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	March 29, 2024
Departmental Element & Site	Bonneville Power Administration (BPA) HQ, 905 NE 11th Ave, Portland, OR
Name of Information System or IT Project	Business Continuity Portal, Global Alert Link (GAL)
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.
New PIA ☐ **Update** X	This is an update of an existing PIA that was signed in 2022. Minimal changes.

	Name, Title	Contact Information Phone, Email
Information System Owner	Yvette Gill, JL Supervisory IT Specialist	503-230-3947 yrgill@bpa.gov
Information Owner	Shane Hester, NNC Continuity and Emergency Management Manager	360-619-6458 shhester@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Candice Palen, CGI Privacy Act Officer	503-230-3602 cdpalen@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	Darla Bennett, NNC Emergency Management Specialist	503-230-3410 ddbennett@bpa.gov
Purpose of Information System or IT Project	Global Alert Link (GAL) is a business continuity tool that serves as an Emergency Notification System and continuity plan (including Business Impact Analysis) repository. The system is designed to provide reliable messaging and information recall. System is used to generate automated calls and text messages to employees that sign up for the communication. The sign-up process occurs in the Human Resources Management Information System (HRMIS), which exports specific data fields to the GAL for emergency notification. GAL contains: first, middle, and last name; work phone number, work cell phone number, home phone number, personal cell phone number; work and personal email address; home address (used for geographically specific emergency notifications); duty station location (city, state, department, position, building, floor, area). This information is collected for both full time employees as well as supplemental labor contract employees. Personnel identified as Key Support Staff, Mission Essential, or Emergency Response Group are required to supply contact information. All other staff may voluntarily provide their contact information. Only the BPA GAL Administrators have access to personal contact information in GAL for validation purposes.	
Type of Information Collected or Maintained by the System:	☐ SSN ☐ Medical & Health Information ☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address (work and home information), email address (work and home information) ☒ Other – BUD ID (login 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 – the above identified non-sensitive PII exists on 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?	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?**	The Global Alert Link system is authorized by the following statutes, directives, and orders: • Title 42, U.S.C. § 7101 et. seq. • The Homeland Security Act of 2002 • Homeland Security Presidential Directive-5 (HSPD-5), "Management of Domestic Incidents" • Department of Homeland Security Federal Emergency Management Agency Federal Continuity Directive 1 (Jan. 17, 2017) • DOE O 150.1B Continuity Programs • DOE O 151.1D Comprehensive Emergency Management System

MODULE II – PII SYSTEMS & PROJECTS

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)?

Personnel in Mission Essential or Emergency Response Group roles are notified of the requirement to provide personal contact information to accept the role.

Staff who voluntarily register information in HRMIS are consenting by virtue of entering the information in the system.

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?

The relevant Privacy Act clauses were included in the contract for the SaaS.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

BPA Privacy impacts of Global Alert Link (GAL) is MODERATE due to the quantity of PII in the system.

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	
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.**	Typically, the data will be retrieved from GAL by generic categories (e.g. floor, building, or department). An alert can be sent to a group or category of individuals (for example everyone on the 5th floor of the 905 building). Alerts sent to Key Support Individuals may be retrieved by name according to the Business Continuity plans.
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*.**	DOE-11: Emergency Operations Notification Call List
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	NO
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Individual-provided, information entered in the Human Resources Management Information System (HRMIS). Information fields are shared via export of specific fields to Global Alert Link (GAL).
9. Will the information system derive new or meta data about an individual from the information collected?	NO
10. Are the data elements described in detail and documented?	YES, data elements are described in detail and documented in the System Security Plan (SSP).
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	PII will be used to contact Key Support Staff in the event of an incident or emergency that impacts continuity of operations at BPA. Employees affected by an incident or emergency receive notifications to their work contact automatically, but only the staff who voluntarily sign up to receive emergency alerts are notified via personal contact information. Notifications will be sent per group or location to impacted individuals.
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?	PII is not shared with any other agency or entity.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports identifying Key Support Staff may be produced for Business Continuity planning purposes. Location based reports may be generated for specific events to allow for tailored emergency notification.
15. What will be the use of these reports?	Reports will be used for business continuity and emergency notification purposes.
16. Who will have access to these reports?	Role Based Access Controls (RBAC). BPA GAL Administrator has access to reports with unmasked PII data. Application Administrator, Plan Administrators, Policy Group Executives, and Notification Administrators have access to reports with masked PII data.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No, the system does not have the capability to identify, locate, or monitor individuals.
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.	PII data elements are collected in the BPA Human Resources Management Information System (HRMIS). The information is pushed to the GAL via an automated process every workday. It is the responsibility of the individual employee to update their contact information. GAL checks the "activity" level of the employee and if they move to an "inactive" status they are removed from the database. For those who voluntarily sign up for emergency notification there will be a regularly published article encouraging them to update their emergency contact information in HRMIS. Employees are also reminded to update their information as part of the emergency notification process and during preparation for inclement weather.
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 HRMIS information system is onsite at BPA. A one-way data feed from the system will be sent to the Global Alert Link system. Updates to the data will be made in the HRMIS system and reflected in Global Alert Link. The vendor operates the system with redundancy.
Records Management	
22. Identify the record(s).	Employee emergency contact information. Business impact analysis data.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. ☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* GRS 5.3, item 010, GRS 5.3, item 020.
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?	Role Based Access Controls (RBAC) with permissions reviewed regularly, provisioned on a need-to-know basis. Documented in the System Security Plan (SSP).

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	Role Based Access Controls (RBAC). BPA GAL Administrator.
27. How is access to PII data determined?	The application System Administrator is the only one who will have access to the PII. All other access is based on role.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	GAL receives a one-way data feed from HRMIS limited to the specific data fields identified within this document. No transfer of any PII data to any other system. Emergency messages are sent in such a way that no recipient can see what other recipients also received the message.
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) YVETTE GILL Digitally signed by YVETTE GILL Date: 2024.04.05 14:18:36 -07'00' (Signature)	
Information Owner	(Print Name) Shane Hester Digitally signed by Shane Hester Date: 2024.04.15 07:34:27 -07'00' (Signature)	
Local Privacy Act Officer	(Print Name) CANDICE PALEN Digitally signed by CANDICE PALEN Date: 2024.04.17 15:41:34 -07'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2024.04.05 11:53:03 -04'00' (Signature)	