MA 1028

Department of Energy
Privacy Impact Assessment (PIA)

Affects Members Of the Public? X

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	May 6, 2010
Departmental Element & Site	Office of Management
Name of Information System or IT Project	Industry Interactive Procurement System (IIPS)
Exhibit Project UID	019-60-01-17-02-3020
New PIA ☐ **Update** X	Updating PIA from 2008-08-13

	Name, Title	Contact Information Phone, Email
System Owner	Douglas Baptist Director, Information Management Systems Division, MA-623	(202) 287-1658 Douglas.Baptist@hq.doe.gov
Local Privacy Act Officer	Jerry Hanley Chief Privacy Officer U.S. Department of Energy	(202) 586-0483 Jerry.Hanley@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Ilir Angjeli Office of Information Resources, MA-90	(202) 586-3282 Ilir.Angjeli@hq.doe.gov
Person Completing this Document	Ellen Colligan System Manager, MA-623	(202) 287-1776 Ellen.Colligan@hq.doe.gov
Purpose of Information System or IT Project	The Industry Interactive Procurement Systems (IIPS) is the application engine that serves as the foundation of the DOE "e-Center" website. The DOE e-Center has been formally designed with the intent to record, publish, and procure external contractual business transactions within the Department of Energy. Such transactions entail the viewing of current business opportunities, registering to submit proposals, and obtaining information and guidance on the acquisition and financial assistance award process. The e-Center website supports the interface and information transactions between government and industry and between government agencies. IIPS: • Enables DOE end-users and members of the public to request and receive email notification of updates to specific solicitations • Enables bid & application submission as appropriate to the DOE in response to a variety of acquisition and financial assistance opportunities • Enables review of proposals by Proposal Evaluators & Project Managers • Enables Contracting Officers or Grant Officers to conduct negotiations and/or clarifications to a prior submission • Publishes announcements to appropriate pan-agency web sites – Grants.gov and/or FedBizOpps	
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 - Procurement Sensitive Information
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.*	PII is known to exist in the system There has not been any attempt to verify that PII does not exist on the system
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 ☐ 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 I – PRIVACY NEEDS ASSESSMENT

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?**	42 U.S.C. 7101 et seq.; 50 U.S.C. 2401 et seq.; the GAO Policy and Procedures Manual; Statement of Federal Financial Accounting Standards published by the Government Accountability Office and the Office of Management and Budget; Debt Collection Improvement Act of 1996, 31 U.S.C. 3512; 5 U.S.C. 5701–09; Federal Property Management Regulations 101–107; Treasury Financial Manual; Executive Order 12009; and Executive Order 9397.

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)?**	IIPS contains copies of proposals and grant applications submitted by potential Vendors to the DOE, in response to DOE-issued Requests for Proposals and Grant Opportunities. Each individual potential Vendor has a choice as to whether or not to submit a proposal or grant application.
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 with the design and development of the system and will be involved with the maintenance of the system. Personal information from IIPS may be disclosed as a routine use to these contractors and their officers and employees in performance of their contracts. Those individuals provided information under this routine use are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need-to-know basis. Contractors are required to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of DOE. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

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 proposals and grant applications may be retrieved by the vendor or applicant name, DUNS #, or proposal or bid number for vendors/applicants. The sensitive information can not been viewed until the proposal is opened. Note, sensitive information is not stored explicitly in the IIPS database, It is only available in the attachments/proposals stored in IIPS.
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-82 Grant and Contract Records for Research Projects, Science Education, and Related Activities
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?	Proposals and grant applications submitted by potential Vendors or applicants to the DOE, in response to DOE-issued Requests for Proposals and Grant Opportunities.
9. Will the information system derive new or meta data about an individual from the information collected?	No.

