Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Energy Contractor Registration System (EnCoRe)
Bureau: Department of Energy
Project Unique ID: EnCoRe
Date: July 15, 2008

A. CONTACT INFORMATION

1. Who is the person completing this document?

Ellen Clayton
Procurement Analyst, MA-623
ellen.clayton@hq.doe.gov, 202-287-1664

2. Who is the system owner?

Ellen Clayton
Procurement Analyst, MA-623
ellen.clayton@hq.doe.gov, 202-287-1664

3. Who is the system manager for this system or application?

Ellen Clayton
Procurement Analyst, MA-623
ellen.clayton@hq.doe.gov, 202-287-1664

4. Who is the IT Security Manager who reviewed this document?

Phil Knopp
Cyber Security Program Manager, Office of Corporate Information Systems
phil.knopp@hq.doe.gov, 301-903-0364

5. Who is the Privacy Act Officer who reviewed this document?

Jerry Hanley
Chief Privacy Officer, U.S. Department of Energy
Jerry.Hanley@hq.doe.gov, 202-287-1563

B. SYSTEM APPLICATION/GENERAL INFORMATION

1. Does this system contain any information about individuals?

a. Is this information identifiable to the individual? [1]

Yes. EnCoRe collects information about individuals in the context of doing business with the Federal government.

b. Is the information about individual members of the public?

Yes. The system contains information about vendors as it relates to conducting business with the Federal government. Unless an award is made, these individuals are considered members of the public.

c. Is the information about DOE or contractor employees?

Yes. EnCoRe contains information about DOE employees who are registered users of the system.

2. What is the purpose of the system/application?

EnCoRe is a database system that duplicates the information in the CCR. The Defense Information Systems Agency (DISA) created and maintains the Central Contractor Registration (CCR) database (www.ccr.gov), as the primary vendor database for the U.S. Federal Government. CCR collects, validates, stores, and disseminates vendor data in support of agency acquisition missions. EnCoRe is a read-only copy of the CCR data, residing within the DOE Office of the CIO's 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 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 a non-disclosure agreement (NDA). Copies of the NDAs are on file in the Office of Procurement and Assistance Management, Information Management Systems Division.

[1] "Identifiable Form" - According to the OMB Memo M-02-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptor).

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:

- EnCoRe includes a function that allows authorized administrators, at the direction of the system owner, to create and manage the accounts that allow only specific DOE officials to view sensitive and/or proprietary information in the database.
- EnCoRe does not allow vendors to register or change their registration information – this function is provided only by DISA's CCR system. In fact, vendors do not have access to EnCoRe and even the EnCoRe system administration function does not allow editing of any vendor information – the vendor 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.

3. What legal authority authorizes the purchase or development of this system/application?

Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. seq., 50 U.S.C. 2401 et. seq.; Freedom of Information Act, 5 U.S.C. 552.

C. DATA IN THE SYSTEM

1. What categories of individuals are covered in the system?

EnCoRe has approximately 15,000 potential users. Of the 15,000 users, only 54 users are contract or finance specialists who are the registered users of EnCoRe. Other end users include all anonymous DOE personnel (no information is collected from employees that access EnCoRe anonymously).

User	Description	Quantity
DOE Employees	All DOE personnel may view the non-sensitive information within EnCoRe. EnCoRe allows anonymous access to the public information and all DOE personnel are registered within the AHE.	15,000
DOE Registered Users	Certain authorized DOE procurement officials (DOE Contracting Officers/Contract Specialists and financial specialists) are registered users who	54

User	Description	Quantity
	may view the sensitive and/or proprietary information in the database. These individuals must register to receive a User ID and password pair.	
Database Administrator	The database administrator ensures the database is running and all data are protected.	1
Application Administrator/ Developer	The application administrator (SA) and application developer (AD) is the same person. The SA/AD has access to all three servers. The developers build and test program code. The developers have access to the development/test server (EnCoRe2) only.	1
Configuration Manager	The configuration manger ensures that EnCoRe is compliant with current DOE configuration management regulations. The configuration manager notifies the system owner of upcoming changes to the system and requests testing of these changes. Upon finalizing the testing, the configuration manager notifies the system administrator of the change and allows the change to move into production.	1

2. What are the sources of information in the system?

a. Is the source of the information from the individual or is it taken from another source?

CCR (Input)

- All updated data within the DISA CCR is extracted daily and pulled by EnCoRe.
- Once a quarter, the entire database is extracted and pulled by EnCoRe.

DOE Registered User (Input/Output)

- The registered user can view sensitive information within EnCoRe, but cannot alter vendor data.
- The registered user can modify their user profile. They can change their telephone number, email address, office number, and password.

