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	07/15/2022	
Departmental Element & Site	Bonneville Power Administration – Headquarters Portland, Oregon	
Name of Information System or IT Project	Occupational Safety & Health Information System (OSHIS) – Cority EHS BAE-GSS	
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions	
New PIA □ **Update** ☒	This is an update to the PIA from July 12, 2018. This update further explains Incident Reporting, Contractor Incidents and Ocupational Health.	
	Name, Title	**Contact Information Phone, Email**
Information System Owner	Yvette Gill Supervisory IT Specialist	(503) 230-3947 yrgill@bpa.gov
Information Owner	Jennifer Rehbein, NFO Safety & Occupational Health Manager	360.418.2390 jlrehbein@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Candice Palen, CGI FOIA/Privacy Act Officer	(503-230-3602) cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Nick Choi, JS Information Systems Security Officer	503.230.5397 hcchoi@bpa.gov
Person Completing this Document	Erik Hagelstein, NFO Safety and Occupational Health Specialist Jennifer Rehbein, CGI Director of Corporate Safety	360.418.8541 ethagelstein@bpa.gov 360.418.2390 jlrehbein@bpa.gov
Purpose of Information System or IT Project	OSHIS is a centralized, third party, cloud-based application and the system of record for all things safety-related at BPA. This one-stop system allows information to flow between programs to clarify program status, automate notices and reminders, and provide comprehensive metrics to track progress and identify trends. The OSHIS software provides BPA the ability to efficiently manage an Occupational Safety and Health Program that exceeds OSHA requirements and meets the ANSI Z10 standards for a Safety Management System. The system is used for: **Incident Reporting:** Providing Federal (BFTE) and Supplemental Labor (CFTE) a way to report incidents and identified hazards. Incident reports are used to create short and long-term corrective actions, identify hazards at BPA, stand up Incident Assessment Teams (IAT), and fulfill regulatory reporting requirements. Reporting types include: • Occupational Injuries and Illness • Near Hits and Safety Concerns • Motor Vehicle and Mobile Equipment incidents The System collects all details (submitted by reporter) and any additional documentation (e.g. pictures, statements, etc.) related to the incident. **Contractor Incidents:** Providing BPA a way to capture and store incident data for contractors working on BPA property. Information collected includes name of contract company, incident details, and type of hazard/incident. **Occupational Health:** BPA's Medical Surveillance Program manages positions that have been reviewed and identified as having the potential for an employee exposure to job hazards. Exposure to toxic substances at low levels or for a long period of time may result in long-term, permanent damage to one's health. OSHIS captures and stores mandatory exams and results per regulatory requirements. OSHIS will also be used to capture the name, test date, and test results for individuals who are required	

MODULE I – PRIVACY NEEDS ASSESSMENT

	to test weekly for COVID-19 per DOE guidance and the BPA COVID-19 Screening Testing program. **Industrial Hygiene:** Recording and managing Similar Exposure Groups (SEGs) by conducting exposure monitoring of employees, tasks, and work environments. Data is used to determine what hazards are present and employees are exposed to. As required by regulation, OSHIS is used to store, analyze and manage the reports and results from testing. **Information collected (PII/PHI):** OSHIS has an automatic feed that is sent from HRMIS with employee demographics data (BFTE and CFTE). This data includes: • Employee Name • DOB • Duty Station • Date of hire/termination • HRMIS ID number As part of Occupational Health OSHIS collects and stores Personal Health Information (BFTE Only). This includes: • Results from medical surveillance exams • Health conditions that prevent an employee from doing part or all of a specific job/task. • Health conditions that result from performing a job/task, includes both chronic and acute conditions. As part of the BPA COVID Screening Testing program OSHIS collects and stores information about those individuals who fall under the programs requirements (including employees and contractors (CFTE and non-CFTE)). • Employee Name • Date of test • Results of COVID test **Members of the Public**: No PII or PHI is collected for members of the public.
Type of Information Collected or Maintained by the System:	☐ SSN ☒ Medical & Health Information – Results of pre-hire physical and medical surveillance, including blood test, X-Ray, lung function, audiometric, vision, urinalysis, blood pressure and any medications (prescription and non-prescription). Results of required COVID-19 screening tests.

