



Affects Members Of the Public?	<input checked="" type="checkbox"/>
--------------------------------	-------------------------------------

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	01/26/2022	
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	Digital storage and management of information associated with DOE-77, Physical Fitness Test 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.)	Richard A. Harkleroad, CISSP CISA ORNL Security Controls Assessor UT-Battelle, LLC Contractor to the US Department of Energy	(865) 385-0068 harkleroadr@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	This information system is used to store and report on physical fitness test records for protective force personnel at Oak Ridge National Laboratory (ORNL). 10 CFR 1046 establishes medical, physical readiness, training, and performance standards for contractor protective force personnel who provide security services at DOE facilities. It further requires a designated physician to regularly evaluate protective force personnel against these standards. This information system collects the results of the required physical fitness testing for DOE contractor employees on the protective force at ORNL.	
Type of Information Collected or Maintained by the System:	<input type="checkbox"/> SSN <input checked="" type="checkbox"/> Medical & Health Information <input type="checkbox"/> Financial Information <input type="checkbox"/> Clearance Information <input type="checkbox"/> Biometric Information <input type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> DoB, Place of Birth <input type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input checked="" type="checkbox"/> Name, Phone, Address <input checked="" type="checkbox"/> Other – (Badge Number, Gender, Age)	



MODULE I – PRIVACY NEEDS ASSESSMENT

<p>Has there been any attempt to verify PII does not exist on the system?</p> <p>DOE Order 206.1, <i>Department of Energy Privacy Program</i>, 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.</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>

Threshold Questions

<p>1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?</p>	<p>YES</p>
<p>2. Is the information in identifiable form?</p>	<p>YES</p>
<p>3. Is the information about individual Members of the Public?</p>	<p>YES</p>
<p>4. Is the information about DOE or contractor employees?</p>	<p>YES</p> <p><input type="checkbox"/> Federal Employees</p> <p><input checked="" type="checkbox"/> Contractor Employees</p>

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.



MODULE I – PRIVACY NEEDS ASSESSMENT

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>10 CFR 1046 requires the collection and retention of physical fitness test records for contractor protective force personnel who provide security services at DOE facilities. 10 CFR 1046.20 specifically requires these records be maintained in accordance with the appropriate DOE Privacy Act System of Records.</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>Protective force personnel are required to provide this information by 10 CFR 1046 and DOE O 473.2A. Failure to provide this information would disqualify an individual from employment. There is currently no formalized opportunity for an individual to consent to uses of information beyond what is required or authorized.</p>
<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>



MODULE II – PII SYSTEMS & PROJECTS

<p>4. IMPACT ANALYSIS: How does this project or information system impact privacy?</p>	<p>DOE has assessed the Physical Test Records system as a moderate risk system for confidentiality, integrity, and availability. This information system collects personally identifiable information (PII) including name (full and partial), age, gender, and related medical and health information from ORNL’s protective force personnel. Additionally, the collection of this information has been identified by DOE as a Privacy Act System of Record (DOE-77, Physical Fitness Test Records).</p> <p>Physical Fitness Test Records is 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>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.</p>	<p>Yes, the data can be retrieved by searching by unique identifiers of individuals. The data is retrievable by the following identifiers: name and badge number.</p>
<p>6. SORNs Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>? 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. DOE-77 Physical Fitness Test Records. Pages 993-1090</p>
<p>7. SORNs 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 subjects, physicians, and persons administering the physical fitness testing.</p>
<p>9. Will the information system derive new or meta data about an individual from the information collected?</p>	<p>No, however, individual data sets are manually aggregated for reporting purposes.</p>
<p>10. Are the data elements described in detail and documented?</p>	<p>Yes.</p>

DATA USE

<p>11. How will the PII be used?</p>	<p>Information is maintained and used to record and evaluate the physical fitness of protective force personnel to satisfy bi-annual testing requirements.</p>
<p>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?</p>	<p>The system does not derive meta data.</p>
<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-77 Physical Fitness Test Records. Pages 993-1090</p>

