Template - January 30, 2009, Version 2

| 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

Please complete electronically: no hand-written submissions will be accepted.

Module I – Privacy Needs Assessment

Date	February 6, 2009
Departmental Element & Site	NNSA Shaw AREVA MOX Services Savannah River Site, Aiken SC
Name of Information System or IT Project	MOX Services Unclassified Information System
Exhibit Project UID	DE-AC02-99CH10888

	Name, Title	Contact Information Phone, Email
System Owner	Dave Stinson, President and Chief Executive Officer, Shaw AREVA MOX Services, LLC	(803) 819-22700 Dstinson@moxproject.com

Module I – Privacy Needs Assessment

Privacy Act Officer	Carolyn Becknell, Privacy Act Officer NNSA Service Center Albuquerque PO Box 5400 Albuquerque, NM 87185	(505) 845-4869 cbecknell@doeal.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Jeff Harris, Cyber Security Site Manager MOX Services	(803) 819-2460 Jvharris@moxproject.com
Person Completing this Document	Jeff Harris, Cyber Security Site Manager MOX Services Susan Sanders, Security/Facility Manager MOX Services	(803) 819-2460 Jvharris@moxproject.com (803) 819-2700 smsanders@moxproject.com
Purpose of Information System or IT Project	The Unclassified MOX Services Information System is used to house information that supports the construction, operation and decommissioning of the Mixed Oxide Fuel Fabrication Facility (MFFF). This facility will make fuel assemblies from weapon-grade plutonium oxide and depleted uranium oxide, which will be transferred to commercial nuclear power reactors to generate electricity. When the MOX fuel has been irradiated, the plutonium will not be readily usable for nuclear weapons.	

Module I – Privacy Needs Assessment

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 /Legal Information
	☒ Name, Phone, Address
	☒ Other - ☒ Gender / ☒ Emergency Contact Information / ☒ Motor Vehicle Records
	☒ Citizenship

Has there been any attempt to verify Information about an Individual in Identifiable Form does not exist on the system? *OMB 03-22 defines Information in identifiable form* as 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 descriptors).	Yes
If "Yes," what method was used to verify the system did not contain Information In Identifiable Form? (e.g. system scan)	Nessus content scan for SS#'s was performed on desktops one time as part of an information assessment.

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

Module I – Privacy Needs Assessment

3. Is the information about individual members of the public?	YES
4. Is the information about DOE or contractor employees?	YES

If the answer to the **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.

For information systems that collect, maintain or disseminate information in identifiable form from or about members of the public, please complete Modules II and III. 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. This template may not be modified. 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 (and III if necessary).

Module II – System Information for All Systems

1.	What categories of individuals are collected or maintained by the information system?	[x] Federal Employees
		[x] Contractor Employees
		[x] Members of the Public Individuals in non-employee or contractor context. This includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE.
		[ ] Other, Please Specify

Module II – System Information for All Systems

2. What is the source(s) of information about individuals in the information system?	Individual provided, MOX HR and Procurement Department or visitor host/escort.
3. With what other agencies or entities will an individual's information be shared? How will the information be used?	DOE – security background checks SRNS – badging AREVA and Shaw – HR purposes
4. Is the use of the information in identifiable form both relevant and necessary for the mission of the organization and DOE?	Yes
5. Are the data elements described in detail and documented?	Yes, data elements are described in the PAR (Personnel Action Request)

REPORTS

6. What kinds of reports are produced about individuals or that contain an individual's data?	Authorized users can generate a variety of reports that include human resources, payroll, benefits and safety information etc.
7. What will be the use of these reports?	Manage payroll, benefits and human resources information.
8. Who will have access to these reports?	Access is limited to those whose official duties require access to the records.

MAINTENANCE

9. If the information system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	The system is maintained and operated by the MOX Services IT Department and is only operated by MOX Services.
10. What are the retention periods of data in the information system?	The data becomes part of the official project records repository with an indefinite retention period.

Module II – System Information for All Systems

11. What are the procedures for disposition of the data at the end of the retention period?	Disposition of the data is addressed in the Information System Security Plan with regards to sanitizing media which contained the information. Online access to the information is controlled by the IT14-2, Account Management. Backup media containing the information is protected as documented in IT14-3, Storage of Backup Media.
12. How does the use of this information system affect privacy? Consider also the use of emerging technologies and how those technologies may impact privacy.	The information system provides a defense-in-depth methodology to secure and protect the privacy of public and employee information.

ACCESS

13. What controls are in place to protect the data from unauthorized access, modification or use?	MOX implements access control requirements at the network, host, and application level. Network data flow is controlled through access control lists (ACL). Other security controls are implemented as required by NAP 14.2C.
14. If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?	N/A
15. Who will have access to this information system and its data (all data)? Will other agencies share data or have access to the data in this system? How will the data be used by the other agency?	The system is self-contained and is not shared with other information systems. SRNS the prime SRS contractor will be provided system information as needed for the site badging purposes. However, they will NOT have access to the system.
16. Who will have access to information in identifiable form or and PII?	HR, Personnel Security, Employee Concerns Program, Accounting, Employee and Visitor Access Control, ES&H
17. How is access to the data determined?	The system owner determines who has access. Access to data is on a need-to-know basis in accordance with the job roles and responsibilities of individuals.

