



Affects Members Of the Public?	<input 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	June 6, 2023	
Departmental Element & Site	Bonneville Power Administration Headquarters, 905 NE 11 th Ave, Portland OR	
Name of Information System or IT Project	Erwin Data Modeler	
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.	
New PIA <input checked="" type="checkbox"/>	This is a new PIA for an existing system.	
Update <input type="checkbox"/>		
	Name, Title	Contact Information Phone, Email
Information System Owner	Yvette Gill Supervisory IT Specialist, JL	503-230-3947 yrgill@bpa.gov
Information Owner	Rebecca Wilde Supervisory IT Specialist, JLS	503-230-4298 rlwilde@bpa.gov



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.)	Elizabeth McNeel, JLSR IT Specialist (APPSW/DATAMGT)	360-619-6860 emmccneel@bpa.gov
Person Completing this Document	Elizabeth McNeel IT Specialist (APPSW/DATAMGT)	360-619-6860 emmccneel@bpa.gov
Purpose of Information System or IT Project	<p>Erwin Data Modeler is used to create logical and physical data models to understand complex data sources (databases with no unique, primary, or foreign keys) and automate design standards and integrity rules. Data Architects work with data generators, data stewards, and consumers to create the data models. Data modeling provides a way to visualize metadata and also to manage and govern enterprise data. Erwin is like a blueprint to design or reverse engineer databases. Erwin connects to a database in development or test environment to provide a diagram of the tables/columns/primary and foreign keys.</p> <p>Erwin uses the Mart Repository to support a multiuser environment, Mart acts as a central repository for saved data models. An individual can open a model from Mart to work individually or collaboratively. The Mart Repository is on a server, but users can save data models to their desktops.</p> <p>Erwin has an Open Version drop-down list all the versions that are associated with the selected model. The default version that Erwin uses is the current state of the model and the remaining versions are previous Delta versions or marked versions of that model. Users can select the lock option when they open a model so that other users do not overwrite their work. Model locking helps to secure models and manage how changes are saved to the mart. One of the mechanisms for ensuring the accuracy of the information in Erwin is the Roles Based Access Controls (RBAC), which ensures that only those with the proper role assignments can update and save data models in the Mart Repository.</p> <p>Erwin only collects email and user ID for system access.</p>	
Type of Information Collected or Maintained by the System:	<input type="checkbox"/> SSN <input type="checkbox"/> Medical & Health Information <input type="checkbox"/> Financial Information <input type="checkbox"/> Clearance Information	



MODULE I – PRIVACY NEEDS ASSESSMENT

- Biometric Information
- Mother's Maiden Name
- DoB, Place of Birth
- Employment Information
- Criminal History
- ~~Name, Phone~~, e-mail Address (only user email address is collected)
- Other – user ID (BUD ID)

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

If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)

Non-sensitive PII (user login ID, email address) exists on the system.

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

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)).

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)?

User or supervisor requests access based on job duties. Erwin provides no functions for modifying or adding new linkable data about an individual.



MODULE II – PII SYSTEMS & PROJECTS

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?

Yes, contractors are involved with creating and maintaining data models. 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.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

Erwin 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

Erwin only collects BUD ID and user email. The ensuing risk to the privacy of individuals is generally low as the focus of Erwin is to create logical and physical data models to understand complex data sources (databases with no unique, primary, or foreign keys) and automate design standards and integrity rules. This does not require or encourage collection of sensitive PII and is not driven by analysis of PII.

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>No, PII cannot be retrieved by an individual's name or identifier.</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>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>Active Directory</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>Described and documented in System Security Plan (SSP).</p>

DATA USE



MODULE II – PII SYSTEMS & PROJECTS

11. How will the PII be used?	PII is used to identify an individual responsible for ownership of data models. Only email address and BUD ID are collected.
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?	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>System is updated manually, with quarterly review.</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; this system is only available internally.</p>
<p>Records Management</p>	
<p>22. Identify the record(s).</p>	<p>Design artifacts, documentation for conceptual, logical, and physical data models.</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 (cite NARA authority(ies) below)</p> <p>N1-305-07-001-5a</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>Access to data in the system is controlled through Roles Based Access Control (RBAC) security.</p>
<p>26. Who will have access to PII data?</p>	<p>Erwin Viewer (read-only), Erwin Architect (update and save models), Erwin Modeller (create, read, update, delete permissions), or Erwin Admin (establishes, updates, and removes accounts).</p>
<p>27. How is access to PII data determined?</p>	<p>Non-sensitive PII data is available to all users. Only Erwin Admin can establish, update, or remove accounts.</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	_____ (Print Name) _____ (Signature)	_____
Information Owner	_____ (Print Name) _____ (Signature)	_____
Local Privacy Act Officer	_____ (Print Name) _____ (Signature)	_____
DOE Chief Privacy Officer	_____ (Print Name) _____ (Signature)	_____