Department of Energy
Office of Science
ORNL Site Office
P.O. Box 2008
Oak Ridge, Tennessee 37831-6269

February 19, 2023

MEMORANDUM FOR W. KEN HUNT
CHIEF PRIVACY OFFICER
DEPARTMENT OF ENERGY

FROM: JOHNNY O. MOORE
MANAGER
OAK RIDGE NATIONAL LABORATORY SITE OFFICE

SUBJECT: PRIVACY IMPACT ASSESSMENT - OAK RIDGE NATIONAL LABORATORY (ORNL) - EXTERNAL DOSE MANAGEMENT SYSTEM (EDMS) AND BIOASSAY DATA MANAGEMENT SYSTEM (BDMS)

Attached is an approved Privacy Impact Assessment for the ORNL EDMS and BDMS. Review and approval of this document has been coordinated with your office and with the Local Privacy Officer, and it is being provided to you per Department of Energy Order 206.1 requirements.

If there are any questions or additional information required, please contact Doug Reed at Doug.Reed@science.doe.gov.

Attachments

cc w/attachments:
Christopher D. Hicks, IM-42
Linda G. Chapman, SC-GCS
Michele G. Branton, SC-OSO
Donte F. Davis, SC-OSO
Douglas R. Reed, SC-OSO
Dan S. DeVore, ORNL
Director's Files

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: ***https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file***

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	9/26/2022	
Departmental Element & Site	U.S. Department of Energy Office of Science Oak Ridge National Laboratory Site Office Oak Ridge National Laboratory	
Name of Information System or IT Project	External Dose Management System (EDMS) and Bioassay Data Management System (BDMS) - digital storage and management of information associated with DOE-35, Personnel Radiation Exposure Records	
Exhibit Project UID		
New PIA [x] **Update** [ ]		
	Name, Title	**Contact Information Phone, Email**
System Owner	Johnny O. Moore Manager ORNL Site Office	(865) 576-3536 johnny.moore@science.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Linda Chapman DOE FOIA/Privacy Act Officer DOE Oak Ridge Office	(865) 576-2129 Linda.chapman@science.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Dustin Reinert ORNL Information Systems Security Officer UT-Battelle, LLC Contractor to the US Department of Energy	865-341-2270 reinertdp@ornl.gov
Person Completing this Document	Dan DeVore ORNL Privacy Officer UT-Battelle, LLC Contractor to the US Department of Energy	(865) 341-1400 devoreds@ornl.gov
Purpose of Information System or IT Project	The purpose of EDMS and BDMS is to collect, record, monitor, and report on worker and visitor occupational radiation exposure at Oak Ridge National Laboratory as authorized and required by 10 C.F.R. § 835. Specifically, EDMS and BDMS are used to monitor worker and visitor occupational radiation exposure in accordance with 10 C.F.R. § 835.401, collect and maintain individual exposure records in accordance with 10 C.F.R. § 835.702, and to fulfill reporting requirements to the individual and the DOE as required by 10 C.F.R. § 835.801 and DOE Order 231.1B, Environment, Safety and Health Reporting. This information system is associated with Department of Energy System of Records, DOE-35, “Personnel Radiation Exposure Records." DOE O 231.1B mandates reporting radiation exposure dose data to the Department of Energy’s Radiation Exposure Monitoring System (“REMS”), and reporting to the REMS requires inclusion of full social security numbers when available: https://www.energy.gov/ehss/downloads/radiological-control-technical-position-regarding-use-social-security-numbers-dose ; https://www.energy.gov/ehss/articles/radiation-exposure-monitoring-systems-data-reporting-guide) The “medical and health information” collected and reported to REMS (and to the individual) is specifically related to the dosage of individual’s occupational radiation exposure, which must be collected, monitored, and reported on.	
Type of Information Collected or	☒ SSN ☒ Medical & Health Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

Maintained by the System:	☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☒ DoB, Place of Birth (DoB only) ☒ Employment Information (Employer information, Employee ID, Division) ☐ Criminal History ☒ Name, Phone, Address ☒ Other (Gender)
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 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.*	N/A – PII and Privacy Act Information are known to exist on this information system.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A – system is known to contain PII.

