MA-1026

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	February 24, 2010	
Departmental Element & Site	Office of Management	
Name of Information System or IT Project	Energy Contractor Registration System (EnCoRe)	
Exhibit Project UID	019-60-01-17-02-3020	
New PIA □ Update ☒	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,	(202) 586-0483 Jerry.Hanley@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

	U.S. Department of Energy	
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Phil Knopp Office of Corporate Information Systems, CF-40 Germantown, U.S. Department of Energy	(301) 903-0364 Phil.Knopp@hq.doe.gov
Person Completing this Document	Larry Hardison System Manager	(202) 287-1565 Larry.Hardison@hq.doe.gov
Purpose of Information System or IT Project	According to the Federal Acquisition Regulation (FAR) policy FAR 4.1102 (October 1, 2003), "Prospective contractors shall be registered in the Central Contractor Registration (CCR) database prior to award of a contract or agreement." The Defense Information Systems Agency (DISA) created and maintains the CCR database (www.ccr.gov), as the primary vendor database for the U.S. Federal Government. CCR collects, stores, and disseminates vendor data in support of agency acquisition missions. For each vendor it contains both public information and some sensitive and/or proprietary information. Therefore CCR allows public (anonymous) access to the public information, but denies access to the sensitive and/or proprietary information to anyone except authorized federal procurement officials who have signed a non-disclosure agreement. The purpose of the existence of the sensitive and/or proprietary information in CCR is to allow Federal (including DOE) authorized procurement officials and financial specialists the ability to set up electronic payment of invoices once an acquisition or financial assistance contract is instituted. DISA manages the secure access and authentication for authorized procurement officials in Department of Defense agencies but does not manage authorized access for civilian agencies. Rather, DISA allows civilian agencies to create and update a read-only copy of the CCR to reside within a secure environment at each respective civilian agency. Each civilian agency maintains the secure access and authentication processes for its own authorized procurement officials, and conducts its operations based upon a Memorandum of Understanding (MOU) with DISA. EnCoRe is the DOE database system that duplicates the information in the CCR. It is a read-only copy of the CCR data, residing within the DOE Office of the CIO's GSS Application Hosting Environment (AHE). Access to EnCoRe is restricted to users within the secure DOE network or to users with DOE VPN access. Such users are	

MODULE I – PRIVACY NEEDS ASSESSMENT

able to gain anonymous access to the publicly-available information within EnCoRe that CCR itself provides to the general public. However, EnCoRe also manages security to allow specific, authorized DOE staff to gain access to the sensitive and/or proprietary information in the database. (This is the primary reason EnCoRe is needed by DOE – anyone inside or outside DOE can view the publicly available information in the CCR itself.) All employees who are given access to the EnCoRe database are required to sign the non-disclosure agreement (NDA) specified by DISA. Copies of the NDAs are on file in the Office of Procurement and Assistance Management, Information Systems Division.

Like CCR itself, EnCoRe comprises an Oracle database back-end, and a browser-based user interface with a search function to locate specific vendors. However, there are two significant differences:

1. EnCoRe includes a function that allows authorized administrators, at the direction of the MA system owner, to create and manage the accounts that allow only specific DOE procurement officials and financial specialists to view sensitive and/or proprietary information in the database, and
2. EnCoRe does not allow any user (anonymous or registered) to change system information – this function is provided only by DISA's CCR system. The EnCoRe system administration function does not allow editing of any vendor information – the database is read-only. EnCoRe pulls information from the CCR using the CCR extracts but does not push information back to the CCR.

For each vendor, EnCoRe duplicates the CCR's business information including its DUNS number, Tax Identification Number (TIN), physical and mailing address, number of employees, points of contact, type of business, and other information that is generally publicly available. EnCoRe also duplicates the CCR's sensitive and/or proprietary information for vendors, including specific sensitive financial information such as bank account numbers.

Type of Information Collected or Maintained by the System:	☒ SSN Social Security number (note: tax identification numbers (TIN) are stored in EnCoRe. In some cases, entities use their social security number (SSN) as their TIN. However, due to the different formatting of the SSN and TIN, there is no way to identify which TIN's stored in EnCoRe are SSN's. Further, no attempt is made to verify whether a TIN is a SSN.)