MODULE II – PII SYSTEMS & PROJECTS	
10. Are the data elements described in detail and documented?	No. The procurement sensitive data present in proposals and grant applications depends upon the requirements present in each specific Solicitation or Grant Opportunity published by DOE in IIPS.
DATA USE	
11. How will the PII be used?	The PII, along with all other data collected, is relevant and necessary for DOE to perform contract/grant solicitation and award activities.
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?**	The IIPS system will NOT derive new data or meta data.
13. With what other agencies or entities will an individual's information be shared?	The Department of Health and Human Services and the General Services Administration
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	N/A
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?	IIPS does not have the capability to identify, monitor, or locate individuals.
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?	IIPS established policies and procedures for controlling and monitoring access to the system. The controls are detailed in the IIPS system security plan. Security Plan Name: System Security Plan For Industry Interactive Procurement System (IIPS), dated April 29, 2010, signed by Douglas Baptist, system owner.
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.	The data in each proposal or grant application is provided by the potential Vendor submitting the information. There is no attempt to verify the accuracy and completeness of the data. Once the DOE-issued solicitation has closed, all proposals or grant applications are stored in IIPS because they are federal records. Federal records are not permitted to be updated or changed.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	IIPS is operated and maintained in the DOE AHE. There is a mirror database located in the hosting environment of the DOE Chicago Operations Office (DOE-CH) for disaster recovery purposes. The mirroring of the information between the two locations is automatic. DOE-CH hosting environment staff does not have login ID access to the system.
Retention & Disposition	
22. What are the retention periods of data in the information system?	The proposals or grant applications are stored in IIPS for the seven year retention period defined by the NARA-approved DOE Records Schedule.
23. What are the procedures for disposition of the data at the end of the retention period?	The proposals or grant applications are deleted from IIPS after the seven year retention period has elapsed.
ACCESS, SAFEGUARDS & SECURITY	
24. What controls are in place to protect the data from unauthorized access, modification or use?	IIPS is a rights and permissions-based system. Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access via userid and password based on user responsibility and job function. These access controls are defined in the system security plan "System Security Plan For Industry Interactive Procurement System (IIPS)", dated April 29, 2010, signed by Douglas Baptist, system owner. A "Rules of Behavior" link containing consequences for violating the rules are displayed to the user each time the user logs onto the system. Administrative controls include separation of duties so individuals only have access to appropriate pieces of personal information and use of system audit logs to monitor access and user activity in the system.

MODULE II – PII SYSTEMS & PROJECTS	
25. Who will have access to PII data?	All DOE personnel connected to the DOE internal network may view the non-sensitive, public information within IIPS via anonymous access. Access to sensitive and/or proprietary data in the system is strictly controlled based on job responsibility and function. Certain authorized DOE procurement officials (DOE Contracting Officers/Contract Specialists and Grant Officers/Grant Specialists) are registered users who may view the sensitive and/or proprietary information in the database via a User ID and password.
26. How is access to PII data determined?	Access to data is determined by evaluation of personnel job responsibilities and functions. Based on the evaluation, access control lists are documents and applied to the system. System controls and integrity reports are reviewed on a regular basis to ensure users have the appropriate level of access. The IIPS System Security Plan more completely documents access controls.
27. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes, IIPS retrieves grant applications from Grants.gov for review and processing within DOE. IIPS also shares data with FedBizOpps for procurement opportunities.
28. 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?	The following MOUs are part of Appendix F, System Security Plan For Industry Interactive Procurement System (IIPS), dated April 29, 2010, signed by Douglas Baptist, system owner. MOU between Grants.gov and IIPS, dated 5-10-07 MOU between DOE-CH and IIPS, dated 10-04-07 MOU between FedBizOps and IIPS, dated 10-03-07 MOA between AHE and IIPS, dated 9-7-2006
29. Who is responsible for ensuring the authorized use of personal information?	Individual users are responsible for the proper use of the data per the non-disclosure requirements fundamental to their positions as Contracting Officers, Contract Specialists, Grant Officers, and Grant Specialists.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	Douglas Baptist (Print Name) (Signature)	5/7/10
Local Privacy Act Officer	Jerry Hanley (Print Name) N/A (Signature)	
Jerry Hanley Chief Privacy Officer		07/14/10
Ingrid Kolb Senior Agency Official for Privacy (SAOP)		8-24-10