



PRIVACY IMPACT ASSESSMENT: SAVANNAH RIVER NUCLEAR SOLUTIONS (SRNS)
 HUMAN RESOURCE MANAGEMENT SYSTEM (HRMS) E-10763
 PIA Template Version 3 – May, 2009

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	May 27, 2010	
Departmental Element & Site	Office of Environment Management Department of Energy – Savannah River Operations Office	
Name of Information System or IT Project	Savannah River Nuclear Solutions (SRNS) Human Resource Management System (HRMS)	
Exhibit Project UID	UPI Code: 019-10-01-15-01-1057-04	
New PIA	<input type="checkbox"/>	
Update	<input checked="" type="checkbox"/>	
	Name, Title	Contact Information Phone, Email
System Owner	Kelly Sanders, Manager, Benefits Solutions, Savannah River Nuclear Solutions	(803) 725-2135 kelly.sanders@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 IMPACT ASSESSMENT: SAVANNAH RIVER NUCLEAR SOLUTIONS (SRNS)
 HUMAN RESOURCE MANAGEMENT SYSTEM (HRMS)
 PIA Template Version 3 – May, 2009

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 People HRMS application is to manage payroll, pension, benefits and human resources data active employees, former employees, retirees, beneficiaries and dependants of active and former employees of the SRS Management and Operating (M&O) contractor. For purposes of this PIA, only former employees, retirees, their survivors and beneficiaries are included.	
Type of Information Collected or Maintained by the System:	<input checked="" type="checkbox"/> SSN Social Security number <input type="checkbox"/> Medical & Health Information e.g. blood test results <input checked="" type="checkbox"/> Financial Information e.g. credit card number <input checked="" type="checkbox"/> Clearance Information e.g. "Q" <input type="checkbox"/> Biometric Information e.g. finger print, retinal scan <input type="checkbox"/> Mother's Maiden Name <input checked="" type="checkbox"/> DoB, Place of Birth <input checked="" type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input checked="" type="checkbox"/> Name, Phone, Address <input type="checkbox"/> Other – Please Specify	
Has there been any attempt to verify PII does not exist on the system? DOE Order 206.1, <i>Department of Energy Privacy Program</i> , 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	



MODULE I – PRIVACY NEEDS ASSESSMENT

If “Yes,” what method was used to verify the system did not contain PII? (e.g. system scan)

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 <input type="checkbox"/> Federal Employees <input checked="" type="checkbox"/> 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.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS



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?

42 U.S.C. [United States Code] 7101 *et seq.*; 50 U.S.C. 2401 *et seq.*; 50 U.S.C. 2401 *et seq.* and the Memorandum of Understanding between the Department of Energy and the Department of Health and Human Services, 56 FR 9701, March 7, 1991.

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 SRNS HRMS system is required to be able to provide compensation and benefits to former employees, dependents, and survivors. Access to or use of the information provided will be limited to SRNS personnel directly involved in the HRMS system. If the information is not provided, SRNS will not be able to provide compensation and benefits to former employees, dependents, and survivors and to manage the payroll.

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.



MODULE II – PII SYSTEMS & PROJECTS

<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>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.</p> <p>Security Plan, Version 0, dated May 30, 2007</p> <p>Date of Accreditation: June 8, 2007</p>
<p>5. SORNs</p> <p>How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?</p> <p>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>Yes. The PeopleSoft uses a unique employee identifier (emplid) that is specific to the application. Data can also be retrieved by using other identifiers, such as SSN.</p>
<p>6. SORNs</p> <p>Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>?</p> <p>If "Yes," provide name of SORN and location in the <i>Federal Register</i>.</p>	<p>Yes. DOE-5, "Personnel Records of Former Contractor Employees"</p> <p>Federal Register Vol. 74, No. 6/Friday, January 9, 2009 (pages 1003-1005)</p>
<p>7. SORNs</p> <p>If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>N/A</p>

DATA SOURCES



MODULE II – PII SYSTEMS & PROJECTS

<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>The system collects information obtained from the former employees, dependants and survivors.</p>
<p>9. Will the information system derive new or meta data about an individual from the information collected?</p>	<p>No</p>
<p>10. Are the data elements described in detail and documented?</p>	<p>Yes. The vendor's database describes and documents the data elements.</p>
<p>DATA USE</p>	
<p>11. How will the PII be used?</p>	<p>The authorized employees will use the PII contained in HRMS to manage payroll, pension, benefits and human resources data of active employees, former employees, retirees, beneficiaries and dependents of active and former employees of the SRS M&O and Liquid Waste contractors.</p>
<p>12. If the system derives meta data, how will the new or meta data be used?</p> <p>Will the new or meta data be part of an individual's record?</p>	<p>N/A</p>
<p>13. With what other agencies or entities will an individual's information be shared?</p>	<p>We provide some of our protected PII data to our benefits providers (e.g. medical, vision, 401k, pension, etc.) as needed for them to provide benefits.</p>
<p>Reports</p>	
<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>The authorized user can generate reports that include human resources, payroll, and benefits administration information about individuals or contain an individual's data.</p>



MODULE II – PII SYSTEMS & PROJECTS

15. What will be the use of these reports?	The use of the data is relevant and necessary for SRNS to perform its required human resources responsibilities to manage benefits, pension data, and human resources data for former employees, dependents, and survivors.
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 HRMS to ensure Departmental compliance with other regulatory requirements.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. The HRMS does not have the capability to identify, locate, and monitor individuals.
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.	HRMS does not verify the accuracy, relevance, and completeness of the data related to the public. HRMS 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 the U.S. Department of Energy Savannah River Operations Office.
Retention & Disposition	



MODULE II – PII SYSTEMS & PROJECTS

<p>22. What are the retention periods of data in the information system?</p>	<p>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/adminirs.htm.</p>
<p>23. What are the procedures for disposition of the data at the end of the retention period?</p>	<p>Procedures for disposition are documented in applicable NARA and DOE records schedule. Information can be obtained at http://cio.energy.gov/records-management/adminirs.htm.</p>
<p>ACCESS, SAFEGUARDS & SECURITY</p>	
<p>24. What controls are in place to protect the data from unauthorized access, modification or use?</p>	<p>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.</p>
<p>25. Who will have access to PII data?</p>	<p>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 may have access to certain records maintained in the HRMS to ensure Departmental compliance with other regulatory requirements.</p>
<p>26. How is access to PII data determined?</p>	<p>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.</p>
<p>27. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>We also provide periodic data files (weekly/monthly/quarterly) with PII to our benefit providers (e.g. medical, vision, 401k, pension, etc.) and a weekly flat file of HR changes or new hires to the SRR Costpoint application.</p>
<p>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?</p>	<p>We have a Business Associate Agreement with each benefit provider in accordance with HIPAA.</p>



MODULE II – PII SYSTEMS & PROJECTS

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 HRMS application must grant permission. Once provided, it is the responsibility of the other system owners to protect the data provided by HRMS.

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