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	07/24/2023	
Departmental Element & Site	USDOE/Bonneville Power Administration (BPA), Headquarters, Portland, Oregon	
Name of Information System or IT Project	SharePoint – HSPD-12 List	
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 collection of hard-copy files that are being digitized and stored on SharePoint. See PIV Files PIA.	
	Name, Title	**Contact Information Phone, Email**
Information System Owner	Kirsten Kler, Supervisory Security Specialist, Personnel and Information Security (NNP)	(503) 230-4411 kmkler@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Information Owner	Kirsten M. Kler, Supervisory Security Specialist, Personnel and Information Security (NNP)	(503) 230-4411 kmkler@bpa.gov
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.)	Nick Choi, JLS IT Specialist	503-230-5397 hcchoi@bpa.gov
Person Completing this Document	Kirsten Kler, Supervisory Security Specialist, Personnel and Information Security (NNP)	(503) 230-4411 kmkler@bpa.gov
Purpose of Information System or IT Project	Personal Identity Verification (PIV) file folders are used to store hard copy files of various pieces of information related to a person's onboarding, identity proofing verification date, and investigation completion date, including reinvestigation completion dates and final play clearance out-processing form. This is hard copy information retained for compliance required by Homeland Security Presidential Directive 12 (HSPD 12) and North Americam Electric Reliaility Corporation Critical Infrastructure Protection (NERC CIP). As of 6 Feb 2023, the PIV file folders are being digitized and stored on Personnel Security's Sharepoint list called "HSPD-12." The digitation process is expected to take place over the course of 12-18 months. During that time, PIV files exist in the Kardex (hard copies) and this SharePoint site concurrently. For more information about SharePoint, see the SharePoint Services PIA.	
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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Mother's Maiden Name ☒ DoB, Place of Birth ☒ Employment Information ☒ Criminal History ☒ Name, Phone, Address ☒ Other – Please Specify (HRMIS ID, BUD ID, email address, family member information, adjudication results, appeals correspondence, Levels of Investigation, denials, etc.)
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, PII exists in the documents.
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?	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?

The following authorities apply:

- Executive order 10450: *Security Requirements for Government Employment*.

- 42 5 U.S.C. § 2165: *Security Restrictions*.

REFERENCES.

- Executive Office of the President, Homeland Security Presidential Directive 12, August 27, 2004, (Reference attached to M-05-24) Homeland Security Presidential Directive 12 | Homeland Security (dhs.gov)
- Executive Office of the President, National Strategy for Trusted Identities in Cyberspace (NSTIC), April 2011. The National Strategy for Trusted Identities in Cyberspace | whitehouse.gov (archives.gov)
- OMB Memorandum 04-04, E-Authentication Guidance for Agencies, December 2003. M-04-04 (archives.gov)
- DOE O 470.4B, Safeguards and Security Program, July 21, 2011 I.
- DOE O 471.3, Identifying and Protecting Official Use Only Information, April 9, 2003.
- DOE O 473.3, Protection Program Operations, June 29, 2011
- DOE Federated ICAM Framework, June 30, 2011,
- X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, fpki-x509-cert-policy-common.pdf (idmanagement.gov)
  - OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005. MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES (archives.gov)
- OMB Memorandum 11-11, Continued Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors, February 2011. Memorandum for the Heads of Executive Departments and Agencies (cac.mil)
- OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006, Memorandum (archives.gov)
- OMB Memorandum, Requirements for Accepting Externally-Issued Identity Credentials, October 6, 2011, Requirements for Accepting Externally Issued Identity Credentials – Digital.gov
- Office of Personnel Management (OPM) memorandum, subject: Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD–12, July 31, 2008, Final Credentialing Standards for Issuing Personal Identity

