PRIVACY IMPACT ASSESSMENT: OFFICE OF LEGACY MANAGEMENT:
RECORDS HANDLING SYSTEM
ROCKY FLATS ENVIRONMENTAL RECORDS DATABASE
PIA Template Version – May, 2009

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.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	June 4, 2009
Departmental Element & Site	Office of Legacy Management, Morgantown, WV
Name of Information System or IT Project	LM Records Handling System (LMRHS01) – Rocky Flats Environmental Records Database
Exhibit Project UID	019-10-01-31-02-1014-00
New PIA [X] **Update** [ ]	Please indicate whether this is a new PIA or an update to an existing PIA. List the name of the PIA being updated.

	Name, Title	Contact Information Phone, Email
System Owner	Deborah Haddix IT Specialist	3600 Collins Ferry Road Morgantown, WV 26505 (304) 285-4849 Deborah.Haddix@lm.doe.gov
Local Privacy Act Officer	John Montgomery Federal Program Cyber Security Manager	3600 Collins Ferry Road Morgantown, WV 26505 (304) 285-4520 John.Montgomery@lm.doe.gov

PRIVACY IMPACT ASSESSMENT: OFFICE OF LEGACY MANAGEMENT:
RECORDS HANDLING SYSTEM
ROCKY FLATS ENVIRONMENTAL RECORDS DATABASE
PIA Template Version – May, 2009

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Michael Bulebush Information System Security Officer	3596 Collins Ferry Road Morgantown, WV 26505 (304) 225-8347 Michael.Bulebush@lm.doe.gov
Person Completing this Document	Len Turton Solutions Architecture Manager	3596 Collins Ferry Road Morgantown, WV 26505 (304) 225 8358 Leonard.Turton@lm.doe.gov
Purpose of Information System or IT Project	The system stores and provides access to consolidated environmental data collected from the EG&G contractor. This database is used as a record-finding aid, allowing LM to achieve its goal to preserve, protect, and make accessible legacy records and information. The information is frequently accessed to respond to current FOIA and routine requests. This system databases provides ties to PDF and TIFF images eliminating the need to pull the physical paper from the FRC. System does not store record content.	
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?		YES

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.*	Some systems employ software tools to scan content (information or data) to search for types of data such as Social Security numbers.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Used database query looking for key words fields.

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 (If "Yes," place an X in the box at the top of first page.) *Member of the Public* refers to individuals in a non-employee or DOE contractor context. *Members of the Public* includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE
4. Is the information about DOE or contractor employees?	YES ☒ Federal Employees ☒ 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 I – PRIVACY NEEDS ASSESSMENT

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 **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	• E-Government Act of 2002 • 10 CFR 1004, Freedom of Information, Department of Energy Guidance • 10 CFR 1008, Records Maintained on Individuals (Privacy Act), DOE Guidance • 20 CFR 30, Claims for Compensation Under the Energy Employee's Occupational Illness Compensation Program Act • 36 CFR, Chapter 12, Subchapter B, Records Management • DOE Order 243.1, Records Management Program • NARA Guidance on Managing Web Records, January 2005 • NARA Records Management Guidance for Agencies Implementing Electronic Signature Technologies, October 2000
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)?**	N/A. The system contains mostly static information extracted from other applications.

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?**	Contractors are involved in the operation and maintenance of the system. Personal information from this system may be disclosed to these contractors and their officers and employees in performance of their contracts. Individuals provided information under this routine use are 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 impact to privacy is negligible as ERD personnel are trained in Privacy Act considerations and the information system utilizes antivirus, firewalls, account permission restrictions, and intrusion detection as measures to protect against breaches in confidentiality. Additionally, data is AES-encrypted during electronic transmission.
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 information is frequently accessed to respond to current FOIA and routine requests. This system databases provides ties to PDF and TIFF images eliminating the need to pull the physical paper from the FRC. Data is retrieved based on key words which are used to search the database.

