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

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	9/6/17
Departmental Element & Site	USDOE/Bonneville Power Administration (BPA), Headquarters, Portland, Oregon
Name of Information System or IT Project	Mentalix Fingerprint Security System (OPM)
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	Timothy M. Steed, Supervisory IT Specialist, IT Service Desk (JRS)	(360) 418-8601 tmsteed@bpa.gov
Information Owner	Kirsten M. Kler, Supervisory Security Specialist, Personnel and Information Security (NNP)	(503) 230-4411 kmkler@bpa.gov

PRIVACY
PROGRAM

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Christopher, M. Frost, Supervisory Government Information Specialist (CGI)	(503) 230-5602 cmfrost@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	Robert E. Barnes, IT Specialist (Customer Support), Client Service Representative (JRS)	(360) 418-1656 rebarnes@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 National Background Investigations Bureau (NBIB) and Office of Personnel Management (OPM) 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" ☒ 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	

PRIVACY PROGRAM

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.*	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?**	☑ 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?**	• 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 5 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 in rejection and lack of consideration for employment.

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?**	This software was purchased as a commercial-off-the-shelf (COTS) product. BPA accepted the standard terms, which meet FISMA requirements.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed Mentalix Fingerprint Security System as a moderate risk system for confidentiality, integrity, and availability according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. Mentalix Fingerprint Security System 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 The focus of the Mentalix Fingerprint Security System is to to capture and transmit fingerprint biometric data from BPA to National Background Investigations Bureau (NBIB) and Office of Personnel Management (OPM). 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. The Mentalix Fingerprint Security System contains some PII. The ensuing risk to the privacy of individuals and potential impact is moderate.

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.**	The data is submitted to OPM by name and SSN. OPM 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 OPM, the data is purged within 10 days from BPA's system.
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.

MODULE II – PII SYSTEMS & PROJECTS

DATA USE

11. How will the PII be used?	The PII is obtained directly from individuals and transmitted to OPM for background investigations, to verify identity, and determine suitability for a position with the government and/or for a security clearance.
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 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.	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).	No Federal record content is created or stored in the system; therefore this is a non-reportable system. All content captured in Mentalix is transmitted to OPM for maintenance and then purged from BPA's system 10 days after transmittal.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	N/A
24. Records Contact	Matt Boris, Records Analyst mjboris@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 Specialist Information Technology Specialist

PRIVACY PROGRAM

MODULE II – PII SYSTEMS & PROJECTS

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 NBIB/OPM for the purpose of transmitting this biometric data.
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	___Timothy M. Steed_____ **(Print Name)** _____ **(Signature)**	_____
Information Owner	____Kirsten M. Kler_____ **(Print Name)** _____ **(Signature)**	_____
Local Privacy Act Officer	_____ **(Print Name)** _____ **(Signature)**	_____
Ken Hunt **Chief Privacy Officer**	_____ **(Print Name)** _____ **(Signature)**	_____