Affects Members Of the Public? X

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	April 19, 2022
Departmental Element & Site	U.S. Department of Energy, Office of Environment, Health, Safety, and Security (AU) Argonne National Laboratory (ANL), National Security Information Systems Section (NSIS), Strategic Security Sciences Division
Name of Information System or IT Project	Foreign Ownership, Control or Influence Electronic Submission & Processing System (e-FOCI)
Exhibit Project UID	UPI: 019-10-01-22-02-3078-00-403-134
New PIA ☐ **Update** x	e-FOCI PIA update in support of three (3) year re-authorization

	Name, Title	Contact Information Phone, Email
System Owner	Michelle Ho, EHSS-72 Office of Information Management	(301) 903-0521 Michelle.Ho@hq.doe.gov
Local Privacy Act Officer	Ray Holmer, EHSS-72 Office of Information Management	(301) 903-7325 Raymond.Holmer@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Joseph F. Petersen Systems, Network, & Cyber Security III, CISSP e-FOCI ISSO Strategic Security Sciences Division Argonne National Laboratory	(630) 252- 3279 jfpetersen@anl.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Douglas E. Johnson Group Leader, NSIS Strategic Security Sciences Division Argonne National Laboratory	(630) 252-6324 djohnson@anl.gov
Purpose of Information System or IT Project	The e-FOCI System electronically obtains and analyzes information to determine whether offerors/bidders or contractors gaining 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. The federal review process may include direct communication with submitting organizations as well as research and verification performed on the Internet and systems external to e-FOCI. 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. DOE and National Nuclear Security Administration (NNSA) FOCI policy is found in DOE O 470.4b Chg. 2, SAFEGUARDS AND SECURITY PROGRAM. The e-FOCI Submission Site application allows public access to the web site. Users must first register and provide company and personal information. The application can be accessed only after the users are registered successfully on the e-FOCI system and are approved. The application is designed to allow a user access to the information stored on the system belonging exclusively to the registered user's organization. Registered users are not allowed to view, remove, add, and change any information beyond the scope of the user's permissions. For example, a registered user of Organization A is not allowed to view Organization B's information. Each organization's data is stored in a database and can be retrieved after the user has the proper authentications. The user cannot access other organizations' data. Public e-FOCI content is limited to the splash/log-in and FAQ pages. All content is only updated as part of a system release by authorized administrators. A monthly review by the system security manager validates that the publicly accessible pages have not been inappropriately modified. The public available content is also reviewed and tested during any production system update/deployment. A monthly Jira (Agile software tool) database item is used to track that the monthly review has taken place, the results of which are provided to DOE upon request.	
Type of Information Collected or Maintained by the System:	☒ SSN ☐ Medical & Health Information ☐ Financial Information ☒ Clearance Information ☐ Biometric Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Mother's Maiden Name ☒ Date of Birth, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☐ Other – Please Specify
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
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?	☐ Federal Employees ☒ Contractor Employees

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?**	The Foreign Ownership Control or Influence (FOCI) process is legislatively mandated by 48 CFR Chapter 9. This system is the DOE tool used for implementation of this policy in compliance with the FOCI legislative mandate.
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)?**	Providing this information is voluntary but is a condition of doing business with the government; individuals declining to provide this information. An individual my decline to provide required information but would thereafter not be authorized to perform contract work at sensitive DOE and NNSA facilities. All users must agree to the security and privacy policies and accept an online Rules of Behavior document annually before they are permitted to provide their information.
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?**	e-FOCI is managed and operated by Argonne National Laboratory (ANL), which also designed and developed the system. e-FOCI was funded by the DOE Office of Environment, Health, Safety and Security through a Work Authorization to UChicago Argonne, LLC, who operates Argonne National Laboratory on behalf of DOE through a Management and Operating (M&O) prime contract with the DOE. All activities related to the e-FOCI system are operated within the provisions of the prime contract, which incorporates DOE O 206.1 Chg.1 Department of Energy Privacy Program (Nov. 1, 2018). 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 the 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?**	DOE has assessed e-FOCI as a moderate-risk system according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. The unauthorized disclosure of information is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The e-FOCI system only collects information required to render a FOCI determination, which includes limited proprietary financial and supplementary business information, and social security numbers (SSNs), birth and clearance information of key management personnel involved with a contract. No additional personal information is collected by the system except that which is required to render the FOCI determination as mentioned above. If personally identifiable information (PII) maintained in this system were disclosed to unauthorized parties, the sensitivity thereof could compromise the trust between employees and the employer and cause embarrassment or harm to the employee/contractor whose information was exposed. The breach of SSNs would result in the most serious potential harm to individuals posed by e-FOCI. In addition, information respecting foreign influence determinations may also adversely impact the privacy of individuals resulting in reputational harm via association with the organization being assessed. Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of e-FOCI being compromised. All data collected, processed, and stored by the system are encrypted at rest and in transit, and all backup tapes are also encrypted using FIPS 140-2 encryption. All system administrative access requires 2-factor authentication and is only accessible by authorized system and cyber security administrators. Contractors using the system are limited to uploading and viewing their own company's information. Information reviewed by FOCI managers in the e-FOCI system is not retrievable by individual identifiers, only by organizational identifiers.