Reports

<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>Administrative reports are produced for use by the medical professionals conducting the physical fitness testing and the appropriate personnel from Medical Services to facilitate compliance with the physical fitness testing and certification requirements of 10 CFR 1046 and DOE O 473.2A. Additionally, de-identified, aggregated reports are produced to convey overall status of compliance with these requirements to limited, appropriate management personnel.</p>
---------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



MODULE II – PII SYSTEMS & PROJECTS

<p>15. What will be the use of these reports?</p>	<p>The administrative reports are used to evaluate and certify the physical fitness of protective force personnel. These reports are also used to identify fitness trends over time. The de-identified, aggregated reports are used to convey overall status of compliance with the testing and certification requirements of 10 CFR 1046 and DOE O 473.2A to limited, appropriate management personnel.</p>
<p>16. Who will have access to these reports?</p>	<p>Medical professionals conducting the physical fitness testing and appropriate personnel from Medical Services will have access to the administrative reports that are not de-identified. Limited, appropriate management personnel will have access to the de-identified, aggregate reports. Given the relatively small sample size, the de-identified, aggregated reports may not be considered truly anonymized, so access to both types of report is limited to the minimum personnel necessary to fulfill the requirements of 10 CFR 1046 and DOE O 473.2A.</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 – system does not have monitoring capabilities.</p>
<p>DATA MANAGEMENT & MAINTENANCE</p>	
<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>Data is collected at a single-point and pertains only to the standardized format, not allowing for unrelated information. Information is reviewed annually and updated, as needed. System is controlled and limited to small party of users accessing information.</p>



MODULE II – PII SYSTEMS & PROJECTS

<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>The information system is only used at ORNL.</p>
<p>Records Management</p>	
<p>22. Identify the record(s).</p>	<p>Protective Force physical fitness test records.</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 (<i>cite NARA authority(ies) below</i>)</p> <p>DOE Admin 1: 1.1 M&O Contractor Employee Files - NARA Approval Authority N1-434-89-1(1)</p>
<p>24. Records Contact</p>	<p>Missy Baird bairdmh@ornl.gov 865-574-6753</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>The Unclassified Cyber Security Program Plan (CSPP) for ORNL is based on the DOE Office of Science Cyber Security Program Plan (CSPP) and implements the technical, operational, and management controls to secure this Information System at a Moderate level. 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 Servers and Workstations Information Systems, where this system resides, operates under a current DOE granted Authority to Operate (ATO).</p>
<p>26. Who will have access to PII data?</p>	<p>Approved and authorized medical professionals conducting and reporting on the physical fitness testing. Level of access is granted through evaluation of need to know, review of requested purpose for access, and ORNL management approvals of the request.</p>




MODULE II – PII SYSTEMS & PROJECTS

<p>27. How is access to PII data determined?</p>	<p>Access is intended only for medical professionals conducting and reporting on the physical fitness testing. 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.</p>
<p>28. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>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>N/A.</p>
<p>30. Who is responsible for ensuring the authorized use of personal information?</p>	<p>The ORNL Information System Owner (ISO) / Designee(s) of the system.</p>

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
<p>System Owner</p>	<p>_____</p> <p>(Print Name)</p> <p> Date: 2022.10.29 18:58:24 -04'00'</p>	



PRIVACY IMPACT ASSESSMENT: Oak Ridge National Laboratory – DOE-77 SOR
PIA Template Version 5 – August 2017

	(Signature)	
<p>Local Privacy Act Officer</p>	<hr/> <p style="text-align: center;">(Print Name)</p> <p>Linda Chapman</p> <hr/> <p style="text-align: center;">(Signature)</p>	<hr/>
<p><i>Ken Hunt</i> Chief Privacy Officer</p>	<hr/> <p style="text-align: center;">(Print Name)</p> <p>William K. Hunt</p> <hr/> <p style="text-align: center;">(Signature)</p>	<hr/>