E-1069

Department of Energy
Privacy Impact Assessment (PIA)

Affects Members Of the Public?	X

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.==

==This template may not be modified.==

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	February 24, 2010
Departmental Element & Site	Office of Environmental Management Department of Energy – Savannah River Operations Office
Name of Information System or IT Project	Savannah River Nuclear Solution (SRNS) Electronic Safeguards Security System (E3S)
Exhibit Project UID	UPI Code: 019-10-01-15-01-1057-00
New PIA ☐ **Update** ☒	

	Name, Title	Contact Information Phone, Email
System Owner	Lloyd Russ Busbee, Jr., Manager, Safeguards and Security Process Engineering, Savannah River Nuclear Solutions	(803) 725-4255 russ.busbee@srs.gov
Local Privacy Act Officer	Pauline Conner, Privacy Act Officer	(803) 952-8134 pauline.conner@srs.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Jannett M. Moran, Cyber Security Manager, Savannah River Nuclear Solutions	(803) 725-6925 jan.moran@srs.gov

PRIVACY PROGRAM

1

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Pauline Conner, Privacy Act Officer	(803) 952-8134 pauline.conner@srs.gov
Purpose of Information System or IT Project	The primary purpose of the Electronic Safeguards & Security System (E3S) is to track and control present and former U.S. Department of Energy (DOE), National Nuclear Security Administration (NNSA), and contractor employees accessing Departmental facilities and classified information areas, while providing protection of nuclear material, facilities, property and personnel. In addition, the E3S documents, tracks, manages, analyzes, and/or reports on foreign visit and assignment access to DOE facilities, including, Field Offices, National Laboratories and Contractor Sites. The purpose of the E3S is to maintain and use the information to determine the eligibility of individuals for a Personal Identity Verification (PIV) credential that provides access to DOE owned or leased facilities in accordance with HSPD-12. This PIA applies to all systems comprising the E3S system including the Test, Development, Production, and Maintenance systems.	
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	
Has there been any attempt to verify PII does not exist on the system?	No	

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.*	
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?	Yes ☒ 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?**	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.*); 5 U.S.C. 552a (the Privacy Act of 1974), Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees Contractors," August 27, 1004, and Title 5, Code of Federal Regulation, Parts 5 and 736. As provided in DOE O 206.1, "The Privacy Act allows an agency to maintain information about an individual that is relevant and necessary to the purpose of the agency as required by statute or by Executive Order of the President."
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)?**	Collection of the information in the E3S is required to verify an individual's identity and for contractors, grantees, and foreign national individuals requesting access to DOE facilities including contractor sites. If the individuals do not provide the information, SRNS will not be able to track and control present and former DOE, NNSA, and contractor employees accessing Departmental facilities and classified information areas. In addition, SRNS will not be able to issue a DOE PIV credential to the employees.

PRIVACY PROGRAM

4

MODULE II – PII SYSTEMS & PROJECTS

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 in the configuration, implementation, and maintenance of the system. Personal information may be disclosed to these contractors and their officers and employees in performance of their contracts. Those individuals provided this type of information is subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Pertinent 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.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The potential impact is MODERATE. The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individual are entitled under law. Security Plan, Version 0, dated May 30, 2007 Date of Accreditation: June 8, 2007
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.**	Yes. The E3S can retrieve data by using name, social security number, site computer user ID, and badge number.

MODULE II – PII SYSTEMS & PROJECTS

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.***	Yes. DOE 51, "Employee and Visitor Access Control Records;" DOE-52, "Access Control and Records of International Visits, Assignments, and Employment at DOE facilities and Contractor Sites;" DOE-63; "Personal Identity Verification;" Federal Register Vol. 74, No. 6/Friday, January 9, 2009 (pages 1053-1057; 1068-1071)
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 E3S collects information from the individual to whom it pertains, as well as information entered into E3S by Badge Office Personnel. For example, foreign national individuals requesting access to DOE facilities including contractor sites, reports from federal investigation agencies, DOE Office of Counterintelligence, Department of State, Department of Defense (DOE), Immigration and Naturalization Service, and other Government agencies.
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 vendor's database describes and documents the data elements.