Module II – System Information for All Systems

18. 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?	No, contractors are involved with design, development, operation, or maintenance of the system.
19. Do other information systems share data or have access to the data in the system? If yes, explain.	No, the system is self-contained and is not shared with other information systems.
20. For connecting information systems, is there an ISA other agreement between System Owners to ensure the privacy of individuals is protected.	The MOX Unclassified Information System is an independent system. There are no ISA or MOU agreements with other system or data owners.
21. Who is responsible for assuring proper use of the information system's information in identifiable form?	Authorized end-users, Chief Technology Officer – Robert Jones, CSSM – Jeff Harris, and FSO – Susan Sanders

Module III – Systems with Information About Members of the Public

1. What legal authority authorizes the purchase, development or maintenance of this information system?	Department of Energy Organization Act of 1977 (42 U.S.C. 7101 *et seq.*); Export Administrative Act of 1979 (50 U.S.C. 2401 *et seq.*); The Energy Employees Occupational Illness Compensation Program Act o 2000, Pub. L. 106-398; Atomic Energy Act of 1954 (42 U.S.C. 2051a), section 31a; Economy Act of 1932, as amended (31 U.S.C. 1535); Memorandum of Understanding between the Department of Energy and the Department of Health and Human Services, 56 FR 9701, March 7, 1991; 42 U.S. C 2201(p); 42 U.S.C.7254; 42 U.S.C. 5801(a); the General Accounting Office (GAO) Policy and Procedures Manual; Statement of Federal Financial Accounting Standards published by the GAO and the Office of Management and Budget; 50 U.S.C. 301; Debt Collection Improvement Act of 1996; 31 U.S.C. 3512 U.S.C. 5701-09; Federal Property Management Regulations 101-107; Treasury Financial Manual; Executive Order 9397; Department of Energy Organization Act, including authorities incorporated by reference in Title III of the Department of Energy Organization Act; Federal Trot Claims Act, 28 U.S.C. 2671-2680; Military Personnel and Civilian Employees Claims Act, 31 U.S.C. 240-243; Executive Order 12009; 10 CFR part 710, subparts A and B; Executive Orders 10450 and 12968; CFR part 732; DOE O 472.1B; Personnel Security Activities, of 3-24-97; Personnel Security Program Manual DOE M 472-1.1, of 5-22-98; and Director of Central Intelligence Directive 1/14 of 1-22-91; 42 U.S.C. 7151 and 7297; 42 U.S.C. 2201(c), 2201(i)(3), 5813 and 5817; 41 U.S.C. 2165; 42 U.S.C. 5813-5815; 3 CFR 1949-1953 as amended; Executive Order 10865; 3 CFR 195901963, as amended; and Personnel Assurance Program [10 CFR 712].
2. Has a Privacy Act System of Records Notice been published in the Federal Register? If "Yes," provide name of SORN and location in the Federal Register.	DOE-3 Employee Concerns Program DOE-5 Personnel Records of Former Contractor Employees DOE-10 Energy Employees Occupational Illness Compensation Program Act Files DOE-18 Financial Accounting System DOE-33 Personnel Medical Records DOE-38 Occupational and Industrial Accident Records DOE-41 Legal Files (Claims, Litigation, Criminal Violations, Patents, and Others) DOE-43 Personnel Security Files DOE-50 Human Reliability Program Records DOE-51 Employee and Visitor Access Control DOE-52 Access Control Records of Internal Visits, Assignments, and Employment at DOE facilities and Contractor Sites DOE-88 Epidemiologic and Other Health Studies, Surveys, and Surveillances

Module III – Systems with Information About Members of the Public

3. If the information system is being modified, will the SORN require amendment or revision?	No, all system modification will be reviewed by the Cyber Security Change Control Board to ensure all security controls are preserved throughout the modification and there is no change to the systems overall security posture.
4. How will data collected from sources other than DOE records be verified for accuracy, relevance and completeness?	The system collects data directly from the individual, company representative, or family members to whom it pertains. Therefore, the data collected is determined it is accurate at the time it was provided. The data in the system is manually and electronically reviewed for completeness. Therefore, the data collected is determined it is complete at the time it was provided.

Module III – Systems with Information About Members of the Public

5. Are records in the system about individuals current? What steps or procedures are taken to ensure the data is current?	The system collects data directly from the individual, company representative, or family members to whom it pertains. Therefore, the data collected is determined it is accurate at the time it was provided.
6. Will the information system derive new or meta data about an individual through aggregation from the information collected? How will this be maintained, including verified for relevance completeness, and accuracy?	No
7. Will the new or meta data be part of an individual's record?	N/A
8. How will the new or meta data be used? Will it be used to make determinations about members of the public?	N/A
9. How will the 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.	No, a personal identifier is not sufficient to gain access to this system. An identifier and authenticator is required for system access. Only individuals with a valid need to know are provided these access credentials.
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)?	The individual provides the information voluntarily.

Module III – Systems with Information About Members of the Public

11. Will this information system provide the capability to identify, locate, and monitor individuals?	No
12. What kinds of information are collected as a function of the monitoring of individuals?	N/A
13. What controls will be used to prevent unauthorized monitoring?	N/A

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