




Department of Energy

Office of Science

ORNL Site Office
P.O. Box 2008
Oak Ridge, Tennessee 37831-6269

September 25, 2023

MEMORANDUM FOR W. KEN HUNT
DEPUTY CHIEF INFORMATION OFFICER
ENTERPRISE RECORDS MANAGEMENT, PRIVACY, AND COMPLIANCE

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

SUBJECT: PRIVACY IMPACT ASSESSMENTS - OAK RIDGE NATIONAL
LABORATORY (ORNL)

Attached are two approved Privacy Impact Assessments for ORNL systems associated with Department of Energy (DOE) System of Records Notices 33 and 38. The three associated ORNL systems are the *Electronic Medical Business Operations System*, the *Days, Away, Restricted, Transferred* drive, and the *Comprehensive Tracking System*. Review and approval of these documents has been coordinated with your office and with the Local Privacy Officer, and they are being provided to you per DOE 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:

Daniel S. DeVore, ORNL

Director's Files

Christopher D. Hicks, IM-42

Linda G. Chapman, SC-GCS

Michele G. Branton, SC-OSO

K. Mike Hatcher, SC-OSO

Douglas R. Reed, SC-OSO

Privacy@hq.doe.gov



Affects
Members
Of the Public?

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	06/28/2023	
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	“DART” (Days, Away, Restricted, Transferred) drive and the Comprehensive Tracking System (CTS) - information systems used for the digital storage and management of information associated with DOE-38, Occupational and Industrial Accident Records.	
Exhibit Project UID		
New PIA <input checked="" type="checkbox"/>		
Update <input type="checkbox"/>		
	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	<p>DOE Order 231.1B, Environment, Safety and Health Reporting requires DOE contractors to record, monitor, and report on work-related injuries and illnesses involving employees and subcontractors at DOE sites. ORNL uses two primary systems to meet these requirements: the “DART” (Days, Away, Restricted, Transferred) drive and the Comprehensive Tracking System (CTS). The federal information maintained in the two systems (DART drive and CTS) are associated with the following DOE System of Record: DOE-38, “Occupational and Industrial Accident Records.”</p> <p>The DART drive is a secure drive that contains access-controlled folders to maintain digital records of each reported work-related injury or illness; the records include medical incident reports, medical notes, medical restrictions, field reports, corrective actions, classification forms and notifications, critiques, and other photos/records/information related to the injury/illness. Information from the records in the DART drive—including case investigation results—is entered into CTS, where it is combined with employee/subcontractor demographic and employment information in preparation for mandatory injury/illness reporting to DOE.</p> <p>CTS is then used to transmit ORNL’s work-related injury/illness incident information to the DOE Computerized Accident/Incident Reporting System (CAIRS) database (https://www.energy.gov/ehss/computerized-accident-incident-reporting-system) as required by DOE O 231.B. For example, the information provided to the CAIRS database via the CTS system is used to generate a completed DOE F 5484.3 (https://www.energy.gov/cio/articles/doe-f-54843), which is the mandatory reporting form for work-related injuries, illnesses, and accidents to DOE. CTS is further used to maintain and organize ORNL’s work-related injury/illness incident information and to generate required reports, which allows tracking and trending of incident/illness cases and rates, as well as monthly reporting to DOE.</p>	



MODULE I – PRIVACY NEEDS ASSESSMENT

<p>SSN</p> <p>Type of Information Collected or Maintained by the System:</p>	<p><input checked="" type="checkbox"/> SSN (CTS only. The DART drive does not maintain SSNs) Social Security Numbers are maintained in CTS to confirm identity and as an identifier for locating historical injury/illness records in response to Freedom of Information Act, Privacy Act, and Energy Employees Occupational Illness Compensation Program Act records requests.</p> <p><input checked="" type="checkbox"/> Medical & Health Information</p> <p><input type="checkbox"/> Financial Information</p> <p><input type="checkbox"/> Clearance Information</p> <p><input type="checkbox"/> Biometric Information</p> <p><input type="checkbox"/> Mother's Maiden Name</p> <p><input checked="" type="checkbox"/> DoB, Place of Birth (Date of Birth only)</p> <p><input checked="" type="checkbox"/> Employment Information</p> <p><input type="checkbox"/> Criminal History</p> <p><input checked="" type="checkbox"/> Name, Phone, Address</p> <p><input checked="" type="checkbox"/> Other – (Employee ID, Gender)</p>
<p>Has there been any attempt to verify PII does not exist on the system?</p> <p><i>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.</i></p>	<p>N/A – PII and Privacy Act Information are known to exist on this information system.</p>
<p>If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)</p>	<p>N/A – system is known to contain PII.</p>
<p>Threshold Questions</p>	
<p>1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?</p>	<p>YES</p>



MODULE I – PRIVACY NEEDS ASSESSMENT

2. Is the information in identifiable form?	YES
3. Is the information about individual Members of the Public?	NO
4. Is the information about DOE or contractor employees?	YES <input checked="" 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