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.**	DOE/NNSA FOCI Managers can retrieve company data, not PII, through unique company identifiers, not personal identifiers. Data is retrieved through a web interface by authorized users only. Contractors submitting FOCI information can only retrieve their own company-submitted data. As of February 2022, 3.1% of all company records belong to sole proprietorships whose company name includes the first and last name of an individual business owner. However, search results display only company name and facility code; search results themselves contain no PII, and PII is therefore not retrieved by personal identifier.
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*.**	N/A
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?	The sources of information are corporate documents and personnel data inputted into FOCI forms and uploaded into the system. Each contracting company designates one or more individuals to input data on their behalf. The corporate documents required by the system are determined by the business structure of the organization. Examples of such document types include Articles or Organization/Incorporation, Charters, Bylaws, Meeting Minutes, and Partnership Agreements. Federal FOCI personnel refer to these documents and additional forms submitted by the organization, such as the Key Management Personnel, Tier Parents, and the Certificate Pertaining to Foreign Interests, to review, assess and mitigate FOCI.

MODULE II – PII SYSTEMS & PROJECTS

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, the database schema describes elements and shows data relationships.
DATA USE	
11. How will the PII be used?	The Key Management Personnel (KMP) data is reviewed by federal FOCI personnel to evaluate the extent of foreign ownership, control, or influence on corporate boards, management teams, and for individuals of influence who will have control over contracts. Personnel security clearances are also noted on KMP forms and this data is used to verify and assess clearance levels for certain types of contract work.
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?**	No metadata is derived from the system.
13. With what other agencies or entities will an individual's information be shared?	No metadata is shared with other agencies.
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports are not produced on individuals by the DOE and NNSA using e-FOCI.
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A
MONITORING	

MODULE II – PII SYSTEMS & PROJECTS

17. Will this information system provide the capability to identify, locate, and monitor individuals?	No
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	
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.	Potential and existing contractors use the e-FOCI system to enter data and upload supporting documentation. The system prevents the submission of incomplete FOCI packages, performing a completeness check of each package before it can be sent to DOE/NNSA FOCI personnel. DOE/NNSA FOCI personnel then review and compare the contractor's electronically submitted data with the supporting documentation for accuracy, relevance, and completeness. Discrepancies are typically resolved through direct communication with the contractor. If data modifications are needed, the package is electronically returned to the contractor to make the requisite changes. Additionally, FOCI policy requires that significant changes to the data be submitted to DOE/NNSA.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The production e-FOCI database is centralized at one site only. This database is mirrored to a second location for contingency purposes, and daily database backups are written to a third location for a disaster recovery purposes. There is only one database that is live at any given time, which ensures data consistency across the production, contingency and disaster recovery environments.
Records Management	
22. Identify the record(s).	Foreign Ownership, Control, or Influence (FOCI) Files.

MODULE II – PII SYSTEMS & PROJECTS

23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	a. DAA-0434-2015-0013(0001) Unsuccessful bidder files containing their representations as to their ownership and any foreign control or influence, and other information pertaining to foreign ownership, control or influence and whether it may pose an undue risk to national security that has been provided by the unsuccessful bidder or otherwise gathered. Cut off at the end of the fiscal year. Destroy 2 years after cutoff. b. (DAA-0434-2015-0013(0002) Successful bidder (contractor) files containing original and subsequent representations as to their ownership and any foreign control or influence, and other information pertaining to foreign ownership, control or influence and whether it may pose an undue risk to national security that has been provided by the contractor or otherwise gathered. Files relating to contract eligibility determinations when foreign ownership, control or influence issues are present. Cut off 5 years after determination date. Destroy 5 years after cutoff. ++++++++++++++++ **A proposed change to the schedule part b is**: Cut off at end of the fiscal year 5 years after determination date. *Destroy 15 years after cutoff.*
24. Records Contact	Mitchell McAllister |mitchell.mcallister@hq.doe.gov 202-586-133 Baldev Dhillon baldev.dhillon@hq.doe.gov 301-903-0990

