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	August 2021
Departmental Element & Site	SC/BNL
Name of Information System or IT Project	Human Capital Management System - Workday
Exhibit Project UID	BNL RFP No. 378448
New PIA X **Update**	

	Name, Title	Contact Information Phone, Email
System Owner	Robert Lincoln, Chief Human Resources Officer Thomas Schlagel,	(631) 344-7435 rlincoln@bnl.gov (631) 344-8765

MODULE I – PRIVACY NEEDS ASSESSMENT

	Chief Information Officer	schlagel@bnl.gov
Local Privacy Act Officer	Miriam Bartos	(630) 252-2041 Miriam.bartos@science.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Ian Ballantyne, ISSM	(631) 344-7589 ballant@bnl.gov
Person Completing this Document	Steve Giovine, IT Manager	(631)344-8610 giovine@bnl.gov
Purpose of Information System or IT Project	The Workday HCMS will be used by BSA to manage and administrate all functions of Human Resources and Payroll for its employees. The functions include but not limited to: Talent Acquisition, Employee On-Boarding, Employee Records, Compensation and Benefits, Payroll, Time and Attendance, Performance Management, Succession Planning and Learning Management.	
Type of Information Collected or Maintained by the System:	☒SSN Social Security number ☐Medical & Health Information e.g. blood test results ☒Financial Information e.g. credit card number ☐Clearance Information e.g. "Q" ☐Biometric Information e.g. finger print, retinal scan ☐Mother's Maiden Name ☒DoB, Place of Birth ☒Employment Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐Criminal History ☒ Name, Phone, Address ☐ Other – Please Specify
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.*	**No, this system must collect or maintain PII to perform its function.**
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	**N/A**

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 or NO (If Yes, select with an "X" in the boxes below) ☐ 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 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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	42 USC 7101, Department of Energy Organization Act DOE O 206.1 provides that contractors may collect information about their employees necessary to carry out activities for DOE's mission.
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)?**	Collection of the information is voluntary. However, failure to provide the necessary employment information may result in the termination of employment.

MODULE II – PII SYSTEMS & PROJECTS	
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 Contractors operate this system, and the Department of Energy Privacy Program CRD and Privacy Act clauses are included in the prime contract.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The collection of personal information is relevant to the business of the Lab functions such as payroll and other HR related functions. Access permissions provide the necessary system restrictions based on "need-to-know".
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.**	No SORN is applicable. This system only contains PII of individuals employed by or seeking employment by the contractor, and thus, the information is contractor-owned and not subject to the Privacy Act.
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*.**	No SORN is applicable. This system only contains PII of individuals employed by or seeking employment by the contractor, and thus, the information is contractor-owned and not subject to the Privacy Act.
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	

MODULE II – PII SYSTEMS & PROJECTS	
8. What are the sources of information about individuals in the information system or project?	All data is individual-provided.
9. Will the information system derive new or meta data about an individual from the information collected?	No. The system will not derive new or meta data.
10. Are the data elements described in detail and documented?	No, Workday does not use a relational database, most data fields and relationships are configured according to customer requirements.
DATA USE	
11. How will the PII be used?	Departments with a "need-to-know" use the data to perform relevant HR business processes required by the Laboratory.
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 – System does not derive meta data.
13. With what other agencies or entities will an individual's information be shared?	Information will be shared for all required state and local filings for HR transactions and any required filings from the Department of Energy.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Personnel, Benefits and Compensation, Diversity, Salary, Training, Talent Acquisition.
15. What will be the use of these reports?	Management of HR functions at the Laboratory.
16. Who will have access to these reports?	Database Administrators, individuals from the HR, Financial, or Medical departments with role based permissions granted from senior management to access the data based on a "need-to-know".

MODULE II – PII SYSTEMS & PROJECTS	
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. This system does not monitor individuals.
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.	The records kept on individuals are kept current by the respective departments responsible for the information. Personal HR and Financial information is available online for review and revision as appropriate by the individual to whom the record pertains.
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
Records Management	
22. Identify the record(s).	Personnel, Compensation and Benefits, Diversity, Salary, Training, Talent Acquisition.

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	DOE RDS 2.1/ GRS 2.1 Employee Acquisitions DOE RDS 2.2/GRS 2.2 Employee Management DOE RDS 2.3/GRS 2.3 Employee Relations Records DOE RDS 2.4/GRS 2.4 Employee Compensation and Benefits GRS 2.5 Employee Separation Records DOE RDS 2.6 Employee Training
24. Records Contact	Patricia Garvey – Records Management Manager (631) 344-6062 pgarvey@bnl.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The SaaS vendor (Workday) has begun their FedRAMP certification process and maintains their systems at a level that meets/exceeds NIST 800-53 Moderate-level system control requirements. Access permissions are based on “need-to-know”.
26. Who will have access to PII data?	Database Administrators, individuals from the HR, Financial, or Medical departments with role based permissions granted from senior management to access the data based on a “need-to-know”.
27. How is access to PII data determined?	Role-based permissions are granted from senior management to access the data.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. A subset of this information is exported into a data repository in BNL's Protected Core for use by other BNL applications. BNL’s Protected Core is specifically architected to support the storage and transmission of PII. The information exported includes first and last name, employee number, supervisor's employee number, department, work email, work phone, work location (building, street number), employment status (active, inactive), citizenship, birth country, home zip code, and termination date. The general work-related contact information and employment status may be used by various BNL applications for generating up to date contact lists, automating emails, etc. The other information is more tightly controlled and used by a small number of BNL applications for computing account and access control purposes.

MODULE II – PII SYSTEMS & PROJECTS	
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?	There are no Interconnection Security Agreements (ISA) in place at BNL.
30. Who is responsible for ensuring the authorized use of personal information?	Role-based permissions are granted from senior management to access the data based on “need-to-know”.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	Robert Lincoln Thomas Schlagel Robert P. Gordon **(Print Name)** DocuSigned by: Robert Lincoln E66A9FEB841447D... DocuSigned by: Thomas Schlagel D6AC1986E73240D... ROBERT GORDON Digitally signed by ROBERT GORDON Date: 2021.11.15 16:58:48 -05'00' **(Signature)**	10/25/2021
Local Privacy Act Officer	Miriam R. Bartos **(Print Name)** Miriam Bartos Digitally signed by Miriam Bartos Date: 2021.11.29 12:44:07 -06'00' **(Signature)**	11/29/21
Ken Hunt **Chief Privacy Officer**	**(Print Name)** **(Signature)**	