PRIVACY IMPACT ASSESSMENT: Office of Fossil Energy
Northeast Home Heating Oil Reserve System
May 3, 2010

MA-1024

Affects Members Of the Public? X

Department of Energy
Privacy Impact Assessment (PIA)

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

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	May 3, 2010
Departmental Element & Site	Office of Fossil Energy Headquarters
Name of Information System or IT Project	Northeast Home Heating Oil Reserve System (Heating Oil)
Exhibit Project UID	**019-20-01-16-02-3624-00**
New PIA X **Update**	New Privacy Impact Assessment

	Name, Title	Contact Information Phone, Email
System Owner	Nancy Marland Northeast Home Heating Oil Reserve System Owner	202-586-4691 Nancy.marland@hq.doe.gov
Local Privacy Act Officer	Edward Kilroy Local FE Privacy Act Officer	301-903-2051 edward.kilroy@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM,	Elizabeth Grimm Fossil Energy-Information System Security	(301) 903-2760 Elizabeth.grimm@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

CSSM, ISSO, etc.)	Officer	
Person Completing this Document	Rowena Clemente Sr. Consultant, Booz Allen Hamilton	(703) 377-5327 clemente_rowena@bah.com
Purpose of Information System or IT Project	**The primary purpose of the Northeast Home Heating Oil Reserve System is to function as an online auction system for the home heating oil reserves in the US Northeast.** Should the President of the United States make the determination that the Heating Oil Reserve should be utilized; the Northeast Home Heating Oil Reserve System will be activated. The auction site, https://www.fossil.energy.gov/heatingoil/home.asp is deployed on the Department of Energy Network (DOENET), with servers in Germantown, and an offsite alternate processing site.	
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 ☐ Mother's Maiden Name ☐ DoB, 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?		No The application developers have

MODULE I – PRIVACY NEEDS ASSESSMENT

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.*	intimate knowledge of the data contained in the system. No scanning tools have been used.
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?	No ☐ 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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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 Energy Act of 2000 (Public Law 106-469), enacted on November 9, 2000, amended the Energy Policy and Conservation Act (Public Law 94-163) and authorized the Secretary of Energy "to establish, maintain, and operate in the Northeast a Northeast Home Heating Oil Reserve." The responsible organization for the Northeast Home Heating Oil Reserve System is the Department of Energy Office of the Under Secretary of Energy Office of Fossil Energy: **Office of Fossil Energy** United States Department of Energy Germantown, MD 20874
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)?**	Input of information by the individual's name is voluntary. Although the name field is marked as mandatory, users/bidders do not have to provide a full name, nor do they have to provide a valid name. Additionally, a privacy statement is included on the website, stating "We collect no personal information about you when you visit home.doe.gov unless you choose to provide this information to us." The privacy statement also states that "This information is NOT shared with anyone beyond the support staff to this home page, except when required by Law Enforcement investigation, and is used only as a source of anonymous statistical 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?**	Yes. Contractors are involved with the development and system maintenance of the application. Cyborg is the third party application developer for Heating Oil. Additionally, other FE HQ contractors are involved with the system administration of the Heating Oil servers. Privacy Act clauses are currently being incorporated in the contracts where contractors are involved with the development and maintenance of Heating Oil.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The information system's impact on the privacy of the users/bidders is low. The only PII collected by Heating Oil is the names of the users who register to use the system. If the system is compromised, information would be limited to a list of names. Names submitted by the users/bidders are only used for correspondence purposes. Additionally, the system is only activated if the emergency use of the Strategic Petroleum Reserve is ordered by the President of the United States.
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 Heating Oil Sales System is not a system of records. It is a system to rank bids and the bids are retrieved by a computer-generated bidder number. Any user profile information, e.g., company name or phone number, is entered at the discretion of the registrant and is not checked or used by the system. The program does not retrieve records about individuals by a 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*.**	NO
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 the PII are from the users/bidders themselves. When they register to use the system, they are prompted to provide a name, email, and company information.