DATA USE

MODULE II – PII SYSTEMS & PROJECTS

11. How will the PII be used?	The authorized employees will use the PII contained in E3S to track and control present and former DOE, NNSA, and contractor employees accessing Savannah River Site facilities and classified information areas. In addition, the authorized employees will issue PIV credential to the DOE, NNSA, and contractor employees accessing the Savannah River Site facilities and classified information areas.
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?	DOE will share individual's information with DOE Office of Counterintelligence, Department of State, Department of Defense, Immigration and Naturalization Service, and other Government agencies.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	The authorized user can generate a variety of reports that include visit/assignment request information and access to sensitive information and for reporting requirements by the local, federal and state agencies about individuals or contain an individual's data.
15. What will be the use of these reports?	The use of the data is relevant and necessary to track and control present and former DOE, NNSA, and contractor employees accessing Departmental facilities and classified information areas. Furthermore, the appropriate local, state and federal agencies will use certain records maintained in the E3S to ensure Departmental compliance with other regulatory requirements.
16. Who will have access to these reports?	Only authorized individuals will have access to the information based on need-to-know and the principle of least privilege. Furthermore, the appropriate local, state and federal agencies may have access to the records maintained in the E3S to ensure Departmental compliance with other regulatory requirements.
Monitoring	

PRIVACY
PROGRAM

MODULE II – PII SYSTEMS & PROJECTS

17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes. Mantrack tracks individuals entering certain facilities at the Savannah River through a Prox Card. Mantrack is not a real time but can provide a report identifying individuals' logical presence.
18. What kinds of information are collected as a function of the monitoring of individuals?	Mantrack collects information about an individual's logical presence.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The administrative controls include annual training emphasizing that it is the individual's responsibility to protect data that they have access to, and that misuse of that data will not be tolerated. The technical controls include restricted access via user-id and password based on user responsibility and job function.

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.	E3S does not verify the accuracy, relevance, and completeness of the data related to the public. E3S collects basic data directly from the individual to whom it pertains. Therefore, it is determined that the information is accurate, timely and complete at the time it was provided.
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 system is licensed by and operated for U.S. Department of Energy Savannah River Operations Office.

Retention & Disposition

22. What are the retention periods of data in the information system?	Retention periods are in accordance with National Archives and Records Administration (NARA) and DOE records schedules. Information can be obtained at http://cio.energy.gov/records-management/adminrs.htm.
23. What are the procedures for disposition of the data at the end of the retention period?	Procedures for disposition are documented in applicable NARA and DOE records schedule. Information can be obtained at http://cio.energy.gov/records-management/adminrs.htm.

ACCESS, SAFEGUARDS & SECURITY

MODULE II – PII SYSTEMS & PROJECTS

24. What controls are in place to protect the data from unauthorized access, modification or use?	Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The administrative controls include annual training emphasizing that it is the individual's responsibility to protect data that they have access to, and that misuse of that data will not be tolerated. The technical controls include restricted access via user-id and password based on user responsibility and job function.
25. Who will have access to PII data?	Only authorized individuals will have access to the information based on need-to-know and the principle of least privilege. Furthermore, the appropriate local, and state and federal agencies will use certain records maintained in the E3S to ensure Departmental compliance with other regulatory requirements. Access to or use of the information provided will be limited to authorized individuals for required management and reporting.
26. How is access to PII 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.
27. Do other information systems share data or have access to the data in the system? If yes, explain.	No
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?	There are no connecting information systems.
29. Who is responsible for ensuring the authorized use of personal information?	The system owner for other systems to have access to data within the E3S application must grant permission. Once provided, it is the responsibility of the other system owners to protect the data provided by E3S.

END OF MODULE II

PRIVACY
PROGRAM

SIGNATURE PAGE		
	Signature	Date
PIA Approval Signatures	Original Copy Signed and On File with the DOE Privacy Office	7 MAY 2010