

Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Electronic Foreign-Owned, Controlled, or Influence (e-FOCI) System

Bureau: U.S. Department of Energy, Office of Health, Safety, and Security

Project Unique ID: 019-10-01-22-02-3078-00

Date: June 25, 2008

A. CONTACT INFORMATION:

1. Who is the person completing this document? (Name, title, organization, and contact information.)

Name: Jacob P. Johnson
Title: e-FOCI System Administrator
Address: Argonne National Laboratory
 Nuclear Engineering Division
 9700 S. Cass Avenue
 Building 362/B125
 Argonne, IL 60439
Phone: (630) 252-3621
E-mail: jayjohnson@anl.gov

and:

Name: Judith A. G. Chiarelli
Title: Manger, National Security Information Systems Section

Address: Nuclear Engineering Division
 Argonne National Laboratory
 Nuclear Engineering Division
 9700 S. Cass Avenue
 Building 362/B107
 Argonne, IL 60439
Phone: (630) 252-6347
E-mail: chiarelli@anl.gov

2. Who is the system owner? (Name, organization, and contact information.)

Name: Mitchell R. McAllister, HS-72
Title: Office of Security Policy, Security Specialist
Address: DOE Headquarters
Forrestal Building
1000 Independence Avenue
Washington, DC
Phone: (202) 586-1331
E-mail: mitchell.mcallister@hq.doe.gov

3. Who is the System Manager for this system or application? (Name, organization, and contact information.)

Name: Mr. Raymond Holmer
Address: DOE Office of Health, Safety and Security
Germantown, Maryland

E-Mail: Raymond.Holmer@hq.doe.gov

4. Who is the IT Security Manager who reviewed this document? (Name, title, organization, and contact information.)

Vinh Le, Office of Information Management, HS-1.22, 301-903-4648.

5. Who is the Privacy Act Officer who reviewed this document? (Name, title, organization, and contact information.)

Kevin Hagerty, Director, Office of Information Resources, MA-90,
202-586-8037.

B. SYSTEM APPLICATION/GENERAL INFORMATION

1. Does this system contain any information about individuals?

Yes, social security numbers, date and place of birth, and security clearance levels are collected for all individuals listed on Key Management Personnel forms for contracting organizations applying for facility clearances to work at sensitive DOE/NNSA facilities.

a. Is this information identifiable to the individual?

Yes, the individual or their company's FOCI Administrator provides the information and the information is part of the company's management profile, which is the Key Management Personnel form.

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

The information is collected only for personnel on Key Management Personnel forms for contracting organizations applying for facility clearances to work on contracts at sensitive DOE/NNSA facilities.

c. Is the information about DOE or contractor employees?

The information is only about DOE and NNSA contractor employees, not federal personnel.

2. What is the purpose of the above system?

The purpose of the e-FOCI System is to electronically obtain and analyze information to determine whether offerors/bidders or contractors, having access to classified information or special nuclear materials, are owned, controlled, or influenced by foreign person(s) or governments and whether as result of this ownership, control or influence there is a potential for risk to the common defense and national security. Based on the extent of foreign ownership, control, or influence, appropriate measures are put in place by the government and vendor/contractor to mitigate risks.

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

The FOCI process is legislatively mandated by 48 CFR Chapter 9. DOE and NNSA FOCI policy is found in DOE O. 470.1-4. This system is the DOE/NNSA tool used for implementation of this policy in compliance with the FOCI legislative mandate.

The e-FOCI system has been funded/developed/authorized by the Department of Energy, Office of Health, Safety, and Security (HSS 1.22) and the NNSA Office of Defense Nuclear Security (NA-72).

C. DATA IN THE SYSTEM:

1. What categories of individuals are in the system?

Key Management Personnel for contracting organizations doing sensitive work at DOE/NNSA facilities.

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? If not directly from the individual, then what other source?**

The FOCI Administrator for the contracting entity inputs the data, this can either be the individual themselves or their secretary/administrative assistant, or the Facility Security Officer.

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

None

- c. What Tribal, State or local agencies are providing data for use in the system?**

None

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

None

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

Social security numbers, date and place of birth, and security clearance levels are collected for all personnel on Key Management Personnel forms for contracting organizations applying for facility clearances to work on contracts at sensitive DOE/NNSA facilities.

3. Accuracy, Timeliness and Reliability:

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

DOE/NNSA FOCI Managers review the information for accuracy. The FOCI Administrator for the contracting organization reviews the submission before sending it and signs and certifies that the information is accurate.

- b. How will data be checked for completeness?**

The e-FOCI System will not allow the submission of incomplete FOCI packages so there is an electronic check of the data in the forms before they are submitted. In addition, the company's FOCI Administrator checks the information before submission. The DOE/NNSA FOCI manager

checks the information when it is received and if more information is needed or corrections need to be made they can electronically return the package to the submitter to have the additional information added.

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

The FOCI process requires annual certifications of contractor data, so contractors have to review and update their data annually. In addition, FOCI policy requires that any significant changes to the data be reported to DOE/NNSA and submitted within three days of the significant change occurring.