AUTHORITY, IMPACT & NOTICE

<p>1. AUTHORITY</p> <p>What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?</p>	<p>DOE O 231.1B requires Department of Energy (DOE) contractors to record and report work-related fatalities, injuries, and illness in accordance with the requirements of 29 C.F.R. 1904. Among other things, the order requires injury and illness incident reports be submitted to the CAIRS (Computerized Accident/Incident Reporting Systems) database, which requires submission of name, home address, employee ID number, date of birth, gender, and employment information for each fatality/injury/illness (See https://www.energy.gov/ehss/articles/injury-and-illness-reporting-guide).</p> <p>Social Security Numbers are maintained in CTS to confirm identity and as an identifier for locating historical injury/illness records in response to Freedom of Information Act, Privacy Act, and Energy Employees Occupational Illness Compensation Program Act records requests.</p> <p>Additionally, the System of Record Notice (SORN) for DOE-38, “Occupational and Industrial Accident Records” includes the following categories of records: name, social security number, accident/incident information, occupational injury and illness experience, property damage experience, and motor vehicle accidents.</p> <p>Department of Energy Privacy Act of 1974; Publication of Compilation of Privacy Act Systems of Records 74 FR 993, January 9, 2009. DOE-38, Occupational and Industrial Accident Records Pages 993-1090</p>
<p>2. CONSENT</p> <p>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)?</p>	<p>There is currently no formalized opportunity for an individual to consent to uses of information beyond what is required or authorized.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>3. CONTRACTS</p> <p>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?</p>	<p>Yes. The ORNL M&O contract includes FAR 52.224-1 Privacy Act Notification, FAR 52.224-2 Privacy Act, and requires compliance with DOE O 206.1.</p>
<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>The DART drive and CTS 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-38, "Occupational and Industrial Accident Records."</p> <p>Under Federal Information Processing Standards (FIPS) Publication 199 impact analysis, a loss of confidentiality involving the PII in the DART drive and CTS could result in a moderate potential impact to individuals (i.e. could be expected to have a serious adverse effect on individuals due to the loss of privacy). The security controls for CTS/DART 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 these information systems.</p> <p>CTS and DART are designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls:</p> <ul style="list-style-type: none"> • Strict access control enforcement based on need-to-know <p>CTS/DART both reside in the Servers Enclave, which operates under a current DOE-granted Authority to Operate (ATO). The Unclassified Cyber Security Program Plan (CSPP), and the Servers Enclave System Security Plan (SSP) describe the technical, operational, and management controls to secure these information systems at a Moderate level.</p>



MODULE II – PII SYSTEMS & PROJECTS

<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 data can be retrieved by searching by unique identifiers of individuals. The data is retrievable from the DART drive by the following identifiers: last name and date of injury.</p> <p>The data is retrievable from CTS by the following identifiers: badge number and Social Security Number.</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.</p> <p>Department of Energy Privacy Act of 1974; Publication of Compilation of Privacy Act Systems of Records 74 FR 993, January 9, 2009.</p> <p>DOE-38, Occupational and Industrial Accident Records Pages 993-1090</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 individuals are the sources of information—the personal information in this system is collected directly from the individuals by ORNL.</p> <p>Specifically, the name (first, middle, last), date of birth, social security number, badge number, home phone number, home address, gender, and work/employment information used in CTS is collected from and generated for employees as a part of the new employee onboarding process and for non-employees as a part of the initial registration process through personnel security. After this information is collected/generated, it is maintained in the ORNL enterprise data repository (SAP), which then provides the information to CTS. This data is refreshed in CTS regularly through a weekly data import from SAP to CTS to keep the information updated, accurate, and complete. For employees, the medical and health information in the DART Drive is collected directly from the individual by ORNL Health Services and/or generated through the individual’s participation in ORNL’s occupational health program (e.g. medical evaluations, medical assessments, etc.) For subcontractors, the medical and health information in the DART Drive is collected from either the subcontractor point-of-contact on-site or the involved ESH&Q coordinator.</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.</p>
<p>DATA USE</p>	
<p>11. How will the PII be used?</p>	<p>The PII in the DART Drive and CTS is used to record, track, document, and report on work-related injury or illness involving ORNL employees and subcontractors in accordance with the requirements of DOE O 231.1B.</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>



MODULE II – PII SYSTEMS & PROJECTS

<p>13. With what other agencies or entities will an individual's information be shared?</p>	<p>This information will be shared within DOE. As necessary, information may be shared with other agencies or entities as permitted by the applicable SORN cited below.</p> <p>Department of Energy Privacy Act of 1974; Publication of Compilation of Privacy Act Systems of Records 74 FR 993, January 9, 2009. DOE-38, Occupational and Industrial Accident Records Pages 993-1090</p>
<p>Reports</p>	
<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>Reports are produced from CTS that display the injury/illness cases and rates over specified time periods (e.g. by month, by fiscal year, etc.). The reports only contain aggregated data and do not include individual identifiers.</p>
<p>15. What will be the use of these reports?</p>	<p>The reports are used to track injury/illness cases at ORNL.</p>
<p>16. Who will have access to these reports?</p>	<p>The reports are provided to DOE on a monthly basis and to division/directorate management on a need-to-know basis.</p>
<p>Monitoring</p>	
<p>17. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>No.</p>
<p>18. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>N/A.</p>
<p>19. Are controls implemented to prevent unauthorized monitoring of individuals?</p>	<p>N/A.</p>