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☒ DoB ☒ Employment Information - Date of Hire, Date of Termination, Duty Station, Supervisor ☐ Criminal History ☒ Name- Full Name ☒ Other – User E-mail, User Login (only to application), Work Phone Number
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 above-listed PII is known to exist in the system.
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 ☒ Federal Employees ☒ Contractor Employees

MODULE I – PRIVACY NEEDS ASSESSMENT

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

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?**	The Bonneville Power Project Act provides administrative authority to contract to fulfill Bonneville Power Administration's mission. (See 16 U.S.C. § 832a(f); 16 U.S.C.§ 839f(a)). To advance Bonneville's mission and properly maintain occupational safety and health related data consistent with 29 CFR 1960 Occupational Safety and Health Standards, Bonneville has contracted for this software system. As set forth in the January 20, 2021, Executive Order 13991 "Protecting the Federal Workforce and Requiring Mask-Wearing," the policy of the Administration is "to halt the spread of coronavirus disease 2019 (COVID-19) by relying on the best available data and science-based public health measures". This Framework has been developed in accordance with relevant orders and guidance, including: the Office of Management and Budget (OMB) memorandum M-21-15, COVID-19 Safe Federal Workplace: Agency Model Safety Principles, issued January 24, 2021; M-21-25, Integrating Planning for a Safe Increased Return of Federal Employees and Contractors to Physical Workplaces with Post-Reentry Personnel Policies and Work Environment, issued June 10, 2021; Safer Federal Workforce Task Force COVID-19 Workplace Safety: Agency Model Safety Principles, updated September 13, 2021; Executive Order 14042, Ensuring Adequate COVID Safety Protocols for Federal Contractors, signed on September 9, 2021, Executive Order 14043, Requiring Coronavirus Disease 2019 Vaccination for Federal Employees, signed September 9, 2021, and relevant court orders; guidance from the Safer Federal Workforce Task Force; updated U.S. Centers for Disease Control and Prevention (CDC) guidance; Occupational Safety and Health Administration (OSHA) guidelines; and other federal guidance: DOE - Entry Protocols for Onsite Support Service Contractor and Subcontractor Employees – February 10, 2022.
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)?**	Federal regulations require BPA to collect and analyze details about work related injuries and illnesses, medical information on workers who perform certain job functions, exposure-related data to determine any hazards the employee is exposed to on the job, and covid testing results. There is no opportunity for employees or contractors in these particular positions to consent or decline to the collection or use of their information, outside of leaving the position.

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. BPA's privacy clause was included in the contract.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The potential impact is HIGH The loss of confidentiality, integrity, or availability of the data could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

OSH is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls:

- Strict access control enforcement based on need-to-know

This project will move PII information from SharePoint to a more secure system meeting Information Security requirements.

Confidentiality Factors	Low	Moderate	High
Identifiability			X
Quantity of PII		X	
Date Field Sensitivity			X
Context of Use		X	
Obligation to Protect Confidentiality			X
Access to and Location of PII		X	
Overall PII Confidentiality Level			X

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.**	Yes, data will be retrieved by personal identifier. Identifiers include HRMIS ID and name.
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*.**	Yes. This system will contain records from multiple SORNs. • DOE-33 Personnel Medical Records • DOE-34 Employee Assistance Program Records • DOE-38 Occupational and Industrial Accident Records • DOE-77 Physical Fitness Test Records • DOE-88 Epidemiologic and Other Health Studies Located at: Federal Register, Vol 74/No. 6, 1/09/2009, pp. 1008-1090. • OPM/GOVT-10 Employee Medical File Systems Records Located at: Federal Register, Vol. 71/No. 117, 6/19/2006, p. 35360.
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?	**Imported from HRMIS:** Name, DOB, Employee ID #, Hire/Termination Date, BPA e-mail address, duty station **Provided by Safety staff**: job-site data, laboratory reports (industrial hygienist samples or medical laboratories), work related medical and health information, clinic visit results for those in Medical Surveillance and pre-hire physical results if required, and COVID test results. **Provided by individuals:** incident reports, work related medical questionnaire data.