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

Yes.

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?**

Yes, the Key Management Personnel data is required to render a FOCI Determination. All of the other forms submitted via the e-FOCI System in an electronic "FOCI package" are necessary for rendering FOCI Determinations which are required for specific types of facility clearances.

- 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 employee/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 is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Data is stored in a centralized, encrypted database, with authentication and other security controls. Secure coding techniques are in place to prevent unauthorized access to the data. See the System Security Plan for more details on the security controls in place for the system.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

Yes, see above as well as the System Security Plan for details on the security controls in place to protect against the unauthorized release of data. A System Risk Assessment has been completed as well. The e-FOCI System Security Plan received its C&A in 2004 and the C&A was renewed in 2007.

8) How will the data be retrieved? Does a personal identifier retrieve the data?

Data is retrieved through a web interface by authorized users only. Contractors submitting FOCI information can only retrieve their own submitted data. DOE/NNSA FOCI Managers retrieve the data through company unique identifiers in the system, not individual identifiers.

9) What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Reports are not produced on individuals.

10) What opportunities do individuals have to decline to provide information (ie where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.

All users must agree to the security and privacy policies and accept an online Rules of Behavior document before they are permitted to upload their information. Users must submit the data required for a FOCI Determination in order to have their organization evaluated for a facility clearance to perform contract work at sensitive DOE and NNSA facilities. If they decline to provide information they cannot receive a facility clearance for the contract work.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

The web interface used by Contractor organizations for data submissions standardizes the process. The data submitted across DOE and NNSA is submitted via the same set of forms using the same web interface. The system database is centralized at one site only. The Rules of Behavior document has to be read, agreed to and signed by all Users of the System.

- 2. What are the retention periods of data in this system?**

Uploaded data is retained indefinitely within the system.

- 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? Where are the procedures documented?**

Hard drives and expired backup tapes must be destroyed according to Argonne National Laboratory policy. Procedures are documented in the System Security Plan.

- 4. Is the system using technologies in ways that the 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? If yes, explain.**

No.

- 7. What kinds of information is 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 Privacy Act systems of records notice does the system operate? Provide number and name.**

The System operates under OMB 1910-1800. The System UPI is 019-10-0122-02-3078-00.

- 10. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain**

Once new upgrades are completed the System will be evaluated to determine if the Privacy Act system of records needs amendment or revision. At this time it is not necessary.

F. ACCESS TO DATA:

- 1. Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)**

Contractors who upload their company data can only access the data they have uploaded and submitted. FOCI Managers authorized to use the system can access but not modify the data of the contractors under the management authority of their own area only. Authorized e-FOCI system administrators who are part of the project team can access the data when necessary. All of these system administrators hold security clearances.

- 2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

There are access criteria, procedures, controls, and responsibilities documented in the System Security Plan. Controls in the e-FOCI System only allow contractors to access the data they have submitted and federal DOE/NNSA FOCI Managers can only access the data in progress that were submitted to their virtual office. Access is controlled by specific user type.

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

Access is restricted based on user type. Contractors using the system can only access the data their specific organization has uploaded. Federal DOE/NNSA FOCI Managers only have access to the data for contractors under the management authority of their own office.

- 4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

All FOCI Managers must sign a Rules of Behavior Form before access to the system is granted, and they have no ability to change any of the information that

was submitted by contractors. All Contractors submitting data must also agree to the Rules of Behavior before access to the system is granted. Access is limited to different users based on User type so browsing is not allowed across User types by system design. A User Guide is issued as part of the training program that outlines the different functionality for the different types of Users.

- 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 Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Argonne National Laboratory designed, developed and now operates the e-FOCI System. ANL is operated by UChicago Argonne, LLC who has met all the DOE Privacy Act contract clauses under the M&O agreement between DOE and UChicago Argonne, LLC.

- 6. Do other systems share data or have access to the data in the system? If yes, explain.**

No.

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

The designated Cyber Security Manager for the system is responsible for ensuring the confidentiality and integrity of the system. Also, the system owner and system manager are responsible for overseeing the proper management and operation of the system.

- 8. Will other agencies share data or have access to the data in this system (Federal, State, Local, and Other (e.g., Tribal))?**

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?**

N/A

The following officials have approved this document:

1. System Owner

Mitchell R. McAllister (Signature) 08/11/08 (Date)
Name: Mitchell R. McAllister
Title: Security Specialist, Office of Security Policy

2. System Manager

Raymond Holmer (Signature) 7/28/08 (Date)
Name: Raymond Holmer
Title: Director, Office of Information Management

3. Privacy Act Officer

Jerry Hanley (Signature) 8/24/08 (Date)
Name: Kevin T. Hagerty ~~Jerry Hanley~~
Title: Director, Office of Information Resources
CHIEF PRIVACY OFFICER

4. Senior Official for Privacy Policy NON-public

____ (Signature) ____ (Date)
Name: Ingrid Kolb
Title: Director, Office of Management