MODULE II – PII SYSTEMS & PROJECTS	
9. Will the information system derive new or meta data about an individual from the information collected?	There is no new or derived meta data about an individual from the information collected by the system.
10. Are the data elements described in detail and documented?	The data elements are documented in system documentation and detail the specific data types and database schemes.
DATA USE	
11. How will the PII be used?	Names submitted by the users/bidders are only used for correspondence purposes. For example, if letters are sent to the bidders, the registered name may be included in the letter.
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?**	N/A
13. With what other agencies or entities will an individual's information be shared?	Heating Oil does not directly share information with other agencies or entities. The Department of Treasury, which coordinates with FE to collect the bid guarantees during actual bidding, does not have any type of access to the information contained in Heating Oil Application, nor does it have an interconnection. It is important to note that Heating Oil resides on the DOE network (DOENET). DOENET is a shared resource managed by the DOE Office of the Chief Information Officer (OCIO) that provides a central communication network for DOE program offices. FE HQ maintains its own separate Firewall to limit access to the servers.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Heating Oil does not produce any types of reports that contain the individual user/bidder's names.
15. What will be the use of these reports?	N/A

MODULE II – PII SYSTEMS & PROJECTS	
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?	Yes.
18. What kinds of information are collected as a function of the monitoring of individuals?	Information collected as a function of monitoring individuals is limited to audit log information. When users/bidders are logged into the system, the Heating Oil administrators have the capability to monitor that the users/bidders are logged on, the originating IP address, and their actions.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. Only individuals within FE who have significant roles, duties and responsibilities for Heating Oil are able to view the information stored by the system. Access to the data and related audit log information is limited to system administrators, system developers and the System Owner. Additionally information related to access controls (AC family of controls) are detailed in the Office of Fossil Energy System Security Plan v2.6.
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.	There are no verification processes in place for accuracy, relevance and completeness of the individual's name. There is no other personally identifiable information collected by the system other than the names of the users/bidders submitted by the users/bidders themselves.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	All Heating Oil production servers are located in Germantown, MD. There are also replicated processing servers located at the Verio data center in Northern California. This is a redundant processing server, and is only used as contingency system in case the actual production servers fail during bidding.
Retention & Disposition	

MODULE II – PII SYSTEMS & PROJECTS	
22. What are the retention periods of data in the information system?	There are no defined retention requirements for Heating Oil data. Periodically, the Heating Oil System developers will clear out all of the accounts and have all the users re-register.
23. What are the procedures for disposition of the data at the end of the retention period?	If the hardware, including the hard drive, needs replacement or needs to be disposed and contains any user/bidder's account information, that hardware will be sanitized using DOE services in the Germantown, MD site.
ACCESS, SAFEGUARDS & SECURITY	
24. What controls are in place to protect the data from unauthorized access, modification or use?	Access controls are in place to protect the data from unauthorized access, modification, and use. Only individuals within the Office of Fossil Energy who have significant roles, duties and responsibilities for Heating Oil are granted access to the system and are able to view the information located in the system. These individuals are involved in the routine operation, maintenance, and management of the system. Additionally, the Heating Oil servers are located behind the OCIO controlled firewalls and further protected by an FE-owned firewall. For additional access controls, please refer to the FE Headquarter (HQ) System Security Plan v2.6.
25. Who will have access to PII data?	Access to the PII data is limited to the System Owner, Application Developers, and System Administrators.
26. How is access to PII data determined?	The System Owner must approve all system level access requests.
27. Do other information systems share data or have access to the data in the system? If yes, explain.	No. However, it is important to note that Heating Oil resides on the DOE network (DOENET). DOENET is a shared resource managed by the DOE Office of the Chief Information Officer (OCIO) that provides a central communication network for DOE program offices. FE HQ maintains its own separate firewall to limit access to the servers.
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?	N/A

MODULE II – PII SYSTEMS & PROJECTS

29. Who is responsible for ensuring the authorized use of personal information?	The Northeast Home Heating Oil Reserve System System/Information Owner is the individual responsible for ensuring that the personal information contained in the system is appropriately used solely for mission and business purposes.

END OF MODULE II

SIGNATURE PAGE		
	Signature	Date
PIA Approval Signatures	Original Copy Signed and On File with the DOE Privacy Office	08/24/2010