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*.**	▪ DOE-5, Personnel Records of Former Contractor Employees ▪ DOE- 10, Energy Employees Occupational Illness Compensation Program Act ▪ DOE-35, Personnel Radiation Exposure Records ▪ DOE-41, Legal Files (Claims, Litigation, Criminal Violations, Patents, and Others) ▪ DOE-55, Freedom of Information and Privacy Act (FOIA/PA) Requests for Records ▪ DOE-72, The DOE Radiation Study Registry
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A. The system is not being modified.
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	The system stores and provides access to consolidated environmental data collected from the EG&G contractor. This database is used as a record finding aid, allowing LM to achieve its goal to preserve, protect, and make accessible legacy records and information. The information is frequently accessed to respond to current FOIA and routine requests. This system databases provides ties to PDF and TIFF images eliminating the need to pull the physical paper from the FRC. System does not store record content.
9. Will the information system derive new or meta data about an individual from the information collected?	The information is only used as a finding aid to respond to current FOIA and routine requests. This system databases provides ties to PDF and TIFF images eliminating the need to pull the physical paper from the FRC.
10. Are the data elements described in detail and documented?	The database contains a data dictionary that was generated during system development.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	The information is frequently accessed to respond to current FOIA and routine requests. This system databases provides ties to PDF and TIFF images eliminating the need to pull the physical paper from the FRC.
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?**	The information is only used as a finding aid to respond to current FOIA and routine requests. This system databases provides ties to PDF and TIFF images eliminating the need to pull the physical paper from the FRC.
13. With what other agencies or entities will an individual's information be shared?	DOE Federal and contractor personnel will have access to the data in the system. Access to personal data in the system is strictly controlled based on job responsibility and function.
Reports	
14. What kinds of reports are produced about individuals or that contain an individual's data?	No reports are produced on individuals.
15. What will be the use of these reports?	N/A. No reports are produced on individuals.
16. Who will have access to these reports?	N/A. No reports are produced on individuals.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system 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?	None.

MODULE II – PII SYSTEMS & PROJECTS	
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.	This database is used as a record finding aid, allowing LM to achieve its goal to preserve, protect, and make accessible legacy records and information. System does not store record content. This data is checked for accuracy and verified for accuracy and completeness upon retrieval of the records.
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 only operated at one site.
Retention & Disposition	
22. What are the retention periods of data in the information system?	The information is frequently accessed to respond to current FOIA and routine requests. This system databases provides ties to PDF and TIFF images eliminating the need to pull the physical paper from the FRC.
23. What are the procedures for disposition of the data at the end of the retention period?	This database is used as a record finding aid, allowing LM to achieve its goal to preserve, protect, and make accessible legacy records and information. System does not store record content.
ACCESS, SAFEGUARDS & SECURITY	
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 technical controls include restricted access via user ID and password based on user responsibility and job function. All system team members (Federal and contractor) are required to complete the Department of Energy Headquarters Annual Cyber Security Refresher Briefing or LM Annual Cyber Security Refresher Briefing as a necessary prerequisite for access to the system. Administrative controls include non-disclosure agreements and separation of duties so individuals only have access to the system for specific projects.

MODULE II – PII SYSTEMS & PROJECTS	
25. Who will have access to PII data?	Access will be restricted by position role and responsibilities and to site specific record libraries. Users do not have access to all site libraries.
26. How is access to PII data determined?	Access to data is restricted to LM record staff and other LM personnel with business need for the information. Based on a specific need, the user is assigned permissions that are applied using system access control lists. User accounts are reviewed monthly to identify and remove users who have left the organization or whose duties no longer require access to the system.
27. Do other information systems share data or have access to the data in the system? If yes, explain.	No other systems share data or have access to the data in the system.
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?	A Memorandum of Understanding and Interconnection Security Agreement will be signed by the System Owners within 30 days of this documentation.
29. Who is responsible for ensuring the authorized use of personal information?	System Owner: Deborah Haddix, IT Specialist
END OF MODULE II	

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