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

MODULE I – PRIVACY NEEDS ASSESSMENT

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

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	10 C.F.R. § 835.401, 10 C.F.R. § 835.702, 10 C.F.R. § 835.801, and DOE Order 231.1B. As it relates to the collection and use of full social security numbers, DOE O 231.1B mandates reporting radiation exposure dose data to the Department of Energy's Radiation Exposure Monitoring System ("REMS"), and reporting to the REMS requires inclusion of full social security numbers when available (https://www.energy.gov/ehss/downloads/radiological-control-technical-position-regarding-use-social-security-numbers-dose; https://www.energy.gov/ehss/articles/radiation-exposure-monitoring-systems-data-reporting-guide).

MODULE II – PII SYSTEMS & PROJECTS	
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 notified at the time of collection that their failure to provide all or part of the requested information may prevent the individual from receiving a personnel dosimeter. There is currently no formalized opportunity for an individual to consent to uses of information beyond what is required or authorized.
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. The ORNL M&O contract includes FAR 52.224-1 Privacy Act Notification, FAR 52.224-2 Privacy Act, and DEAR 952.223-75 Preservation of individual occupational radiation exposure records.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	EDMS and BDMS maintain personally identifiable information (PII) including the types of PII indicated on page 2 of this assessment. Additionally, the federal information collected and maintained by this system has been identified by DOE as a Privacy Act System of Record: DOE-35, "Personnel Radiation Exposure Records." EDMS and BDMS incorporate components of the Fair Information Practice Principles (FIPPs) to reduce potential privacy impact to individuals arising from these systems. In furtherance of data minimization, EDMS and BDMS collect and maintain only PII that is reasonably necessary and required to monitor worker and visitor occupational radiation exposure, collect and maintain individual exposure records, and fulfill reporting requirements to the individual and the DOE. In furtherance of transparency, individual participation, purpose specification, and use limitation, individuals are presented with a Privacy Act Notice when their information is collected for a personnel dosimeter, which conveys the purpose of the collection of PII, permissible uses and disclosures of the PII, the legal authority for the collection of PII, and the impact of choosing not to provide the PII. Additionally, DOE has provided notice to the public regarding the collection, use, and maintenance of information for this System of Record through a System of Record Notice provided in the Federal Register (identified in Question 6 below), which further these principles. In furtherance of Security, EDMS and BDMS are designed to protect and safeguard PII via the controls specified in the ACCESS, SAFEGUARDS & SECURITY section below, access to BDMS and EDMS is based on need-to-know, and information within the system is only shared in accordance with the Privacy Act. In furtherance of data quality and integrity, BDMS and EDMS receive a scheduled, nightly feed from the ORNL HR system as described in Question 20 below. These measures and others outlined in this PIA are designed to prevent negative impacts on privacy arising from EDMS and BDMS.
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 data can be retrieved by searching by unique identifiers of individuals. The data is retrievable by the following identifiers: name, badge number, date of birth, Social Security Number, and person ID (system-specific ID).