CCR is the registrant database for the U.S. Federal Government. The CCR collects, validates for completeness, 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."

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) and the U.S. Small Business Administration (SBA), for example.

Individuals are exempt from CCR registration.

b. What Federal agencies are providing data for use in the system?

DISA, which owns the CCR.

c. What tribal, state, and local agencies are providing data for use in the system?

Tribal, state, and local agencies may apply for procurement and financial assistance awards or respond to procurement and/or financial assistance solicitations and notices, as a potential contractor or recipient, but these organizations do not provide any information other than that expected of other potential contractors or recipients.

d. From what other third party sources will data be collected?

None.

e. What information will be collected from the individual and the public?

No personal information is collected from the public. Information collected from registered DOE employees and contractors includes name, organization, phone number, and e-mail address.

3. Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOE records be verified for accuracy?

The majority of 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 as to the accuracy of the

information in the CCR, not the Department of Energy or any other government entity.

The CCR validates the registrant information for completeness and electronically shares the secure and encrypted data with the Federal Agencies' finance offices to facilitate payments through electronic funds transfer (EFT). Additionally, CCR shares the data with Federal government procurement and electronic business systems.

b. How will data be checked for completeness?

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.

c. Are the data current? What steps or procedures are taken to ensure the data are current and not out-of-date?

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.

d. Are the data elements described in detail and documented?

Yes, data elements are described in detail in the document Business Partner Network Business Rules.

D. ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

All data collected is relevant and necessary for DOE to perform contract solicitation and award and payment activities.

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No

3. Will the new data be placed in the individual's record?
N/A

4. Can the system make determinations about employees/the public that would not be possible without the new data?

N/A

5. **How will the new data be verified for relevance and accuracy?**

   N/A

6. **If the data are being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   N/A

7. **If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?**

   N/A

8. **How will data be retrieved? Does a personal identifier retrieve the data? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

   The information is retrieved from CCR via the vendor's TIN and DUNS Number.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   None. N/A. N/A.

10. **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.

    Individuals are exempt from CCR registration.

E. <u>Maintenance and Administrative Controls</u>

1. **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

   EnCoRe is operated and maintained in only one site, the DOE AHE.

2. **What are the retention periods of data in the 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.

3. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept?**

   The procedures used by CCR are followed inherently.

4. **Is the system using technologies in ways that DOE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

   No

5. **How does the use of this technology affect public/employee privacy?**

   N/A

6. **Will this system provide the capability to identify, locate, and monitor individuals?**

   EnCoRe does not have the capability to identify, monitor, or locate individuals.

7. **What kinds of information are collected as a function of the monitoring of individuals?**

   N/A

8. **What controls will be used to prevent unauthorized monitoring?**

   N/A

9. **Under which PA system of records notice does the system operate?**

   DOE-82 – Grant and Contract Records for Research Projects, Science Education, and Related Activities.

10. **If the system is being modified, will the PA system of records notice require amendment or revision?**

    N/A

F. ACCESS TO DATA

1. **Who will have access to the data in the system?**

   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.

2. **How is access to the data by a user determined?**

All DOE personnel connected to the DOE internal network may view the non-sensitive, public information within EnCoRe via anonymous access.

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.

Access to data is determined by evaluation of personnel job responsibilities and functions. Based on the evaluation, access control lists are documented 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.

3. **Will users have access to all data on the system or will the user's access be restricted?**

All DOE personnel connected to the DOE internal network may view the non-sensitive, public information within EnCoRe via anonymous access.

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.

Access to data is determined by evaluation of personnel job responsibilities and functions. Based on the evaluation, access control lists are documented 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.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access via User ID and password based on user responsibility and job function. These access controls are defined in the EnCoRe System Security Plan. All system team members (Federal and contractor) are required to take the DOE standard cyber security certification course as a prerequisite for the system access. Rules of

Behavior and consequences for violating the rules are executed when the user physically signs the non-disclosure agreement and Rules of Behavior. Administrative controls include non-disclosure agreements and separation of duties so individuals only have access to appropriate information, and use of system audit logs to monitor access and user activity in the system.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were PA contract clauses included in their contracts and other regulatory measures addressed?**

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.

6. **Do other 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.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

In addition to the System Owner, all EnCoRe users are advised of their rights and must be responsible to protect this data.

8. **Will other agencies share data or have access to the data in this system?**

No

9. **How will the data be used by the other agency?**

N/A

10. **Who is responsible for assuring proper use of the data?**

The System Owner, as identified on the following approval page.

PIA Approval Signatures

Original copy signed and on file with the DOE Privacy Office.