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	03-20-2018
Departmental Element & Site	BPA Headquarters, JST-2 server room
Name of Information System or IT Project	Cisco Meeting Server
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.
New PIA [X] **Update** [ ]	

	Name, Title	Contact Information Phone, Email
System Owner	Chuck Dockery, JNN Supervisory IT Specialist	360-418-8205 cldockery@bpa.gov
Information Owner	George Dover, JNN IT Specialist	503-230-5488 gbdover@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Christopher Frost, CGI FOIA/Privacy Act Officer	503-230-5602 cmfrost@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Jessica Rackley, JBC IT Specialist	503-230-4416 jlrackley@bpa.gov
Person Completing this Document	Dale Kimball, System Architect III (Contractor) Nita Guidoux, CGI Privacy Analyst (Contractor)	503-230-5993 dakimball@bpa.gov 503-230-4705 ahguidoux@bpa.gov
Purpose of Information System or IT Project	Cisco Meeting Server provides and manages voice and video conference call services, including audio bridges, to eliminate MCU-Multiple Call Unit.	
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 – BUD ID, BPA Email	

MODULE I – PRIVACY NEEDS ASSESSMENT

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.*	No, the above listed PII is known to exist 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?	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.

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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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 Bonneville Power Project: Administrative Authority to Contract (16 U.S.C. §§ 832a(f), 839f(a)) grants the Bonneville Power Administration authority to procure contracts to advance the agency's mission. Cisco Meeting Server allows personnel to conduct their jobs in line with BPA's mission.
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)?**	The information shared in Cisco Meeting Server is automatically available through the Outlook address book; it is accessed through Active Directory. Individuals are not asked specifically if they consent to collection of information and BPA employees and contractors must have active accounts in Active Directory.
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 Cisco Meeting Server must sign a non-disclosure agreement (NDA) that includes a Privacy Act clause to cover any exposure to confidential or proprietary information belonging to BPA.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	Cisco Meeting Server 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 • System password protection While Cisco Meeting Server contains some PII, the ensuing risk to the privacy of individuals is generally low as the focus of Cisco Meeting Server is to provide and manage voice and video conference call services, including audio bridges, to eliminate MCU-Multiple Call Unit. This does not require or encourage collection of sensitive PII and is not driven by analysis of PII. No data goes outside of BPA and the information shared in Cisco Meeting Server is the same information available through the Outlook address book. The privacy impact is low sensitivity/low risk PII.
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.**	Data is not retrieved from the system. End users currently dial a common bridge phone number and enter a passcode (sent by the conference host) to join the audio bridge.
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

MODULE II – PII SYSTEMS & PROJECTS

DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Cisco Meeting Server receives data inputs from Active Directory.
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?	No
DATA USE	
11. How will the PII be used?	To facilitate management of conference bridges.
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, the system does not create metadata.
13. With what other agencies or entities will an individual's information be shared?	N/A
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	No reports are produced.
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A

MODULE II – PII SYSTEMS & PROJECTS	
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Voice Administrators can view active calls and identify participants to provide real-time support; no other monitoring and location functionality exists.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A, the system does not monitor individuals.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	The Voice Administrator role is defined within Cisco Meeting Server and is password protected.
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.	Cisco Meeting Server receives data from Active Directory. Active Directory data is updated by Access Control, HRMIS (Human Resources Management Information System), and CMLS (Central Mail List System). Records are kept current, accurate, relevant, and complete in their source systems.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Data is kept at only one site and replicated to local redundant servers.
Records Management	
22. Identify the record(s).	Cisco Meeting Server does not store or transmit Federal records. Cisco meeting invites and call-in data are managed as transitory or short term records, automatically disposed of after 90 days or 3 years, respectively.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	N/A
24. Records Contact	Matt Boris, CGI Records Analyst mjboris@bpa.gov

MODULE II – PII SYSTEMS & PROJECTS

ACCESS, SAFEGUARDS & SECURITY

25. What controls are in place to protect the data from unauthorized access, modification or use?	The data is only accessible by the Voice Administrator. The role is defined within Cisco Meeting Server and is password protected.
26. Who will have access to PII data?	The Voice Administrator.
27. How is access to PII data determined?	Access is determined based on need-to-know.
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?	Cisco Meeting Server ISO and Voice Team Lead.

END OF MODULE II

SIGNATURE PAGE		
	Signature	**Date**
System Owner	MICHAEL BRADEN **(Print Name)** Digitally signed by MICHAEL BRADEN Date: 2022.07.18 07:47:55 -07'00' **(Signature)**	
Information Owner	PAUL DICKSON **(Print Name)** Digitally signed by PAUL DICKSON Date: 2022.07.15 13:21:33 -07'00' **(Signature)**	
Local Privacy Act Officer	Candice Palen **(Print Name)** Digitally signed by Candice Palen Date: 2022.07.19 17:07:42 -07'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	William K. Hunt **(Print Name)** Digitally signed by William K. Hunt Date: 2022.07.07 12:33:55 -04'00' **(Signature)**	