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. Department of Energy Privacy Act of 1974; Publication of Compilation of Privacy Act Systems of Records 74 FR 993, January 9, 2009. DOE-35 Personnel Radiation Exposure Records Pages 993-1090
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 individuals are the sources of information—the personal information in this system is collected directly from the individuals by ORNL. Specifically, the names, phone numbers, addresses, genders, dates of birth, and employment information used in EDMS/BDMS are collected/generated for employees as a part of the new employee onboarding process and for non-employees as a part of the visitor registration process. The ORNL HR system then provides this information to EDMS/BDMS. The SSN is collected from employees as a part of the new employee onboarding process, and it is provided by the HR system to EDMS/BDMS. The SSN for non-employees is collected directly from non-employees as a part of their participation in ORNL's occupational radiation exposure monitoring program. The medical and health information in EDMS/BDMS is collected/generated through the individual's participation in ORNL's occupational radiation exposure monitoring program.
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.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	The PII will be used to collect, monitor, record, and report on worker and visitor occupational radiation exposure at ORNL. Specifically, the PII will be used to monitor worker and visitor occupational radiation exposure as required by 10 C.F.R. § 835.401, maintain individual exposure records as required by 10 C.F.R. § 835.702(a) and (b), and to fulfill reporting requirements to the individual and the DOE as required by 10 C.F.R. § 835.801(a) and DOE Order 231.1B, Environment, Safety and Health Reporting.
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?	This information will be shared within DOE, including with other DOE contractors in performance of their contracts. As necessary, information may be shared with other agencies or entities as permitted by the applicable SORNs cited below. Department of Energy Privacy Act of 1974; Publication of Compilation of Privacy Act Systems of Records 74 FR 993, January 9, 2009. DOE-35 Personnel Radiation Exposure Records Pages 993-1090
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	An annual report of occupational radiation exposure data is submitted to the DOE Radiation Exposure Monitoring System (REMS) Repository in accordance with the requirements of DOE Order 231.1B, Environment, Safety and Health Reporting. An annual (or more frequent) report of individual radiation exposure data is made to each monitored individual as required by 10 C.F.R. § 835.801. Internal reports are created on an ad-hoc basis in support of ORNL's occupational radiation exposure monitoring program, which facilitates compliance with the requirements of 10 C.F.R. Part 835.
15. What will be the use of these reports?	Reports are used to meet reporting requirements to DOE and to monitored individuals as well as to monitor and support compliance with requirements 10 C.F.R. Part 835 and DOE Order 231.B.
16. Who will have access to these reports?	The REMS report will be accessible by authorized DOE personnel. The individual reports are accessible by the individual. The internal reports are accessible by limited, authorized ORNL personnel with an official need-to-know.
Monitoring	

MODULE II – PII SYSTEMS & PROJECTS	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. This system allows monitoring of an individual's occupational exposure to radiation at ORNL, but it does not have a monitoring capability beyond this.
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.	EDMS and BDMS receive a scheduled, nightly feed from the ORNL HR system that refreshes names, phone numbers, addresses, genders, dates of birth, employment information, and when available, social security numbers (ORNL employees only) to ensure accuracy, relevance, and completeness.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Not Applicable. The systems are not operated in more than one site.
Records Management	
22. Identify the record(s).	Nuclear & Radiological Protection Personnel Radiation Exposure Records
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. □ Unscheduled XX Scheduled (cite NARA authority(ies) below) DOE Admin 1: 21.4C Individual Employee Health Hazard Case Files – NARA Approval Authority NCI-430-76-9 (4b(3))
24. Records Contact	Gayla Creasey creaseygd@ornl.gov 865-576-8788
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The *Servers* Enclave, where this system resides, operates under a current DOE granted Authority to Operate (ATO). The security controls for this system are based on FISMA requirements to achieve compliance with Federal law and Department of Energy (DOE) policy and to protect the confidentiality, integrity, and availability of this Information System. The Unclassified *Cyber Security Program Plan* (CSPP), and the *Servers* Enclave System Security Plan (SSP) implement the technical, operational, and management controls to secure this Information System at a Moderate level.
26. Who will have access to PII data?	Only those staff who have a need to know, and that have requested and been granted access will have access to this data. Level of access is granted through evaluation of need to know, review of requested purpose for access, and ORNL management approves of the request. The Information owner either controls access or is asked whether access is warranted before ITSD staff alters membership.
27. How is access to PII data determined?	Access to the PII in this Information System is provided by the ORNL Universal Computer Access Management System (UCAMS) and is role based. Level of access is through evaluation of need-to-know, review of requested purpose for access, and ORNL management approvals of the request.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes, the ORNL HR system transmits PII to EDMS and BDMS. Specifically, EDMS and BDMS receive a scheduled, nightly feed from the ORNL HR system that refreshes names, phone numbers, addresses, genders, dates of birth, employment information, and when available, social security numbers (ORNL employees only) to ensure accuracy, relevance, and completeness of the information in EDMS and BDMS. The ORNL HR system cannot, however, access data in EDMS or BDMS.
29. 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
30. Who is responsible for ensuring the authorized use of personal information?	The ORNL Information System Owner (ISO) / Designee(s) of the system.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) Date: 2023.02.19 13:01:21 -05'00' (Signature)	
Local Privacy Act Officer	(Print Name) Linda Chapman Digitally signed by Linda Chapman Date: 2023.02.01 10:44:07 -05'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.01.19 10:38:34 -05'00' (Signature)	