MODULE I – PRIVACY NEEDS ASSESSMENT

	□ 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: Tax Identification Number, DUNS Number
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 when a individual (sole proprietor) elects to use he/her SSN as the entity's TIN. 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

MODULE I – PRIVACY NEEDS ASSESSMENT

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 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?**	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. Agencies are required to collect TINs [31 U.S.C.7701(c)] and to include the TIN in vouchers submitted for payment [31 U.S.C. 3325(d)].
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)?**	Each individual Vendor has a choice as to which information they provide to the CCR. The decision to place personal versus business information into the CCR is at the sole discretion of the individual person. In order for a sole proprietorship to be awarded a Federal acquisition or financial assistance award and be reimbursed for products and services provided to the Department of Energy, they are required to register with the CCR. This information is used only to perform the required procurement and financial functions.
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 EnCoRe 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.

MODULE II – PII SYSTEMS & PROJECTS

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.
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 information is retrieved via the vendor's TIN and DUNS number.
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-18 Financial Accounting System.
7. SORNs If the information system is being modified, will the SORN(s) require amendment or revision?	N/A

DATA SOURCES

MODULE II – PII SYSTEMS & PROJECTS	
8. What are the sources of information about individuals in the information system or project?	CCR (Input) DOE Registered User (Input/Output) Small Business Contact (SBC) -(Output) Procurement and Assistance Data System (PADS) – (Output) Corporate Planning System (CPS) – (Output) Western Area Power Administration (WAPA) – (Output) Standard Accounting and Reporting System (STARS) – (Output) CCR is the registrant database for the U.S. Federal Government. The CCR collects, stores, and disseminates data in support of agency acquisition missions, including Federal agency contract and assistance awards. Note that the term "assistance awards" includes grants, cooperative agreements, and other forms of Federal assistance. Whether applying for assistance awards, contracts or other business opportunities, all entities are considered "registrants". CCR registration is not required for individuals seeking grants. Note that the CCR itself does not validate the content of the data; parts of the data are validated through various interfaces, i.e., the Internal Revenue Service (IRS) validates TIN information.
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, data elements are described in detail in the CCR User's Guide https://www.bpn.gov/ccr/doc/CCRUsersGuide.pdf
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 solicitation and award and payment activities.

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?	The EnCoRe system will NOT derive new data or meta data.
13. With what other agencies or entities will an individual's information be shared?	N/A
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?	EnCoRe 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
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.	All of the information stored on the EnCoRe production database is an exact replica of the CCR; therefore, EnCoRe data is as accurate as the data in CCR. Vendors are required to be registered with the CCR to obtain a Federal award and to receive payment (FAR4.11) and to submit applications via Grants.gov. Vendors are required to maintain this information as current, and review and update (if necessary) the information provided to the CCR at least annually. The vendors are responsible for the accuracy of the information in the CCR, not the Department of Energy or any other government entity. The CCR validates completeness of initial entry (i.e., no partially filled records will be accepted at the CCR entry point). The EnCoRe DBA ensures all CCR data is replicated completely and accurately. Registrants of CCR and EnCoRe must update or renew their registration at least once per year to maintain an active status. Additionally, EnCoRe regularly retrieves Vendor information daily to ensure that it is up-to-date. Data elements are described in detail in the CCR User's Guide https://www.bpn.gov/ccr/doc/CCRUsersGuide.pdf
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	EnCoRe is only operated and maintained in one site, the DOE AHE.
Retention & Disposition	
22. What are the retention periods of data in the information system?	The EnCoRe database is completely refreshed every quarter with what is contained in CCR. As the original source of the data, CCR is responsible for retention of the data.
23. What are the procedures for disposition of the data at the end of the retention period?	The procedures used by CCR are followed inherently.
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS

24. What controls are in place to protect the data from unauthorized access, modification or use?	EnCoRe is a rights and permissions-based system. Please see the latest system security plan for details regarding controls in place.
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 EnCoRe 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 financial specialists) are registered users who may view the sensitive and/or proprietary information in the database via a User ID and password once they have signed a non-disclosure agreement.
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 EnCoRe 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, STARS, PADS, CPS, and WAPA share EnCoRe data (from extracts) and SBC pulls data from EnCoRe. EnCoRe pulls data from CCR. The EnCoRe System Security Plan describes how the data is shared. **Inbound Connections: CCR, AHE** **Outbound Connections: SBC, CPS, PADS, STARS, WAPA** **Note: AHE has two-way data flow**

MODULE II – PII SYSTEMS & PROJECTS

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?	Interconnection Security Agreements (ISA) outline the responsibilities and expectations associated with system interconnection. ISAs specify security requirements and controls necessary for interconnection and compliance. AHE: MOA SBC: MOA CSP: MOA CCR: MOA/ISA PADS: Operational MOU STARS: MOA
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 agreements that are signed before access is provided.

END OF MODULE II

SIGNATURE PAGE		
	Signature	Date
PIA Approval Signatures	Original Copy Signed and On File with the DOE Privacy Office	7 MAY 2010