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	04/04/2022
Departmental Element & Site	USDOE/Bonneville Power Administration (BPA), Headquarters, Portland, Oregon
Name of Information System or IT Project	Mentalix Fingerprint Security System (DCSA)
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.
New PIA ☐ **Update** X	This is a PIA update for an existing system (09.06.2017) that was previously signed on 03.16.2022.

	Name, Title	Contact Information Phone, Email
Information System Owner	ISO Yvette Gill Supervisory IT Specialist ISO Delegate	(503) 230-3947 yrgill@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

	Timothy M. Steed, Supervisory IT Specialist, IT Service Desk (JRS)	(360) 418-8601 tmsteed@bpa.gov
Information Owner	IO Sarah Laylo Chief Security Officer IO Delegate Kirsten M. Kler, Supervisory Security Specialist, Personnel and Information Security (NNP)	503-230-5295 smlaylo@bpa.gov (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.)	George M. Callaway III, Cyber Forensics & Intelligence (JBB)	(503) 230-5902 gmcallaway@bpa.gov
Person Completing this Document	Stefhanie McLaughlin, Security Specialist, Personnel and Information Security (NNP)	(503) 230-3283 samclaughlin@bpa.gov
Purpose of Information System or IT Project	Mentalix is a fingerprint transaction system used to capture and transmit fingerprint biometric data from BPA to Defense Counterintelligence and Security Agency (DCSA) for the purpose of performing personnel background investigations.	
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"	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ 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
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 is contained in the system.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A, PII is contained in the system.

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

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?**	• Executive order 10450: Security Requirements for Government Employment. • Executive Order 10865: Safeguarding Classified Information within Industry. • Executive Order 12333: United States Intelligence Activities. • Executive Order 12356: National Security Information. • 5 U.S.C. § 3301: Government Organization and Civil Service, Generally. • 5 U.S.C. § 9101: Access to Criminal History Records for National Security and other Purposes. • 42 U.S.C. § 2165: Security Restrictions.
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)?**	Individuals can decline to provide information, but doing so will result lack of consideration for employment.
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?**	This software was purchased as a commercial-off-the-shelf (COTS) product. BPA accepted the standard terms, which meet FISMA requirements. The Privacy Act clauses were included in the contract.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The potential impact is High. The potential for privacy concerns if the system is compromised could be expected to have a serious adverse effect on individuals or BPA's operations or assets.

	Impact Level		
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.

The data is submitted to DCSA by name and SSN. DCSA is the sole consumer of the data. The data can be retrieved by name for the first 10 days, but there is no regular business process that requires BPA to retrieve it. Once submitted to DCSA, the data is purged within 10 days from BPA's system.

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-43: Personnel Security Files. 74 FR 1044-1045.
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 data directly.
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. All of the data elements (Name, DOB, POB, SSN plus fingerprint images) are described and documented in the SSP.
DATA USE	
11. How will the PII be used?	The PII is obtained directly from individuals and transmitted to DCSA for background investigations, to verify identity, and determine suitability for a position with the government and/or for a security clearance.

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?**	This system uses applicant-provided data and does not create new data.
13. With what other agencies or entities will an individual's information be shared?	Yes. Information is shared with Defense Counterintelligence and Security Agency (DCSA).
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
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.	Records are retained by BPA for 10 days then purged.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	System Owners and information owners are responsible for ensuring information is used and managed consistently for its stated purpose in support of the organization. The system will be monitored and patched in compliance with BPA system processes and procedures.
Records Management	
22. Identify the record(s).	All content captured in Mentalix is transmitted to DCSA and then purged from Mentalix 10 days after transmittal.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 5.2, Item 010, Transitory records.
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 all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. The system was certified and accredited (SSP and POAM in process) and found to have mitigated risk to an acceptable level.
26. Who will have access to PII data?	Personnel and Information Security Specialists Information Technology Specialists
27. How is access to PII data determined?	Personnel and Information Security Specialists, IT System Administrators, and Contractors who are cleared for this system will have access. Access will be granted strictly on a 'need to know' basis.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	This system will utilize a 'point to point' virtual private network (VPN) encryption tunnel between these two computers and DCSA for the purpose of transmitting this biometric data.

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?	Yes, there is a current Interconnection Security Agreement.
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)** YVETTE GILL Digitally signed by YVETTE GILL Date: 2023.03.10 09:20:42 -08'00' _____ **(Signature)**	_____
Information Owner	**Kirsten M. Kler** **(Print Name)** KIRSTEN KLER Digitally signed by KIRSTEN KLER Date: 2023.03.13 10:16:14 -07'00' _____ **(Signature)**	_____
Local Privacy Act Officer	_____ **(Print Name)** Candice Palen Digitally signed by Candice Palen Date: 2023.03.13 11:37:10 -07'00' _____ **(Signature)**	_____
DOE Chief Privacy Officer	_____ **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.03.10 10:17:17 -05'00' _____ **(Signature)**	_____