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: http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

Please complete electronically: no hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	November 9, 2009
Departmental Element & Site	Bonneville Power Administration Ethics Helpline, hosted and operated by Global Compliance Charlotte, North Carolina
Name of Information System or IT Project	Bonneville Power Adminstration Ethics Helpline Hosted and operated by Global Compliance Charlotte, North Carolina
Exhibit Project UID	BPA Contract Number: 43705
New PIA X **Update**	

	Name, Title	Contact Information Phone, Email
System Owner	John Hairston, Chief Compliance Officer	(503) 230-5262 jlhairston@bpa.gov
Local Privacy Act Officer	Christina J. Brannon – Freedom of Information Act/Privacy Act Officer & Chief Public Affairs Officer	(503) 230-7303 cjbrannon@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Sean Barry, Information Security Officer	503-230-3382 spbarry@bpa.gov
Person Completing this Document	Helen A. Goodwin, Ethics Program Manager	503-230-3129 hagoodwin@bpa.gov
Purpose of Information System or IT Project	The BPA ethics helpline will be used by BPA to document and resolve employee concerns about environmental, safety and health issues, employee-supervisor relations, work processes and practices, and other work-related issues consistent with DOE-3.	
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: Any or all of the above may be reported consistent with the categories of records listed in DOE-3. Reporters must provide sufficient detail to permit investigation or other appropriate levels of review	

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. This is a new system.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	NA

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 *Member of the Public* refers to individuals in a non-employee or DOE contractor context. *Members of the Public* includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE.
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

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.

...odule II must be completed for all systems if the answer to any of the four (4) threshold

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	42 U.S.C. 7101 *et seq.*; 50 U.S.C. 2401 *et seq.*; 42 U.S.C 2201(p); 42 U.S.C. 7254; 42 U.S.C. 5801(a).

MODULE II – PII SYSTEMS & PROJECTS

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)?**	Employees or contractors calling into BPA's third-party vendor operated helpline or using the vendor's web portal to report employee concerns may do so anonymously. They may decline to answer any question, give as much or as little information to the vendor operated contact center or on the web as they feel comfortable reporting.
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. Privacy Act clause 5-1 of the Bonneville Purchasing Instructions is included in BPA's contract number 43705 with Global Compliance.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	Using FIPS Publication 199, BPA has determined the security categorization (SC) for the ethics helpline system to be as follows: Confidentiality = moderate Integrity = low Availability = low Resulting in an overall security categorization of moderate. BPA and its vendor, Global Compliance have taken steps to ensure there is low risk of a security breach. Global Compliance has a system security plan in place to ensure the appropriate protection, retention, and destruction of BPA's information. The security controls protect the confidentiality of the information stored. Should the system fail and a breach occurs, the identities of reporter (unless anonymous), subject, investigator and any other parties could be revealed. Information about the reported incident and any investigation, both of which could contain information about individuals, might also be revealed to unauthorized sources. This could result in a loss of credibility for BPA.

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.**	Data may be retrieved by the unique identifier provided by the third-party vendor, Global Compliance. A search feature allows data to be retrieved by name, location, date, type of complaint, etc.
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. A SORN has been published in the Federal Register. BPA has been added as a system location under DOE-3, Employee Concerns Program Records. DOE-3 can be found in the Federal Register/Volume. 74, No. 6/Friday, January 9, 2009.
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	The notice to amend DOE-3 to include BPA as a system location was published in Volume 74, No. 158 of the Federal Register on August 18, 2009. The amendment became effective on October 2, 2009. No comments were received.

