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	06/06/2023	
Departmental Element & Site	Bonneville Power Administration, Portland Oregon	
Name of Information System or IT Project	Resolver Governance, Risk, and Compliance (GRC)	
Exhibit Project UID	Contract #85426	
New PIA ☒ **Update** □	This is a new PIA for an existing system.	
	Name, Title	**Contact Information Phone, Email**
Information System Owner	Yvette Gill, JLS (Information System Owner) Supervisory IT Specialist (delegate) Jason Stabe, JLSI System Security Manager Supervisory IT Specialist	503-230-3947 yrgill@bpa.gov 503-230-3569 jtstabe@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Information Owner	Christopher Frost, CG Chief Compliance Officer	503-230-5602 cmfrost@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, JLS IT Specialist	503-230-5397 hcchoi@bpa.gov
Person Completing this Document	Ryan Buss, CGF FERC Compliance Officer	503-230-4274 rdbuss@bpa.gov
Purpose of Information System or IT Project	Resolver GRC is used to monitor and track BPA's compliance with the North American Electric Reliabilty Corporation (NERC) Reliability Compliance Standards. These Standards are mandatory for the Power Industry under Federal Energy Regulatory Commission (FERC) Orders 693 and 706. This tool stores evidence of compliance with these requirements, as well as tracking and managing workflows to prepare evidence and certify compliance with these Reliability Standards. Resolver GRC is the official source of record for information related to NERC Reliability Compliance. This includes data regarding compliance processes, mitigation plans, and audit history.	
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 ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Criminal History ☒ Name ☒ email address for workflow, employees’ organization code
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 PII listed above is known to exist in the system. Only names and emails.
If “Yes,” what method was used to verify the system did not contain PII? (e.g. system scan)	Review of attachments.

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 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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	Resolver ensures agency compliance and therefore is authorized by the following: NERC Relaibility Compliance Standards, Standards made mandatory by FERC Order 693 and 706.
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)?**	Individuals in roles responsible for certifying compliance requirements do not have an opportunity to consent to or decline the use of their information in the system. These individuals are identified as Tier 1 or Tier 2 Managers based on their role.

MODULE II – PII SYSTEMS & PROJECTS

<table>
<tr>
<td><strong>3. CONTRACTS</strong>
<strong>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?</strong></td>
<td>The contract contains privacy protection clauses.</td>
</tr>
<tr>
<td><strong>4. IMPACT ANALYSIS:</strong>
<strong>How does this project or information system impact privacy?</strong></td>
<td>The privacy impact of this system is low due to the low sensitivity/risk of the nature of personal information collected.

Resolver GRC 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
<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>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>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><strong>Overall Privacy Risk</strong></td><td><strong>x</strong></td><td></td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td><strong>5. SORNs</strong>
<strong>How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?</strong>
<strong>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</strong></td>
<td>Information is retrieved by organization name, function, or compliance requirement, not by name in the regular course of business.</td>
</tr>
</table>

MODULE II – PII SYSTEMS & PROJECTS	
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*.**	No
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?	Information about individuals is provided from the BPA agency directory.
9. Will the information system derive new or meta data about an individual from the information collected?	No new or metadata will be derived about individuals.
10. Are the data elements described in detail and documented?	The data fields are documented in the System Security Plan.
DATA USE	
11. How will the PII be used?	Name and email address are used for workflow purposes, as well as to identify ownership of particular project(s), and track compliance requirements.

MODULE II – PII SYSTEMS & PROJECTS	
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?	BPA shares processes and supporting evidence with WECC. PII used to track progress is not shared with WECC, but occasionally names appear on some of the specific evidence being shared (like on an email, for instance).
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports will be developed to document the progress of projects (i.e., whether an action plan is on track). Individuals associated with those projects may be listed in the reports.
15. What will be the use of these reports?	The reports will be used to assess the health of project(s) and provide increased metrics around agency compliance.
16. Who will have access to these reports?	The CGF organization Business Unit Coordinators Reliability Compliance Participants Executive Leadership
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No, this system does not have the capability to identify, locate, and/or monitor individuals.
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.	Projects are run on an annual basis. Individuals' information is updated for accuracy, relevancy, and completeness at the start of each project period.
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 housed in the Cloud.
Records Management	
22. Identify the record(s).	This tool stores evidence supporting compliance with these requirements as well as tracks and manages workflows to prepare evidence and certify compliance with these Reliability Standards. GRC is the official source of record for information related to NERC Reliability Compliance. This includes data regarding compliance processes, mitigation plans, and audit history.

MODULE II – PII SYSTEMS & PROJECTS

23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	(a) Input Documents Manual data entry and spreadsheet uploads. Retention Authority: N1-305-07-1-5/a Destroy when superseded, updated, replaced or no longer applicable. (b) System Content Resolver stores data in SQL database tables. Retention Authority: N1-305-07-1-5/c Destroy 8 years after the records are closed. (c) System Output (1) Convenience and reference reports, periodic and on demand reports that are printed to paper or digitial media and used for convenience, reference or distribution. Retention Authority: N1-305-07-1-5/a Destroy when superseded, updated, repolaced or no longer applicable. (2) Documents exported from the system and stored in a case file to document a program, decision or other activity. Retain for the specified retention of the case file where the output is filed. This retention is identified in the BPA Records Manual.
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?	Users must be granted access to GRC; permissions are role-based. Only Administrators can view all data.
26. Who will have access to PII data?	The system administrator and those employess Bonneville Full-Time Equivalent (BFTE) and Contracted full-time equivalent (CFTE) with a need to know based on their individual role.
27. How is access to PII data determined?	Access to PII is determined by role and limited to only what each individual has a need to know.

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, other systems do not share data or have access to the data in the system. Data can be manually extracted from the system and exported to a CVS file.
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?	This is a standalone SaaS system in the Cloud. There are no connecting information systems.
30. Who is responsible for ensuring the authorized use of personal information?	System Administrators
END OF MODULE II	

SIGNATURE PAGE

	Signature		Date
System Owner	(Print Name) YVETTE GILL Digitally signed by YVETTE GILL Date: 2023.07.05 10:31:20 -07'00' (Signature)		
Information Owner	(Print Name) CHRISTOPHER FROST Digitally signed by CHRISTOPHER FROST Date: 2023.07.05 10:50:41 -07'00' (Signature)		
Local Privacy Act Officer	(Print Name) Candice Palen Digitally signed by Candice Palen Date: 2023.07.05 12:45:03 -07'00' (Signature)		
DOE **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.07.03 12:50:08 -04'00' (Signature)		