



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	06/09/2022	
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	Personnel Access System (PAS)	
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.)	Brian Brown ORNL Security Controls Assessor UT-Battelle, LLC Contractor to the US Department of Energy	(865) 574-8688 brownbg@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>PAS is an information system at ORNL associated with the following Department of Energy (DOE) Systems of Record: <i>DOE-51, Employee and Visitor Access Control Records</i> and <i>DOE-52, Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites</i>. PAS is used to create and maintain site access control records for employees, non-employees (e.g. visitors, contractors), and foreign nationals who access ORNL facilities. Specifically, PAS is used to register, manage, track, document, and report on employee, non-employee, and foreign national access to ORNL facilities.</p> <p>PAS is one of the systems at ORNL used to manage access to the Lab. Prior to accessing ORNL campus, facilities, or information, an individual must first be registered and approved in the PAS system. PAS “tracks” an individual’s access to ORNL in that it maintains a record of a given individual’s registration/approval to access ORNL, but there is no active tracking in PAS beyond that. Ad-hoc reports are occasionally used for data analysis as necessary for ORNL to comprehensively manage site access and security and fulfill the requirements of DOE O 142.3B and DOE O 473.1A.</p>	
Type of Information Collected or Maintained by the System:	<input checked="" type="checkbox"/> SSN (last 4) <input checked="" type="checkbox"/> Medical & Health Information <input type="checkbox"/> Financial Information <input type="checkbox"/> Clearance Information <input checked="" type="checkbox"/> Biometric Information (Badge photo) <input type="checkbox"/> Mother’s Maiden Name	



MODULE I – PRIVACY NEEDS ASSESSMENT

- DoB, Place of Birth
- Employment Information
- Criminal History
- Name, Phone, Address
- Other – (Passports, VISAs, emergency contact name and phone number, email address)

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

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 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?

DOE O 142.3B defines the requirements for unclassified foreign national access to all DOE sites. Among other things, DOE O 142.3B requires: (1) a risk-based review and approval process for foreign national access for ORNL and (2) a process for documenting and tracking access by foreign nationals to ORNL. DOE O 473.1A defines site-specific requirements and procedures for receiving and escorting visitors and requirements for security badges to be used to support physical access control operations at DOE facilities. In order to meet the requirements of these orders, ORNL uses PAS to collect and retain the personal information of employees, non-employees (e.g. visitors, contractors), and foreign nationals who access ORNL facilities.



MODULE II – PII SYSTEMS & PROJECTS

<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>Failure to provide this information would disqualify an individual from accessing ORNL facilities. 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 142.3B and DOE O 473.1A.</p>
<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>DOE has assessed PAS as a moderate risk system for confidentiality, integrity, and availability. PAS collects personally identifiable information (PII) including the types of PII indicated on page 2 of this assessment. Additionally, the federal information collected and maintained by PAS has been identified by DOE as a Privacy Act System of Record (DOE-51, Employee and Visitor Access Control Records and DOE-52, Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites.</p> <p>PAS 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</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 by the following identifiers: badge number, name, last 4 of SSN, date of birth.</p>



MODULE II – PII SYSTEMS & PROJECTS

<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. DOE-51, Employee and Visitor Access Control Records and DOE-52, Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites. 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

<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>The employees, non-employees (e.g. visitors, contractors), and foreign nationals requesting access to ORNL facilities are the sources of information—the personal information in PAS is collected directly from the individuals by ORNL.</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>

DATA USE

<p>11. How will the PII be used?</p>	<p>PII is used to document, track, manage, analyze, report on, and control access to ORNL facilities by employees, non-employees, and foreign nationals to meet the requirements of DOE O 142.3B and DOE O 473.1A.</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 SORNs 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-51, Employee and Visitor Access Control Records and DOE-52, Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites. 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>PAS does not produce standard reports. Ad-hoc reports about individuals may be produced in response to requests by authorized ORNL management personnel.</p>
<p>15. What will be the use of these reports?</p>	<p>Ad-hoc reports will be used for data analysis as necessary for ORNL to comprehensively manage site access and security and fulfill the requirements of DOE O 142.3B and DOE O 473.1A.</p>
<p>16. Who will have access to these reports?</p>	<p>Limited, authorized ORNL personnel as necessary to comprehensively manage site access and security and fulfill the requirements of DOE O 142.3B and DOE O 473.1A.</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>System entries have a standardized format and are time limited. After an access request expires, a new request must be submitted, which requires verification of all PII data previously collected.</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.</p>
<p>Records Management</p>	
<p>22. Identify the record(s).</p>	<p>DOE 51 – Title: Employee and Visitor Access Control Files (SOR) DOE-51 Description: Visitor Registers, Foreign National Pink Cards, Visitor Access Control Records, Special Visitors and Group Tours Records, Non-citizen visitor approval cards This has been identified as a System of Records (SOR).</p> <p>DOE 52 – Title: Foreign National Assignments Files (SOR) DOE-52 Description: Foreign National Assignments files with PAS request, approvals, host report, VISA information for length of work assignment. This has been designated as a System of Record (SOR).</p>
<p>23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.</p>	<p>Check appropriately and cite as required.</p> <p><input type="checkbox"/> Unscheduled <input checked="" type="checkbox"/> Scheduled (cite NARA authority(ies) below)</p> <p>DOE-51 and DOE-52 are both scheduled under this citation</p> <p>DOE Admin 18:17.1a Files retained by sites (incoming visitor control) with potential for exposure to hazardous material. (N1-434-98-21(17.1a))</p> <p>Retention: Cut off at the end of the fiscal year. Destroy 75 years after cutoff.</p>
<p>24. Records Contact</p>	<p>Missy Baird bairdmh@ornl.gov 865-574-6753</p>



MODULE II – PII SYSTEMS & PROJECTS

ACCESS, SAFEGUARDS & SECURITY

<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>Authorized security, administrative, and technical support personnel whose official duties require access to the data.</p>
<p>27. How is access to PII data determined?</p>	<p>Level of access is determined through job or role-based authorization, and is only granted on a need to know basis.</p>
<p>28. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>PAS transmits encrypted PII to ORNL's Site Access Control System (SACS). Transmission of PII between systems is necessary for ensuring only approved and vetted individuals with a valid need-to-know gain access to the laboratory and the associated resources involved with both PAS and SACS.</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 – ORNL Information Systems only.</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



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

	Signature	Date
System Owner	<hr/> <p>(Print Name) Date: <i>Jogom</i> 2022.10.29 19:04:59 -04'00'</p> <hr/> <p>(Signature)</p>	<hr/>
Local Privacy Act Officer	<hr/> <p>(Print Name) Digitally signed by Linda Chapman Date: 2022.10.17 15:56:32 -04'00'</p> <hr/> <p>(Signature)</p>	<hr/>
Ken Hunt Chief Privacy Officer	<hr/> <p>(Print Name) Digitally signed by William K. Hunt Date: 2022.08.29 13:33:59 -04'00'</p> <hr/> <p>(Signature)</p>	<hr/>