DATA SOURCES

MODULE II – PII SYSTEMS & PROJECTS

8. What are the sources of information about individuals in the information system or project?	BPA employees and contractors may call into the third-party vendor operated helpline or use web reporting to report a concern or ask a question. The categories of records in the system will be consistent with DOE-3. The BPA ethics helpline is available to employees and contractors 24/7/365. All reports will be entered into the case management system. BPA will be notified by the vendor, Global Compliance, when a new report is made. In order to access a report, authorized BPA employees will need to log into the case management system. The case management system is password protected. The BPA system administrator will control access to the case management system.
9. Are the data elements described in detail and documented?	BPA is working with the third-party vendor, Global Compliance to document all the data elements in detail in a system security plan. The system security plan will be reviewed and approved by BPA's Chief Operating Officer.
DATA USE	
10. How will the PII be used?	Information, including PII, will be used by executives, managers and others to promote ethical behavior at BPA and promote a culture of compliance. All reports coming in through the call center or through the web will be investigated. In some cases, disciplinary action may be taken as a result of an investigation consistent with BPA policy and procedures.
11. With what other agencies or entities will an individual's information be shared?	BPA will share information consistent with DOE-3, routine uses of records maintained in the system, including categories of users and the purposes of such uses.
12. What kinds of reports are produced about individuals or contain an individual's data?	BPA does not intend to produce reports about individuals or contain an individual's data. Summary reports will be provided to management regarding the type and number of reports received and the disposition of those reports. No reports containing information about individuals or contain an individual's data will be shared.
13. What will be the use of these reports?	Reports will be used by management and staff to improve the ethics program, identify risk areas, take remedial action and promote a culture of compliance.

MODULE II – PII SYSTEMS & PROJECTS	
14. Who will have access to these reports?	BPA's ethics program manager is the system administrator. Executive management, compliance staff, attorneys and employees involved in disciplinary actions may have access to reports. Subject matter experts may receive reports on a need to know basis.
15. Will this information system provide the capability to identify, locate, and monitor individuals?	Information will not be collected to monitor individuals.
16. What kinds of information are collected as a function of the monitoring of individuals?	Information will not be collected to monitor individuals.
17. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. The system administrator has the ability to limit users of the case management system.
DATA MANAGEMENT & MAINTENANCE	
18. 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.	All reports received via the Global Compliance third-party vendor operated helpline will be investigated. If the information received cannot be verified, the case will be closed and it will be so stated. PII data collected from sources other than DOE records, such as reporter attestations, may be verified through the course of the investigation.
19. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Information will be centrally stored in the Global Compliance case management system using a unique identifier and is password protected. Individuals with access to the case management system will be asked to add investigator notes or other information to the case file. Access to each case file is limited to those whose official duties require access to the records.

MODULE II – PII SYSTEMS & PROJECTS

20. What are the retention periods of data in the information system?	Records retention authorities are contained in the NARA General Records Schedule and BPA records schedules that have been approved by NARA. Data in the case management system will be purged on a schedule set by BPA; the current retention schedule is a minimum of eight years. Procedures for the disposition of data at the end of the retention period will be provided to the third-party vendor by BPA.
21. What are the procedures for disposition of the data at the end of the retention period?	BPA's will enforce retention periods of data in the third-party vendor operated case management system through the ethics helpline contract. As a best practice, Global Compliance does not purge client data automatically. They do not have standard processes for deleting electronic records on a particular schedule. Global Compliance can if specifically requested and authorized by BPA, completely purge client report records from their system. This process must be initiated by BPA. BPA will ask Global Compliance to purge data on a schedule set by BPA; the current NARA retention schedule N1-305-07-1-5/c is a minimum of eight years. Procedures for the disposition of data at the end of the retention period will be provided to the third-party ethics helpline provider by BPA.

ACCESS, SAFEGUARDS & SECURITY

22. What controls are in place to protect the data from unauthorized access, modification or use?	Following the BPA PCSP and applicable NIST guidelines, the security controls for the system will be documented and evaluated prior to the system receiving an authority to operate.
23. Who will have access to PII data?	BPA's Chief Operating Officer, Deputy Administrator, Chief Compliance Officer, Ethics Program Manager, Internal Audit Manager, Ethics Advisors in the Office of General Counsel, managers and subject matter experts with a need to know.
24. How is access to PII data determined?	The BPA System Administrator will control access to the system. Access is limited to those whose official duties require access to the records contained in the case management system.
25. Do other information systems share data or have access to the data in the system? If yes, explain.	No

MODULE II – PII SYSTEMS & PROJECTS	
26. 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?	An Interconnection Security Agreement (ISA) is not required. The BPA Ethics Helpline is software for service and will be hosted by a third party vendor, Global Compliance.
27. Who is responsible for ensuring the authorized use of personal information?	Chief Compliance Officer, Ethics Program Manager
END OF MODULE II	

SIGNATURE PAGE		
	Signature	Date
PIA Approval Signatures	Original Copy Signed and On File with the DOE Privacy Office	