Affects Members Of the Public?	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	07/20/2022
Departmental Element & Site	Bonneville Power Administration (BPA) Portland, OR
Name of Information System or IT Project	KnowBe4 Security & Awareness Training Platform
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions
New PIA [X] **Update** [ ]	This is a new PIA for a new system

	Name, Title	Contact Information Phone, Email
Information System Owner	Paul Dickson Supervisory IT Specialist	503-230-4075 prdickson@bpa.gov
Information Owner	Gary Dodd Supervisory IT Cybersecurity Specialist	503-230-4474 gadodd@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.)	Sean Barry IT Cybersecurity Specialist Team Lead Ryan Paradis IT Cybersecurity Specialist	503-230-3382 spbarry@bpa.gov 503-230-4388 rcparadis@bpa.gov
Person Completing this Document	Victoria Bauras IT Cybersecurity Specialist	503-230-3390 vlbauras@bpa.gov
Purpose of Information System or IT Project	KnowBe4's Diamond-level Enterprise Security & Awareness Training Platform is integrated with the Phish Alert Button (PAB) and an add-on called PhishER PhishER – Knowledge Base (knowbe4.com). This Software as a Service (SaaS) platform is Federal Risk and Authorization Management Program (FedRAMP) certified and it is the Department of Energy (DOE)'s current training and awareness web-based platform. BPA currently uses the Security & Awareness Training Platform and the PAB through DOE's enterprise license, but is required to procure it separately in order to purchase the add-on of PhishER. The Security & Awareness Training Platform used for remedial cyber trainings, internal phishing awareness campaigns, executive-level reporting, and cyber awareness month outreach. Users submit potentially malicious emails for review using the PAB. PhishER will allow BPA to automatically "triage" submitted emails with software that integrates with BPA's existing platform. With the addition of PhishER, submitted emails go through KnowBe4 servers to triage as part of PhishER's offerings. It is possible, but not expected, for emails containing sensitive PII to be submitted for review. Additional information can be found here: https://www.knowbe4.com/products/phisher	
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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ 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, Work Email Address ☒ Other – Please Specify: Training assignments and completion status
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 PII listed above exists in 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?	Yes, limited to name and email address only
4. Is the information about DOE or contractor employees?	YES or NO (If Yes, select with an "X" in the boxes below) ☒ Federal Employees ☒ Contractor Employees

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	Department of Energy Authorization Act, Title 42 United States Code (U.S.C.) Section 7101, et seq. 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. Exchange Online allows personnel to communicate and share electronic files via email in furtherance of their jobs. 5 USC Chapter 41 - Training

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)?

Consent is derived through use of BPA email (Microsoft Exchange). All BPA email users are provided notice in the form of the login warning banner prior to accessing the email system. BPA does not allow public access to the system. Only authorized BPA employees and contractors have access to the email system.

External users may decline to provide information by not emailing to a BPA email address. BPA email users also have the option of not using the "report phishing" button to submit suspicious emails.

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, and BPA contract clause 5-2 includes privacy protection under the Privacy Act.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The Privacy Impact rating is Low:

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.

Yes, training completion information is retrieved by name.

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, DOE-28: General Training Records
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?	PII can be found in the email messages sent through PhishER by use of the "report phishing" button, usually limited to name and email address only. The sources include all senders and recipients of email messages contained in the BPA email system.
9. Will the information system derive new or meta data about an individual from the information collected?	No, the system does not derive new information or metadata about individuals.
10. Are the data elements described in detail and documented?	Yes, see vendor documentation here: Knowledge Base (knowbe4.com)
DATA USE	
11. How will the PII be used?	The PhishER system is not intended to operate as a data repository. The system is designed and intended to be used to triage reported suspicious emails. The email address information of the BPA email users is required to facilitate email message delivery. All other information (the sender or recipient's name, phone number, mailing address, content of the email message and the content of any email message attachment) that is contained within the email message is incidental and not targeted for collection.

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?	None
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports can be run from the PhishER platform and contain email user submission behavior, but they contain no PII aside from email addresses and message subject. Reports can also be run to show cyber training completion status.
15. What will be the use of these reports?	Reports will be run by the Training, Outreach, & Awareness (TOA) Team internal to BPA's Office of Cyber Security
16. Who will have access to these reports?	BPA's Office of Cyber Security
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system does not 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.	The PhishER system requires correct email addresses to send or receive email. Contact information is kept current through Active Directory and Exchange.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	This platform is a SaaS solution operated by KnowBe4
Records Management	
22. Identify the record(s).	BPA's cyber training and awareness software that focuses on both phishing exercises and real-world phishing investigations.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 2.6, item 030 (training records), GRS 3.2, item 020 (security incident reporting and follow-up records)
24. Records Contact	Information Governance & Lifecycle Management iglm@bpa.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Only users authorized by BPA's Office of Cyber Security may access the system.
26. Who will have access to PII data?	Only users authorized by BPA's Office of Cyber Security will have access to PII data. These users include members of the Training, Outreach, and Awareness team.
27. How is access to PII data determined?	Role Based Access Control
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Planned Security Event and Incident Management integration with Splunk for monitoring security events

MODULE II – PII SYSTEMS & PROJECTS	
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?	The Information Owner
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	_____ **(Print Name)** PAUL DICKSON Digitally signed by PAUL DICKSON Date: 2023.03.09 06:53:09 -08'00' _____ **(Signature)**	_____
Information Owner	_____ **(Print Name)** GARY DODD JR Digitally signed by GARY DODD JR Date: 2023.03.20 07:56:22 -07'00' _____ **(Signature)**	_____
Local Privacy Act Officer	_____ **(Print Name)** Candice Palen Digitally signed by Candice Palen Date: 2023.03.20 10:50:00 -07'00' _____ **(Signature)**	_____
Ken Hunt **Chief Privacy Officer**	_____ **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.03.08 09:30:09 -05'00' _____ **(Signature)**	_____