Affects Members Of the Public? ☐

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT		
Date	8/15/2023	
Departmental Element & Site	Department of Energy Office of Science (SC) Princeton Plasma Physics Laboratory (PPPL) Princeton, NJ	
Name of Information System or IT Project	Oracle Financial SaaS System, part of the PPPL Increased Control IT FISMA System.	
Exhibit Project UID	Contract Number DE-AC02-09-CH11466 with Princeton University for the Operation of the Princeton Plasma Physics Laboratory.	
New PIA [X] **Update** [ ]	New	
	Name, Title	**Contact Information Phone, Email**
System Owner	Jaclyn Pursell, Director, Strategic Business Planning, Analysis and Compliance, PPPL	609-243-3532 jpursell@pppl.gov
Local Privacy Act Officer	Miriam Bartos Privacy Act Officer, DOE SC ISC-CH	(630) 252-2041 miriam.bartos@science.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Jim Hirsch PPPL Chief Information Security Officer	(609) 243-3388 jhirsch@pppl.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Jim Hirsch PPPL Chief Information Security Officer	(609) 243-3388 jhirsch@pppl.gov
Purpose of Information System or IT Project	The Oracle Financial SaaS System is an automated, web-based financial system used to manage enterprise functions such as accounting, budgeting, labor distribution, project costing, procurement, and materials management. Financial transactions are recorded in the system and ultimately reported to DOE through STARS reporting. Oracle contains contractor-owned and operated PII used for payroll and transaction processing. This PII is accessible exclusively to the contractor; DOE cannot directly access the PII. Oracle contains non-PII DOE financial information maintained by the contractor, which DOE may obtain via request by way of external information sharing.	
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: • General financial information • Supply chain management information • Procurement information • Projects management information • Other personnel/HR information	

MODULE I – PRIVACY NEEDS ASSESSMENT

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.*	The system contains PII.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Not applicable

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?	No
4. Is the information about DOE or contractor employees?	Yes ☐ Federal Employees ☒ Contractor Employees

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

MODULE II – PII SYSTEMS & PROJECTS	
1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	This system contains government-owned financial non-PII and contractor-owned PII. Because there is a component of government-owned information on this system, the system itself is a federal information system with collection of that information authorized under the Department of Energy Organization Act 5 USC Section 301 and 42 USC Section 7101. However, the PII portion of the information is contractor-owned and collection of that PII is therefore authorized by the contractor.
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)?**	If an individual is a DOE PCard (credit card) holder, the card information must be provided as a requisite of card use. In addition, employee information is required for all employees with labor processed in the Oracle Financial SaaS system.
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?**	The M&O Contractor is involved with the design, development, and maintenance of the system. DOE O 206.1 CRD and the Privacy Act clause are currently in the M&O contract.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	Contractor PII is collected and maintained in the system by and for the contractor. A compromise of employment PII could have a moderate impact on privacy resulting in personal, professional, or financial harm to individuals. All PII in this system is contractor-owned. DOE does not have direct access to PII in Oracle. In addition, the system observes a number of protections in contemplation of the Fair Information Practice Principles. The system maintains only required PII for particular authorized uses in observation of data minimization, purpose specification, and use limitation. The system implements a series of administrative and technical controls to further data quality and security.

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.**	The system contains exclusively contractor PII which is retrievable by unique identifier by and for the contractor. DOE cannot and does not retrieve PII in Oracle.
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*.**	The system does not require a SORN because the PII is contractor-owned and operated; DOE cannot retrieve PII in the system.
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 information is obtained from the individual, may be pre-populated from existing organizational data, or may be fed into the Oracle system from the Princeton University PeopleSoft system.
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, detailed data elements are documented and were reviewed during system development and during cyber security impact assessment.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	Contractor credit card transaction processing and payroll.
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?	None
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports include labor history reports and payroll reports.
15. What will be the use of these reports?	Projects and lab management use labor history reports to see which projects an employee is charging and the cost. Payroll reports are used by payroll staff to reconcile pay to Princeton University staff payments.
16. Who will have access to these reports?	PPPL staff with a need to know as part of their job role have access to the reports, including payroll staff, budget officer staff, and line managers.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	For the limited use of cyber security purposes, IT system audit logs are maintained to record IT system activity and user activity.
18. What kinds of information are collected as a function of the monitoring of individuals?	For the limited use of cyber security purposes, IT system audit logs are maintained to record IT system activity and user activity. This activity includes invalid logon attempts and access and modification to data in the system.

MODULE II – PII SYSTEMS & PROJECTS	
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Cyber security controls have been implemented in compliance with FedRAMP authorization and standard FedRAMP processes are in place to ensure that controls are operating effectively. Numerous defensive technical and administrative controls are in place to prevent the misuse of data by individuals with access.
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.	The employee information is reviewed for accuracy, relevance, and completeness by appropriate PPPL business operations and IT staff.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A. The information system is operated at only one site.
RECORDS MANAGEMENT	
22. Identify the record(s).	Financial transaction records related to procuring goods and services, bill payment, collecting debts, accounting, budgeting, labor, assets and inventory.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	DOE O 243.1C NARA General Records Schedule GRS 1.1 item 010
24. Records Contact	Svetlana Drapkin, PPPL Controller, sdrapkin@pppl.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	IT systems and data are hosted in a FedRAMP-authorized cloud-based information system with authorized and tested cyber security controls conforming to the NIST 800-53 Rev 4 baseline including password-controlled login, multi-factor authentication, encryption, and numerous defense in depth cyber controls.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	DOE does not have access to PII. PPPL business operations personnel with a need to know in performance of their job responsibilities, including the PPPL Procurement Card Administrator, PPPL IT staff and Oracle support staff.
27. How is access to PII data determined?	Access by PPPL staff is grated on a need to know basis, is determined and authorized by the system owner based on PPPL organizational role, and is restricted to those personnel assigned to the roles designated with this access.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No.
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 system owner, the PPPL Director of Strategic Planning, Analysis and Compliance, is responsible for ensuring the authorized use of personal information. Access control lists are contained with the Oracle cloud software application. PPPL employees are required to sign an annual Commitment to Integrity which includes specific responsibilities for confidentiality and protection of personally identifiable information.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) Jaclyn Pursell Digitally signed by Jaclyn Pursell Date: 2023.09.08 13:59:25 -04'00' (Signature)	
Local Privacy Act Officer	(Print Name) MIRIAM BARTOS Digitally signed by MIRIAM BARTOS Date: 2023.09.11 07:45:59 -05'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.09.08 11:30:34 -04'00' (Signature)	