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 11, 2009
Departmental Element & Site	Idaho National Laboratory Willow Creek Building RIOT-Center
Name of Information System or IT Project	INL SECURITY INFORMATION MANAGEMENT SYSTEM BUSINESS ENCLAVE
Exhibit Project UID	311
New PIA ☐ **Update** X	DOE PIA - SECIMS Final lxw.doc

	Name, Title	Contact Information Phone, Email
System Owner	Kelley R. Moedl Manger, Safeguards/Personnel Security	208-526-8671 Kelley.Moedl@inl.gov
Local Privacy Act Officer	Dale Claflin Privacy Act Officer	208-526-1199 Dale.Claflin@inl.gov

PRIVACY

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Daniel Jones Technical Lead, Cyber Security	208-526-6477 Daniel.Jones@inl.gov
Person Completing this Document	Kenneth Kelley, Computer System Administration	208-5261453 Kenneth.Kelley@inl.gov
Purpose of Information System or IT Project	The purpose of this data system is to collect, maintain, utilize, and archive information relating to an individual's security posture, credentials, clearances, etc. for authorized access to the Department of Energy's Idaho National Laboratory	
Type of Information Collected or Maintained by the System:	☒ SSN ☐ Medical & Health Information ☐ Financial Information ☒ Clearance Information ☐ Biometric Information ☐ 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? **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*		YES

MODULE I – PRIVACY NEEDS ASSESSMENT

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)	Manual validation was provided by the Data Services group. Additionally, when performing the Privacy Impact Assessment information was verified.

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 <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 **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Contract No. DE-AC07-05ID14517
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)?**	Individuals are required to provide information in the self-identification portion of the application form.
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 not involved with the life cycle of the system.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The data maintained on this system has the same potential to impact an individual's privacy as would the loss of similar data from any public, private, government, or other system if not properly safeguarded.

MODULE II – PII SYSTEMS & PROJECTS	
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.**	Data are retrieved using name, S number, SS number.
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-43.
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	NO
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Individual-provided, BEA, and the Department of Energy; No other tribal, state or local government entities; or third parties contribute.
9. Will the information system derive new or meta data about an individual from the information collected?	YES

MODULE II – PII SYSTEMS & PROJECTS	
10. Are the data elements described in detail and documented?	YES – The SECIMS database schema
DATA USE	
11. How will the PII be used?	The use of this data system will determine and track an individual's security posture, security credentials, access, clearances, etc. for authorized access to the Department of Energy's Idaho National Laboratory
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 meta data generated is utilized to flag actions to be taken on part of the Personnel Security Office. This data is not retained once the flag is cleared. Additionally the system automatically assigns an individual tracking number (key) for the individual, security credential numbers and credential status. This data is archived.
13. With what other agencies or entities will an individual's information be shared?	Validation of Social Security number and birth date in association with name is performed by DOE/NNSA Counter Intelligence. No other tribal, state or local government entities; or third parties will share this information.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports of current participants are produced daily, weekly, quarterly and annually – ad hoc reports are produced when required.
15. What will be the use of these reports?	Examples: investigations, requests from program sponsors, daily action list, etc.

MODULE II – PII SYSTEMS & PROJECTS

16. Who will have access to these reports?	Access to standard and ad-hoc reports are on a need-to-know basis
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	This system does not provide 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.	Data is current at the time of employment. Employee validation is taken to ensure the data are current.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	This system is not operated in more than one site.
Retention & Disposition	
22. What are the retention periods of data in the information system?	The retention time is as much as 5 years after termination of employment
23. What are the procedures for disposition of the data at the end of the retention period?	Disposition of all information follows company and federal regulation record retention and disposition policies and procedures.

MODULE II – PII SYSTEMS & PROJECTS

ACCESS, SAFEGUARDS & SECURITY

24. What controls are in place to protect the data from unauthorized access, modification or use?	The INL has implemented controls per the DOE's Program Cyber Security Plan Version 1.2 and continues to operate within the guidance of the PCSP. This system is included in the Business Enclave, which is categorized as moderate, and was certified and accredited December 19, 2007.
25. Who will have access to PII data?	Access is determined via need-to-know and roles and responsibilities.
26. How is access to PII data determined?	Access to PII data is determined by the data owner. Access is reviewed and justified annually.

MODULE II – PII SYSTEMS & PROJECTS

27. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes, this system collects and shares data with multiple systems at the INL. Specifically: CHARGEBACK – Archibus & Facility Management DOSELINK – Dosimetry FSPRD – ICP Financial Systems GDS1 – Electronic Directory Services GDS2 – sitepeople SQL Server HRPRD88 – Human Resources HUB – Lotus Notes IPRD – Passport MED1 – Medical RCMS – Radcom Passport SANDS – Misc Security TRAIN – Training
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?	No.
29. Who is responsible for ensuring the authorized use of personal information?	All users are responsible for assuring proper use of the data. All printed matter is required to be reviewed for Official Use Only (OUO)and handled as OUO until such review has determined otherwise.

MODULE II – PII SYSTEMS & PROJECTS

END OF MODULE II

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