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	08/09/2022	
Departmental Element & Site	TTO – Dittmer & Munro Control Centers	
Name of Information System or IT Project	Physical Infrastructure Program – Critical Area Security (PIP-CAS), part of the Physical Infrastructure Program – General Support System (PIP-GSS) Also known as “Prowatch”	
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions	
New PIA ☒ **Update** □	This is a new PIA for an existing system	
	Name, Title	**Contact Information Phone, Email**
Information System Owner	Huy Ngo Supervisory Electronics Engineer	(360) 418-8094 hnngo@bpa.gov
Information Owner	Huy Ngo	(360) 418-8094 hnngo@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

	Supervisory Electronics Engineer	
Local Privacy Act Officer	Candice Palen Privacy Act Officer	503-230-5602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Rustin Jones Security Systems Consultant	(360) 418-2228 rpjones@bpa.gov
Person Completing this Document	Vicki Mitchell Operations Analyst	(360) 418-2059 vlmitchell@bpa.gov
Purpose of Information System or IT Project	Physical Infrastructure Program – Critical Area Security (PIP CAS) is provided through a physical access control system (ProWatch) and a video monitoring system (Ocularis). This service is available 24/7 as required to meet NERC CIP-006 “Physical Security of Critical Cyber Assets” and FISMA compliance regulations. The main purposes of PIP CAS is to: • Control access to the Control Centers • Monitor physical access points for illicit or unauthorized access • Log physical access • Maintain accurate physical access lists for the Control Centers The system collects the following PII on employees and contractors: - Name - Work phone number - Work email address - Photographs - Work location - BUD ID - PIN code and secret question The system also collects the names of visitors/members of the public, as well as video. There is no identifying information connected to video images.	

MODULE I – PRIVACY NEEDS ASSESSMENT

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, work phone, work email address ☒ Other – photographs with name, video (unidentified), work location, BUD ID, the visitor access request form provides visitor name stored in prowatch, PIN and secret question
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 – this system contains PII
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

MODULE I – PRIVACY NEEDS ASSESSMENT

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?	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.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

MODULE II – PII SYSTEMS & PROJECTS	
1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Bonneville's use of ProWatch to meet security requirements is authorized by 42 USC § 7101, et seq. and Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors.*
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)?**	Indiviuals consent by individually providing their information, either as employees/contractors to BPA, or as members of the public via the Visitor Access Request form. Failure to provide the information could mean loss of employment or denial of a visitor access request.
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, contractors are involved in the design, development, and maintenance of this system. The contract includes the appropriate Privacy Act Clause. Privacy Protection clause (5-2) (FEB 2016) (BPI 5.1.4) and Privacy Assurance clause (5-1) (FEB 2016) (BPI 5.1.4) have been incorporated into the appropriate vendor contracts.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

PIPCAS 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
- Security Controls

The focus of PIPCAS is to maintain access to control centers, which does not require or encourage collection of sensitive PII. However some PII may be required for the general functionality of this system.

The Privacy Impact is moderate.

Confidentiality Factors	Low	Moderate	High
Identifiability		x	
Quantity of PII		x	
Date Field Sensitivity		x	
Context of Use		x	
Obligation to Protect Confidentiality		x	
Access to and Location of PII		x	
Overall PII Confidentiality Level		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, the data can be retrieved by personal identifier, and the routine method of retrival is 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, the SORN is DOE-51, Employee and Visitor Access Control 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?	The Human Resource Information Management System (HRMIS) for standard data about personnel, Access Card PIN database for card key pins, USAccess for badge information, and the Visitor Access Request form for visitor names.
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, in manuals for security personnel and authorized HR staff.
DATA USE	
11. How will the PII be used?	PII is used to verify and permit authorized access to Federal employees, contractors, and other Federal affiliates (including personnel from Federal Protective Services, Counter Intelligence, etc.) seeing authorized access to BPA facilities. General visitors (members of the public) are not entered into PIP CAS and do not have regular access to BPA facilities. Family members and US citizen guests can typically visit controlled parts of BPA after a 24-hour guest application is processed. However, their information is not processed in ProWatch.

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?	Access logs, including the names of employees accessing controlled areas, are submitted to the Western Electricity Coordinating Council (WECC) as required by the Federal Energy Regulatory Commission (FERC). These logs are shared to demonstrate Bonneville's compliance with NERC CIP control requirements. WECC does not share this information with third parties. All other information is shared in accordance with DOE-51.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	The system allows authorized physical and personnel security employees to produce reports on individuals and groups. The following reports/queries can be produced: • Current access status • Access grant history • Access usage history • Area access • Contractor Full Time Employee (CFTE) access history
15. What will be the use of these reports?	These reports are used to ensure that no inappropriate access has been granted.
16. Who will have access to these reports?	Authorized staff from physical security, personnel security, system operations, and grid operations information system security.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes. This system is designed to identify and monitor the ingress and egress of individuals at BPA control centers.

MODULE II – PII SYSTEMS & PROJECTS

18. What kinds of information are collected as a function of the monitoring of individuals?	Date and time ingress and egress for individual access to BPA locations and facilities based on type of access.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Multi-factor authentication, role based access controls (RBAC), periodic verification of accounts, and security event montiroing are implemented to prevent system access to unauthorized individuals. System access requires Information Owner (IO) approval and Information System Owner (ISO) validation prior to being provided access though Active Directory and application security controls.
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.	PIP CAS PII is updated daily by: • Standard information about people which is populated by informatica ETL (Extract, Translate and Load) from HRMis. HRMis has online and batch edits that are built into the system to prevent incomplete or incorrect data entry. Queries and reports within HRMis are used to verify and validate the information in the system regularly. HRMis data is provided to EHRI and error reports are returned to the agency for correction. Self-service access by employee and supervisors ensures the accuracy and completeness of information. • Access Card PIN data is pulled from the source system near real time. Data is provided by individuals and has required fields. • USAccess information is entered manually by the BPA Personnel Security Office.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Information in the system is centrally managed through IO/ISO access approval, Active Directory roles, and system specific roles.
Records Management	
22. Identify the record(s).	Physical access lists, access logs

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	N1-305-07-001-15bSR-1200 - Destroy 6 years after the records are closed.
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?	The System Owner has implemented and tested baseline security controls appropriate to its FIPS categorization in accordance with BPA's Cyber Security Program Plan (CSPP) and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. The system was certified and accredited 6/21/21 and found to have mitigated risk to an acceptable level
26. Who will have access to PII data?	The following roles have access to PII: • Physical Security • Personnel Security • System Operations Staff • Grid Operations Information System Security
27. How is access to PII data determined?	Access is based on the roles and responsibilities of the individual authorized on need-to-know, with the least permissions necessary to complete job duties.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. SSRS (SQL Server Reporting Services) is used for extracting data to report format (internal system/process). Dittmer Prowatch system and Munro Prowatch 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

MODULE II – PII SYSTEMS & PROJECTS

30. Who is responsible for ensuring the authorized use of personal information?	The Manager, and Physical Security/Information Owner are responsible for ensuring the authorized use of personal information.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) HUY NGO Digitally signed by HUY NGO Date: 2023.04.17 11:14:30 -07'00' (Signature)	
Information Owner	(Print Name) HUY NGO Digitally signed by HUY NGO Date: 2023.04.17 11:14:41 -07'00' (Signature)	
Local Privacy Act Officer	(Print Name) Candice Palen Digitally signed by Candice Palen Date: 2023.04.17 11:51:14 -07'00' (Signature)	
DOE **Chief Privacy Officer**	(Print Name) Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2023.04.06 11:11:05 -04'00' (Signature)	