MODULE II – PII SYSTEMS & PROJECTS

<table>
<tr><td></td><td>Verification Cards under HSPD-12 (opm.gov)</td></tr>
<tr><td><b>2. CONSENT</b>
<b>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)?</b></td><td>Individuals can decline to provide information, but doing so will result in lack of consideration for employment/badge issuance and access to government facilities and information.</td></tr>
<tr><td><b>3. CONTRACTS</b>
<b>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?</b></td><td>For SharePoint, see the SharePoint Services PIA. For HSPD-12 SharePoint list, yes, contractors are involved in the operations and management of information. Contractors are required to safeguard all information in accordance with the Privacy Act and BPA and DOE Policy.
All employees and contractors must complete Cyber Security training prior to being granted network access and yearly thereafter. All employees and contractors are required to complete annual privacy training.</td></tr>
<tr><td><b>4. IMPACT ANALYSIS:</b>
<b>How does this project or information system impact privacy?</b></td><td>The privacy impact risk is HIGH
<table>
<tr><th>Confidentiality Factors</th><th>Low</th><th>Moderate</th><th>High</th></tr>
<tr><td>Identifiability</td><td></td><td></td><td>x</td></tr>
<tr><td>Quantity of PII</td><td></td><td></td><td>x</td></tr>
<tr><td>Data Field Sensitivity</td><td></td><td></td><td>x</td></tr>
<tr><td>Context of Use</td><td></td><td></td><td>x</td></tr>
<tr><td>Obligation to Protect Confidentiality</td><td></td><td></td><td>x</td></tr>
<tr><td>Access to and Location of PII</td><td></td><td></td><td>x</td></tr>
<tr><td><b>Overall Privacy Risk</b></td><td></td><td></td><td><b>x</b></td></tr>
</table>
</td></tr>
</table>

MODULE II – PII SYSTEMS & PROJECTS

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 is retreived by name.
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*.**	The applicable SORNs are: DOE-43: Personnel Security Files DOE-51: Employee and Visitor Access Control Records DOE-63: Personal Identity Verification files
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?	Individuals provide most of the data directly to Information Security. Some information is received from other federal agencies as it relates to background investigation information.
9. Will the information system derive new or meta data about an individual from the information collected?	In some cases, yes. New data such as suitability determination is derived from the data provided.
10. Are the data elements described in detail and documented?	Yes. All of the data elements (name, DOB, POB, SSN, fingerprint images) are described and documented in Information Security procedures.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS

11. How will the PII be used?	The PII is obtained directly from individuals and transmitted to the Defense Counterintelligence and Security Agency (DCSA) for background investigations, to verify identity, and to determine suitability for a position with the government and/or for a security clearance. This data is printed and placed in PIV hard copy files, HSPD-12 and ShareDrive working folder for evidence and used for required compliance actions related to access issuance and revocation.
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?**	Some new data such as suitability determination becomes a part of the convenience copy in the file.
13. With what other agencies or entities will an individual's information be shared?	Data is shared with the Office of Personnel Management (OPM).
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	No reports are created by BPA.
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?	No
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A

MODULE II – PII SYSTEMS & PROJECTS

19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A
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.	New information is requested of individuals as part of reinvestigations and the data is reviewed for accuracy at that time.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A – All of the KARDEX files are located in one location while all digital files are located in HSPD-12. Some extra-sensitive files and intermediary files are stored on the Network Drive.
Records Management	
22. Identify the record(s).	HSPD-12 Checklist is a Microsoft SharePoint list hosted on BPA's Intranet and is the system of record for Personal Identity Verification (PIV) records. PIV records are digital files containing various electronic forms used to collect information related to a persons' on-boarding/out-processing actions, identity verification, and investigation/re-investigation completion. PIV records are artifacts utilized to ensure compliance with Homeland Security Presidential Directive 12 (HSPD 12) and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP).
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	SR-1205; Destroy mandatory/optional data housed in agency identity management system and printed on the ID card 6 years after terminating an employee or contractor's employment.
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?	HSPD-12 has role-based permissions that are reviewed quarterly. NNP will complete and maintain a SharePoint Governance plan which includes permissions management.

MODULE II – PII SYSTEMS & PROJECTS

26. Who will have access to PII data?	Personnel and Information Security Specialists assigned to NNP.
27. How is access to PII data determined?	Personnel and Information Security Specialists, and NNP Contractors who are cleared for this system will have access. Access is granted strictly on a 'need to know' basis. Personnel Security group maintains a SharePoint Governance plan.
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?	Personnel and Information Security Supervisory Security Specialist

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) STEFHANIE MCLAUGHLIN Digitally signed by STEFHANIE MCLAUGHLIN Date: 2024.04.09 07:55:50 -07'00' (Signature)	
Information Owner	(Print Name) STEFHANIE MCLAUGHLIN Digitally signed by STEFHANIE MCLAUGHLIN Date: 2024.04.09 07:56:21 -07'00' (Signature)	
Local Privacy Act Officer	(Print Name) CANDICE PALEN Digitally signed by CANDICE PALEN Date: 2024.04.09 10:19:53 -07'00' (Signature)	
DOE **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2024.04.01 09:59:32 -04'00' (Signature)	