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** | July 21, 2009 |
| **Departmental Element & Site** | Office of Fossil Energy<br>Strategic Petroleum Reserve Office – New Orleans, LA 70123 |
| **Name of Information System or IT Project** | Unclassified Business Operations General Support System (GSS) |
| **Exhibit Project UID** | UPI Code: 019-20-01-16-02-3612-00 |
| **New PIA** ☒<br>**Update** □ | |

| | Name, Title | Contact Information Phone, Email |
|---|---|---|
| **System Owner** | Michael McWilliams, Assistant Project Manager, Management and Administration | (504) 734-4015<br>Michael.mcwilliams@spr.doe.gov |
| **Local Privacy Act Officer** | Deanna Harvey, Program Analyst | (504) 734-4316<br>Deanna.harvey@spr.doe.gov |
| **Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)** | Allen Rome, Cyber Security Program Manger<br>Chris Shipp, Information System Security Manager | (504) 734-4482<br>Allen.rome@spr.doe.gov<br>(504) 734-4905<br>Chris.shipp@spr.doe.gov |

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | | |
|---|---|---|
| **Person Completing this Document** | Coby Pennington, Information System Security Officer | (504) 734-4496<br>Coby.pennington@spr.doe.gov |
| **Purpose of Information System or IT Project** | The SPR GSS manages the common functionalities and storage for the extranet, intranet, and internet required for the day-to-day operations, mission, and technology need of the SPR. The GSS consists of several business applications utilizing a common security architecture. PII processing on the GSS applies to business functions relating to:<br>- Federal employee performance evaluations,<br>- Personnel security (legacy badging application for federal and contractors),<br>- Contractor payroll and human resources activities (utilized by the M&O contractor, does not have PII on federal employees).<br>The SPR does not collect information about members of the general public. All PII information relates to current and former employees and contractors, and only as relates to information needed to conduct business operations. | |
| **Type of Information Collected or Maintained by the System:** | ☒ SSN Social Security number<br>□ Medical & Health Information e.g. blood test results<br>☒ Financial Information e.g. credit card number<br>☒ Clearance Information e.g. "Q"<br>□ Biometric Information e.g. finger print, retinal scan<br>□ Mother's Maiden Name<br>☒ DoB, Place of Birth<br>☒ Employment Information<br>□ Criminal History<br>☒ Name, Phone, Address<br>□ Other – Please Specify | |
| **Has there been any attempt to verify PII does not exist on the system?**<br>**DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as *any information collected or maintained by the Department about an individual,*** | | YES |

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| *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)** | PII Risk Assessment was completed. |

### 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 (not the general public, former federal and contractors only) |
| **4. Is the information about DOE or contractor employees?** | YES<br>☒ Federal Employees<br>☒ Contractor Employees |

If the answer to <u>all</u> 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 | |
|---|---|
| AUTHORITY, IMPACT & NOTICE | |
| **1. AUTHORITY**<br>**What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?** | Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et.seq., 50 U.S.C. 2401 et seq.; Freedom of Information Act, 5 U.S.C. 552; and Privacy Act, 5 U.S.C. 552a.<br>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**<br>**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)?** | During the hiring process SPR collects mandatory personnel security information from federal employees and contractors. In order to be given access to the facilities and be a registered user of the system, the applicant must provide all required personal information and go through the background investigation. Information obtained during the hiring process is not voluntary, but is only used for authorized business purposes.<br>The contractor collects information required to process payroll and health care administration of its employees. |
| **3. CONTRACTS**<br>**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 |
| **4. IMPACT ANALYSIS:**<br>**How does this project or information system impact privacy?** | Technical, physical, and administrative controls are used to minimize the possibility of unauthorized access, use, or dissemination of the data in the system. Data is only used by authorized personnel for authorized business purposes. The system also has had a full certification and accreditation. |