ACCESS, SAFEGUARDS & SECURITY

25. What controls are in place to protect the data from unauthorized access, modification or use?	The e-FOCI ISSO and supporting team at Argonne has implemented and tested all baseline security controls appropriate to its **FIPS-199 Moderate** categorization in accordance with the DOE Energy Information Technology Services PCSP, DOE Directives and NIST SP 800-53 Revision 4. The e-FOCI System was last authorized in March 2019 and found to have mitigated risk to an acceptable level. • All FOCI Managers must sign a Rules of Behavior Form before access to the system is granted and annually afterwards, and they have no ability to change any of the information submitted by contractors. • Access controls restrict all Submission Site users to read/write access to their own company data only. • Contractors using the Submission Site to submit data must also agree to the Rules of Behavior before access to the system is granted and annually afterwards. • While federal personnel in DOE Headquarters and DOE/NNSA operations offices have access to all contractors information within the e-FOCI Processing Site, users in subordinate M&O offices are limited to viewing sensitive data for only those contractors submitting directly to their office. • All logins to the system are audited and reviewed for suspicious behavior, with notifications sent to all administrators of any login failures, and auditing is enabled on the database itself so that all database transactions are recorded and logged as to what user took what action and when. • All PII access events are logged in the database. • 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 made available as part of the training program that outlines the different functionality for the different types of Users. The e-FOCI system complies with the requirements of the hosting facility (DOE and ANL) which mandate periodic scheduled and unscheduled security scans. These scans consist of both offsite and onsite (from behind the facility's firewalls) penetration testing of systems and defense. Independent scans are performed by DOE and ANL security teams. Any vulnerability identified through either process is tracked to correction in tenable.sc enterprise tool, the ANL site's central vulnerability-tracking database and reported to the appropriate Cyber Security Program Representative (CSPO). Security scans and penetration testing are performed with tenable.sc continuously by ANL computer support staff and project technical staff. Scanning is performed continuously on all systems with authorized conduits (open ports) to the Internet. Monthly Nessus admin-level scans are performed on all production e-FOCI system components. Scans are

MODULE II – PII SYSTEMS & PROJECTS

	also performed by project or divisional personnel whenever a significant change to system configuration is judged to have occurred. Critical and High vulnerabilities discovered are remediated within 30 days. Web applications developed for the e-FOCI system undergo web application security testing as part of the software release cycle and normal software QA testing process using Burp Suite tools. Password checkers that enforce DOE and NIST password policy are integrated into the e-FOCI web application. Password checking policy and procedures and their execution are the responsibility of the support staff.
26. Who will have access to PII data?	Authorized users for each contracting company can access data that has been entered and uploaded for their organizations. FOCI Managers authorized to use the system can access but not modify the data submitted by the contractors under the management authority of their own area only. Authorized e-FOCI system administrators based at ANL who are part of the project team can access the data when necessary.
27. How is access to PII data determined?	There are access criteria, procedures, controls, and responsibilities documented in the System Security Plan. • Access is determined based on user roles. • Contractors can only access data through the e-FOCI Submission Site and can only view data entered and uploaded into the system for their organization. • M&O contractor data access on the e-FOCI Processing Site is limited to packages submitted specifically to their offices and the system does not allow M&O access to rendered determinations. • Federal personnel in DOE Headquarters and DOE and NNSA operations offices may access all data within the e-FOCI Processing Site.

MODULE II – PII SYSTEMS & PROJECTS

28. Do other information systems share data or have access to the data in the system? If yes, explain.	There is no interconnectivity with other information systems. Any information contained within e-FOCI that is shared with other systems is done out of band and at the discretion of federal FOCI personnel.
29. 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 e-FOCI system does not connect to any other information systems.
30. Who is responsible for ensuring the authorized use of personal information?	The DOE FOCI Program Manager and the NNSA FOCI Program Manager are responsible for ensuring the authorized use of PII in the e-FOCI System.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	**Michelle Ho** **(Print Name)** Michelle Huyen Ho Digitally signed by Michelle Huyen Ho Date: 2022.05.05 10:44:06 -04'00' **(Signature)**	
Local Privacy Act Officer	**Raymond Holmer** **(Print Name)** RAYMOND HOLMER Digitally signed by RAYMOND HOLMER Date: 2022.05.05 13:49:09 -04'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**Ken Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2022.05.04 15:13:36 -04'00' **(Signature)**	