DATA MANAGEMENT & MAINTENANCE



MODULE II – PII SYSTEMS & PROJECTS

<p>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.</p>	<p>For the records on the DART drive, the records stay open for 5 years or until injury or treatment is completed (i.e. after a combined 180 days of lost work/restricted days). During this time, additional medical treatment information is collected from ORNL Health Services and the records are updated accordingly.</p> <p>For CTS, demographic and employment data are updated weekly via a weekly, one-way feed from ORNL’s enterprise data repository (SAP) to keep the information updated, accurate, and complete.</p>
<p>21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?</p>	<p>N/A – only operated at ORNL.</p>
<p>Records Management</p>	
<p>22. Identify the record(s).</p>	<p>Title: Occupational and Industrial Accident Records Maintained in CTS-ISIS (SOR) DOE-38</p> <p>Description: Injury/illness records maintained in Comprehensive Tracking System -Industrial Safety Information System (CTS-ISIS), includes motor vehicle, and property damage data documenting injury/illness data in compliance with the OSHA Act and recordkeeping regulations in 29 CFR 1904 and 1952. System creates OSHA 200 Log and 300 Log, DOE Accident/Incident Reports (form 5484.3), performance indicator reports, and trending data reports.</p>
<p>23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.</p>	<p><input type="checkbox"/> Unscheduled <input checked="" type="checkbox"/> Scheduled (cite NARA authority(ies) below)</p> <p>DOE2.4-100 Workers Compensation (Personal Injury Compensation) Records; Case files on injuries employees sustain while performing their duties that result in lost time or death, whether or not the employee filed a workers’ compensation claim. Includes:</p> <ul style="list-style-type: none"> • forms, reports, correspondence, claims • medical and investigatory records • administrative determinations or court rulings • payment records <p>Temporary. Destroy 250 years after compensation is terminated or when deadline for filing claim has passed. (DAA-0434-2020-0013-0002) [Note retention increased from 75-years per DOE RDS]</p> <p>***Note that these types of records are currently in a frozen disposition authority under Department of Energy epidemiological moratorium on the destruction of health-related records.***</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>24. Records Contact</p>	<p>Gayla Creasey creaseygd@ornl.gov 865-576-8788</p>
<p>ACCESS, SAFEGUARDS & SECURITY</p>	
<p>25. What controls are in place to protect the data from unauthorized access, modification or use?</p>	<p>CTS/DART both reside in the <i>Servers Enclave</i>, which 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 <i>Unclassified Cyber Security Program Plan (CSPP)</i>, and the <i>Servers Enclave System Security Plan (SSP)</i> describe the technical, operational, and management controls to secure this Information System at a Moderate level.</p>
<p>26. Who will have access to PII data?</p>	<p>CTS/DART- Only those staff that have a valid need to know to access this information.</p>
<p>27. How is access to PII data determined?</p>	<p>CTS- On a need-to-know basis only approved by the responsible person or manager. Access to CTS is granted on an individual basis and controlled through a SAP role.</p> <p>DART- On a need-to-know basis only approved by the responsible person or manager. DART utilizes Active Directory groups to grant access.</p>
<p>28. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>CTS- Yes. Enterprise data from ORNL SAP containing employee and non-employee information is imported into the system via a weekly, one-way feed (see answers to questions 8 and 20 for more information).</p> <p>DART- No.</p>
<p>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?</p>	<p>CTS- There are no persistent connections between the CTS and other entities. Any data exchange will implement processes and requirements required for handling, storing, and transmitting PII and sensitive information as defined in ORNL Standards Based Management System (SBMS) requirements for handling sensitive information.</p> <p>DART- N/A.</p>
<p>30. Who is responsible for ensuring the authorized use of personal information?</p>	<p>CTS- Health & Safety Professional – Programs.</p> <p>DART- Health & Safety Specialist controls access.</p>



MODULE II – PII SYSTEMS & PROJECTS

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
<p>System Owner</p>	<p>_____</p> <p>(Print Name)</p> <p><i>Jagom</i></p> <p>Date: 2023.09.25 15:35:42 -06'00'</p> <p>_____</p> <p>(Signature)</p>	<p>_____</p>
<p>Local Privacy Act Officer</p>	<p>_____</p> <p>(Print Name)</p> <p>Linda Chapman</p> <p>Digitally signed by Linda Chapman Date: 2023.09.11 09:09:22 -04'00'</p> <p>_____</p> <p>(Signature)</p>	<p>_____</p>
<p>Ken Hunt Chief Privacy Officer</p>	<p>_____</p> <p>(Print Name)</p> <p>William K. Hunt</p> <p>Digitally signed by William K. Hunt Date: 2023.09.08 11:27:19 -04'00'</p> <p>_____</p> <p>(Signature)</p>	<p>_____</p>