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **5. SORNs**<br>**How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?**<br>**If yes, explain, and list the identifiers that will be used to retrieve information on the individual.** | Personnel security data can be retrieved by using: name or SSN.<br>Contractor payroll and health care benefits data can be retrieved by using personnel number or employee name. |
| **6. SORNs**<br>**Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?**<br>**If "Yes," provide name of SORN and location in the *Federal Register*.** | Federal Register, Vol. 74, No. 6, Friday, January 9, 2009<br>Energy Department, Privacy Act; System of Records<br>DOE-5 Personnel Records of Former Contractor Employees<br>DOE-13 Payroll and Leave Records<br>DOE-63 Personal Identity Verification (PIV) Files |
| **7. SORNs**<br>**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?** | Directly from the individual during the hiring and employment process. |
| **9. Will the information system derive new or meta data about an individual from the information collected?** | NO |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **10. Are the data elements described in detail and documented?** | YES, at the business application level. |
| DATA USE | |
| **11. How will the PII be used?** | The protected PII is used by DOE employees for performance evaluations.<br>Protected PII is used for personnel security processes for physical and logical access to SPR facilities and systems.<br>The contractor uses protected PII for payroll and health care administration of its employees. |
| **12. If the system derives meta data, how will the new or meta data be used?**<br>**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?** | The contractor shares payroll and health care administration data as required with the following:<br>Health Insurance Providers – uses the data from the GSS for the purposes of SPR providing health care provider information; and<br>US Treasury – uses the data to provide state and federal tax information to the US Treasury.<br>Financial Institutions – uses the data to deposits funds into employees bank accounts.<br>Legal Representatives – uses the data to fulfill court mandated garnishments and payments. |
| Reports | |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **14. What kinds of reports are produced about individuals or contain an individual's data?** | Finance and human resources personnel can generate reports related to contractor payroll and health care administration.<br>Personnel security staff can generate reports related to badging activities and for system administrators in order to determine if any terminated or inactive users still have active accounts on the GSS. |
| **15. What will be the use of these reports?** | Finance and human resources utilize reports in performance of their official duties for processing contractor payroll and health care benefits.<br>Personnel security staff and system administrators utilize reports from the SPR badging system to obtain the listing of SPR authorized personnel. This is compare to the listing of all GSS users. If there are accounts that belong to individuals who are not on the listing of authorized personnel, they are removed from the system immediately. |
| **16. Who will have access to these reports?** | Reports for contractor payroll and health care benefits can be accessed by finance and human resources staff.<br>Personnel security reports can be accessed by personnel security, system administrators, and cyber security. |
| Monitoring | |
| **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?** | YES |
| DATA MANAGEMENT & MAINTENANCE | |

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **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.** | All data is user provided and data currency is verified at time of collection by finance, human resources, and personnel security staff..<br>.<br>The contractor provides annual lists of benefits and personal data to its employees to ensure that the information is accurate and complete.<br>Also, the SPR badging system maintains a list of authorized personnel and is updated when an employee is terminated. The employee list is pushed out nightly and SPR personnel must compare it to the badging system. If accounts of terminated employees are active on the system, they are removed. |
| **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 SPR GSS is located at SPR Headquarters in New Orleans, LA. The GSS is not operated at the SPR field sites. |
| **Retention & Disposition** | |
| **22. What are the retention periods of data in the information system?** | Retention periods vary per data type and applicable laws and RIDS. |
| **23. What are the procedures for disposition of the data at the end of the retention period?** | GSA approved shredders along with shred drop bins are used to dispose of sensitive unclassified paper documents (SUI, OUO, etc). Approved processes for clearing, purging, and destroying storage media have been developed and are documented in the GSS System Security Plan (SSP). SPRPMO Help Desk or Cyber Security provides oversight of the process as required. |
| **ACCESS, SAFEGUARDS & SECURITY** | |
| **24. What controls are in place to protect the data from unauthorized access, modification or use?** | Technical (network devices, user accounts, access privileges, etc), physical (guards, locks, etc), and administrative controls (policies and procedures) are utilized to protect data from unauthorized access, modification, or use. Controls are captured in detail in the GSS System Security Plan (SSP). Additionally, the Learning Management System is used to provide new and existing users with cyber security awareness training. The Learning Management System provides users training on protected personally identifiable information (PII) and sensitive unclassified information (SUI). New users must complete awareness training within 30 days of hire and undergo a refresher annually. The system also has had a full certification and accreditation. |

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **25. Who will have access to PII data?** | Finance, human resources, personnel security, business systems analysts, and cyber security in performance of their official duties. |
| **26. How is access to PII data determined?** | User's access is restricted based on functional role, user account, business application, and data required to perform official duties. |
| **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?** | N/A, PII data is not shared with any connecting system. |
| **29. Who is responsible for ensuring the authorized use of personal information?** | System Owner |

## END OF MODULE II

## SIGNATURE PAGE

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