Affects Members Of the Public? Mark if Applicable w/ an X

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	12/31/18
Departmental Element & Site	BPA HQ, Portland, OR. SaaS hosted by the vendor Global Alert Link in geo redundant data centers (parent organization is Resolver).
Name of Information System or IT Project	Business Continuity Portal, Global Alert Link
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.
New PIA ☐ **Update** ☒	Last PIA document signed on 9/7/12

	Name, Title	Contact Information Phone, Email
System Owner	Jason Stabe, JSI Supervisory IT Specialist	503-230-3569 jtstabe@bpa.gov
Information Owner	John Nguyen, NNC Manager, Continuity of Operations and Emergency Management	503-230-5054 jgnguyen@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Candice Palen, CGI FOIA/Privacy Officer	503-230-3602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Nick Choi, JS Cyber Security Specialist	503-230-5397 hcchoi@bpa.gov
Person Completing this Document	John Nguyen, NNC Manager, Continuity of Operations and Emergency Management	503-230-5054 jgnguyen@bpa.gov
Purpose of Information System or IT Project	The system is designed to provide Bonneville reliable and efficient operations recall in the event of an emergency. The system is used by Bonneville's Continuity of Operations (COOP) Emergency Management (EM) organization to meet planning and response requirements.	
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 ☐ Criminal History ☒ Name, Phone, Address ☒ Other – Please Specify: Phone, Work Email, Home Email, Work location (street, city, state, zip), Org Code, Floor, Mail Drop	
Has there been any attempt to verify PII does not exist on the system?		Yes

MODULE I – PRIVACY NEEDS ASSESSMENT

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.*	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	The system is configured to collect the above listed PII. No other PII resides in 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?	☒ 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.

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: The Homeland Security Act of 2002 (https://www.dhs.gov/homeland-security-act-2002) Department of Homeland Security Federal Emergency Management Agency Federal Continuity Directive 1 (Jan. 17, 2017) (https://www.fema.gov/media-library-data/1486472423990-f640b42b9073d78693795bb7da4a7af2/January2017FCD1.pdf) DOE O 150.1A Continuity Programs (https://www.directives.doe.gov/directives-documents/100-series/0150.1-BOrder-a) DOE O 151.1D Comprehensive Emergency Management System (https://www.directives.doe.gov/directives-documents/100-series/0151.1-BOrder-d) DOE O 200.2 Information Collection Management Program (https://www.directives.doe.gov/directives-documents/200-series/0200.2-BOrder)
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)?**	Key Support Staff (Mission Essential or Emergency Response Group) who are named in business continuity plans are required to supply their personal contact information for Continuity of Operations (COOP) and Emergency Management (EM) purposes. All other Staff may sign up voluntarily for Emergency notification alerts. These staff members, whether Bonneville Full Time Employee (BFTE) or Contract Full Time Employee (CFTE), can enter their PII data directly into Human Resources Management Information System (HRMIS). By entering their PII they grant permission for the business continuity portal to send them emergency alerts. Only supervisors of non-key Support Staff will have access to personal contact information.

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. Global Alert Link is a SaaS product. Background checks will be performed by the vendor and their representatives on all their personnel who have access to the BPA data. Yes. The Privacy Act clauses were included in the contract. A copy of the vendor process for background checks is on file.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed Global Alert Link as a moderate risk system for confidentiality, integrity, and availability according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. Global Alert Link 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 • Encryption The privacy impact of the Business Continuity Portal/Global Alert Link is moderate due to the nature and volume of personal data contained in the system.
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.**	The data will be retrieved in the business continuity portal system by generic categories (i.e., floor, building, or department, etc.). When an alert is sent, it is sent to a group or category of individuals (example everyone on the 5th floor of the 905 building). Generally, no information will be retrieved using a personal identifier. However, alerts might be sent to a specific Key Support Individual named in a recovery plan for Business Continuity purposes during an event.

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*.**	Yes, the records in the Business Continuity Portal/Global Alert Link are covered by DOE-11: Emergency Operations Notification Call List. 74 FR 1011.
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?	The personal information contained in the system is collected from Bonneville's HRMIS.
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. The following data elements are described in detail: Name–first, middle, last; Phone–work, work cell, home, home cell; Email–work, home; Address–street, city, state, zip; Duty Station–city, state, department, position, building, floor, area.
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 Bonneville. Staff may voluntarily sign up to receive Emergency alerts. This PII will be stored in the business continuity portal and 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?	Individuals' information 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?	A list of named Key Support Staff may be produced for Business Continuity planning purposes.
15. What will be the use of these reports?	Reports will be used for business continuity purposes.
16. Who will have access to these reports?	PII access will be restricted to system administrator.
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 monitor individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	None
19. Are controls implemented to prevent unauthorized monitoring of individuals?	The system does not have the ability to monitor individuals.

MODULE II – PII SYSTEMS & PROJECTS

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 will be collected in the BPA HRMIS system. Periodically, an auto generated report will be sent to each manager from the HRMIS system asking them to verify the currency, accuracy, and completeness of information for their designated Key Support Staff person. If necessary, the information will be updated in HRMIS and subsequently fed into Global Alert Link.
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 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. Data will not be transferred or tied to any other system.
Records Management	
22. Identify the record(s).	Employee Emergency Contact Information: Records used to account for and maintain communication with personnel during emergencies, office dismissal, and closure situations. Records include name and emergency contact information such as phone numbers or addresses. Records may also include other information on employees such as responsibilities assigned to the individual during an emergency situation.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	General Records Schedule (GRS) 020 Disposition Instruction: Destroy when superseded or obsolete, or upon separation or transfer of employee. Disposition Authority: DAA-GRS- 2016-0004-0002
24. Records Contact	Information Governance and Lifecycle Management iglm@bpa.gov
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Global Alert Link controls data access: Policy dictates that client data never leave the hosted environment. Only select individuals maintain access to system administrative accounts within the hosted environment. No one outside of our organization maintains an account or access to data in an unencrypted form. All system passwords are stored in an encrypted management system which is only accessible by the core administrative team. System administrators do not have physical access to the servers. The individuals with physical access do not have login credentials to the server or access to the data in an unencrypted form. Access to the server is performed through both VPN and remote desktop connection, requiring dual authentication for management.
26. Who will have access to PII data?	Access to PII data will be role-based and limited to those employees with a need to know. BPA application System Administrator – RWD Plan Administrators –R Policy Group Executives – R Notification Administrators – R R = Read Access W = Write Access D = Delete Access
27. How is access to PII data determined?	The application System Administrator is the only one who will have write 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.	The business continuity portal will receive a one way data feed from HRMIS. The business continuity portal will not transfer PII data to any other system.
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?	Business Continuity Program Manager and System Administrator
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	YVETTE GILL (Print Name) Digitally signed by YVETTE GILL Date: 2022.03.22 13:35:48 -07'00' (Signature)	
Information Owner	John G. Nguyen (Print Name) Digitally signed by John G. Nguyen Date: 2022.03.22 13:45:43 -07'00' (Signature)	
Local Privacy Act Officer	Candice Palen (Print Name) Digitally signed by Candice Palen Date: 2022.03.22 13:59:48 -07'00' (Signature)	
Chief Privacy Officer	William K. Hunt (Print Name) Digitally signed by William K. Hunt Date: 2022.03.16 08:59:38 -04'00' (Signature)	