MODULE II – PII SYSTEMS & PROJECTS

9. Will the information system derive new or meta data about an individual from the information collected?	Yes, There is new medical information and derived data from Occupational Health based on testing and medical monitoring. Safety-related information: incident-specific data used in tracking and reporting workplace safety events, injury related incidents, motor vehicle/mobile equipment incidents, and safety concerns.
10. Are the data elements described in detail and documented?	Yes, there is a mapping document that has the data outlined, and data elements are detailed in that document. In addition, there is a solution summary document that illustrates the relationships of the data elements in the system.
DATA USE	
11. How will the PII be used?	PII will be used to document and track employees monitored by the Occupational Safety and Health program and used to manage the process of recognizing hazards, monitoring for health effects, designing controls to mitigate hazards, and assessing the effectiveness of the program. No PII or PHI is collected on members of the public.
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?**	The new data will be used to create, track, and manipulate data to determine work-related risks and exposures to BPA employees. The data will become part of an individual's record.
13. With what other agencies or entities will an individual's information be shared?	Information will be shared with Occupational Safety and Health Administration (OSHA), Department of Labor, and the Department of Energy as required. PII shared includes name and medical information. Some information, including DOB and relevant medical information, may be shared with medical service providers as allowed by law.
Reports	

MODULE II – PII SYSTEMS & PROJECTS

14. What kinds of reports are produced about individuals or contain an individual's data?	OSHA 301 and OSHA 300 log, Medical Surveillance related information, Workplace exposure data collected through Industrial Hygiene monitoring.
15. What will be the use of these reports?	To meet regulatory requirements and generate employee notifications as required.
16. Who will have access to these reports?	BPA Operating Experience Analyst/Program Manager, BPA Industrial Hygienist, and the following who are contractors with BPA: Medical Program Manager, Medical Director. Contractor Safety managers and contractor medical providers may have limited access. Individuals may request access to their own reports.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No
18. What kinds of information are collected as a function of the monitoring of individuals?	None
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.	Subject matter experts with need-to-know access review all incoming reports (medical, injury) and data for accuracy before input into the system. Information about the employee is kept current through a weekly import from HRMIS.

MODULE II – PII SYSTEMS & PROJECTS

21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	System Owners and information owners are responsible for ensuring information is used and managed consistently for its stated purpose in support of the organization. Those with access to the system are trained in the proper use of the information. Access is granted on an as-needed/need-to-know basis and is reviewed at least annually.
Records Management	
22. Identify the record(s).	Work-related medical and health information, clinic site visits, physical results, safety incidents, COVID test results.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 2.7, Item 061 - Occupational individual case files. GRS 2.7, Item 080 - Non-Occupational health and wellness program records GRS 2.7, Item 060 - Occupational individual medical case files GRS 2.7, Items 065 and 066 – Symptom screening and testing records N1-305-07-001-14c - Safety and risk management-related records: ergonomics GRS 5.4, Item 140 - Motor vehicle incidents
24. Records Contact	IGLM@bpa.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The system is certified and operates an information security management system that complies with the requirements of ISO/IEC 27000:2013. The vendor has provided proof of this certification and the assessment report substantiating the security controls for the protection levels for that designated standard. The certificate and the assessment report from an established/recognized 3rd party security assessor has been provided to the office of Cyber Security for evaluation and evidence based documentation of the controls that are in place.
26. Who will have access to PII data?	Operating Experience Analyst/Program Manager, Industrial Hygienist, Medical Program Manager, Medical Director, and Safety Managers (limited access).
27. How is access to PII data determined?	Restricted Access is controlled through permissions and roles granted by the site Administrators.

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes, OSHIS receives an automated feed from HRMIS that includes Employee Name, DOB, and HRMIS ID number.
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?	Yes, the Interconnection Security Agreements (ISA) outline the responsibilities and expectations associated with systems interconnection. ISAs have details of the specific security requirements and controls necessary for interconnection and compliance.
30. Who is responsible for ensuring the authorized use of personal information?	Information Owner System Administrator Super User (By module: Occupational Health, Industrial Hygiene and Safety) Control aspect is that any request for adding a new user to the system or adding/enhancing permissions of an existing user will be submitted by electronic or written form to the Information Owner for approval. If approved by the IO the System Admin will provision the user role by and to only the access and areas of the system approved and documented in the request.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) YVETTE GILL Digitally signed by YVETTE GILL Date: 2023.02.13 15:00:06 -08'00' (Signature)	
Information Owner	(Print Name) JENNIFER REHBEIN Digitally signed by JENNIFER REHBEIN Date: 2023.02.16 11:46:17 -08'00' (Signature)	
Local Privacy Act Officer	(Print Name) Candice Palen Digitally signed by Candice Palen Date: 2023.02.16 12:53:07 -08'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.01.20 09:24:37 -05'00' (Signature)	