BILS; they are the Customer Billing Center (CBC) and PowerOptix Billing. These two systems generate customer bills at BPA.</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, there is application documentation that details the data elements of the database in the System Security Plan.</p>
<p>DATA USE</p>	
<p>11. How will the PII be used?</p>	<p>Customer address will be used to communicate about bills.</p> <p>Employee's BUD IDs are used for login, auditing, and logging purposes.</p> <p>Revenue Analyst's work email will be used for customer communication and provided on the customer's bill.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>12. If the system derives meta data, how will the new or meta data be used?</p> <p>Will the new or meta data be part of an individual's record?</p>	<p>N/A</p>
<p>13. With what other agencies or entities will an individual's information be shared?</p>	<p>N/A</p>
<p>Reports</p>	
<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>Customer Account Bill</p> <p>System Access Usage Report</p>
<p>15. What will be the use of these reports?</p>	<p>To determine who is performing what actions and when.</p>
<p>16. Who will have access to these reports?</p>	<p>Access to the audit reports reports are limited to administrators, which includes about 24 BPA employees or contractors.</p>
<p>Monitoring</p>	
<p>17. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>No.</p>
<p>18. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>N/A</p>
<p>19. Are controls implemented to prevent unauthorized monitoring of individuals?</p>	<p>N/A</p>

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>System is kept current through Active Directory updating for BPA personnel. Inactive customer data is purged annually per the records retention schedule. Active customer data is kept updated through reports from the customer billing system.</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>Power and Transmission bills BPA sends to customers and their back-up copies. Retain for 10 years after the date the bill was issued.</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. <input type="checkbox"/> Unscheduled <input checked="" type="checkbox"/> Scheduled (cite NARA authority(ies) below) N1-305-07-001-2a and N1-305-07-001-2c</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>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) directives and requirements.</p>
<p>26. Who will have access to PII data?</p>	<p>Access to audit reports are limited to those individuals who are responsible for administering the system through Active Directory Role Based Access Controls (RBAC). General access to the system is provided to all BPA personnel except for the members of the Transmission or Power marketing groups.</p>
<p>27. How is access to PII data determined?</p>	<p>Based on lawful government purpose basis and IO approval.</p>
<p>28. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>No</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>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?</p>	<p>N/A</p>
<p>30. Who is responsible for ensuring the authorized use of personal information?</p>	<p>Information Owner</p>

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
<p>System Owner</p>	<p><u>Yvette Gill</u> _____ (Print Name)</p> <p>_____ (Signature)</p>	<p>_____</p>
<p>Information Owner</p>	<p><u>Henry Tieu</u> _____ (Print Name)</p> <p>_____ (Signature)</p>	<p>_____</p>
<p>Local Privacy Act Officer</p>	<p><u>Candice Palen</u> _____</p>	<p>_____</p>



PRIVACY IMPACT ASSESSMENT: JLSC - BILS
PIA Template Version 5 – August 2017

	<p>(Print Name)</p> <hr/> <p>(Signature)</p>	
<p>DOE Chief Privacy Officer</p>	<p>(Print Name)</p> <hr/> <p>(Signature)</p>	