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	1/22/2020
Departmental Element & Site	Bonneville Power Administration (BPA) Portland, Oregon
Name of Information System or IT Project	Exchange 2016
Exhibit Project UID	BPA is a Non-Appropriated Federal agency and is exempt from Exhibit 300 submissions
New PIA ☐ **Update** X	Exchange 2016 is an upgrade to the existing 2010 email system that is currently in place in BPA.

	Name, Title	Contact Information Phone, Email
System Owner	John O'Donnell, JNP Supervisory IT Specialist	503-230-4676 jpodonnell@bpa.gov
Information Owner	Paul Dickson, JN Manager, IT Enterprise Technology Operations Services	503-230-4075 prdickson@bpa.gov

PRIVACY PROGRAM

Benjamin L Berry Digitally signed by Benjamin L Berry
Date: 2022.08.22 13:05:05 -07'00'

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Candice Palen, CGI FOIA/Privacy Act Officer	503-230-3602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Jessica L. Rackley, JBC Cyber Assessment & Verification	503-230-4416 jlrackley@bpa.gov
Person Completing this Document	Mark R. Gooshaw, JNI System Administrator 3 Enterprise Messaging Team	503-230-3919 mrgooshaw@bpa.gov
Purpose of Information System or IT Project	Microsoft Exchange is the platform on which BPA's email operates and is an integral component of the agency's day-to-day operations. The current version (Exchange 2010) has reached the end of its five-year lifecycle and will no longer be supported. The primary intent of this project is to architect and replace the current implementation of Exchange 2010 with Exchange 2016.	
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 • Email Address	

MODULE I – PRIVACY NEEDS ASSESSMENT

	• Active Directory Account • Title • Company • Department • Office • General information content
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
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.

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?**	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 2016 allows personnel to communicate and share electronic files via email in furtherance of their jobs.
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)?**	External users may decline to provide information by not emailing to a BPA email address. To maintain employment at BPA, employees and contractors must maintain Exchange email accounts. All BPA email users are provided notice through a login warning banner prior to accessing the Exchange 2016 email system.

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?**	All contractors involved with the design, development, maintenance, administration and use of Exchange must sign a non-disclosure agreement (NDA) that includes a Privacy Act clause to cover any exposure to confidential or proprietary information belonging to DOE and associated PII.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	There is the risk that individual users will transmit sensitive personal information through Exchange, but all users are provided a warning banner when they access BPA or DOE-issued hardware, software, or networks stating that they have no expectation of privacy when using such tools. Exchange 2016 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 Taken as a whole, Exchange is assessed as moderate-impact system according to the criteria outlined in Federal Information Processing Standards (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to agency should the system's confidentiality, integrity, or availability be compromised.
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.**	Exchange is used to facilitate communication and workflow sharing between personnel and third parties. Users may be searched for by name. Identifiers include: name, subject matter, date range.

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*.**	Microsoft Exchange 2016 is an update to BPA's current email system. It is not a mechanism used by BPA to collect Privacy Act protected information. BPA employees and contractors are instructed to maintain Privacy Act information that is incidentally captured by the system according to the various SORNs applicable to that particular subset of information.
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?	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, the data elements are detailed in the System Design Specification Documentation.
DATA USE	
11. How will the PII be used?	The email system is not intended to operate as a data repository. The system is designed and intended to be used as a mail relay and is part of the agency's information infrastructure. 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?	Information that is protected by the Privacy Act will be removed from Exchange and continue to be maintained according to the applicable SORN.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	N/A
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?	Yes, use of the email system can be tracked.
18. What kinds of information are collected as a function of the monitoring of individuals?	User login; send and receive logging; all email content logging (i.e. journaling); policy violations.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. Role Based Access Control (RBAC) requires that the appropriate role be assigned to individuals in order to set or use the information collected by monitoring processes
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 email system requires correct email address in order to send or receive email. System users can notify the help desk to request information corrections or updates. All other information that is stored in the Email system is information that is contained within the email message and are not are not verified for accuracy, relevance or completeness.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Email data stores are synchronized between sites using Exchange Database Availability Groups (DAG). The security mechanisms are the same at both sites.
Records Management	
22. Identify the record(s).	The retention period is enforced per BPA policy. The default retention of email data is 90 days. However, BPA email users can extend the retention period up to 3 years by tagging the email with the appropriate retention tag. Users are instructed to move emails that are designated as Federal Records to an authorized Electronic Information System. The appropriate retention period based on NARA approved retention schedules is applied to that record content. Legal holds supersede the retention policies. BPA has adopted NARA's Capstone approach for Senior Executives and Executive Associates Outlook content (see BPA Policy 236-261). These emails are copied from Exchange into Discovery Core Consolidated Archive through a process called journaling and retained within that system for 15 years and then offered to NARA (if permanent) or retained for 7 years (if temporary).
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	There is no disposition authority for non-federal record contents. BPA policy for short term records is to retain while active or until superseded, not to exceed 3 years.
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?	Only authorized users and administrators may access the system.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	• Exchange System Administrators • Backup System Administrators • Active Directory Administrators • Cyber Security Roles • Legal Discovery Roles
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.	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 System Owner
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	PAUL DICKSON (Print Name) Digitally signed by PAUL DICKSON Date: 2022.08.22 12:10:50 -07'00' (Signature)	
Local Privacy Act Officer	Candice Palen (Print Name) Digitally signed by Candice Palen Date: 2022.08.23 09:08:49 -07'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	William K. Hunt (Print Name) Digitally signed by William K. Hunt Date: 2022.08.22 13:22:11 -04'00' (Signature)	