



Affects
 Members
 Of the Public?

Department of Energy

Privacy Impact Assessment (PIA)



MODULE I – PRIVACY NEEDS ASSESSMENT

Date	11/9/2021	
Departmental Element & Site	West Valley Demonstration Project, CH2M HILL BWXT West Valley, LLC (CHBWV) – 10282 Rock Springs Rd, West Valley NY 14171	
Name of Information System or IT Project	Software Configuration Management	
Exhibit Project UID	019-60-02-00-01-5013-00	
New PIA <input checked="" type="checkbox"/>	Software Configuration Management	
Update <input type="checkbox"/>		
	Name, Title	Contact Information Phone, Email
System Owner	Paul Contreras	716-942-4450 Paul.contreras@chbvw.com



MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Michelle Farris Office of Legal Services EMCBC, U.S. Department of Energy	Phone (513) 246-0584 Fax (513) 246-0524 michelle.farris@emcbc.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Corey Chun (ISSM) Business Manager & CFO	716-942-4515 Corey.chun@chbvw.com
Person Completing this Document	Paul Contreras	716-942-4450 Paul.contreras@chbvw.com
Purpose of Information System or IT Project	Tracks software created/procured internally (SQA Database)– specialty apps. The system is not focused on individuals and contains only very limited administrative PII to assist in product tracking.	
Type of Information Collected or Maintained by the System:	<input type="checkbox"/> SSN <input 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 – Please Specify – Listing of software (e.g.; description, operating system), associated documentation, and software custodian.	



MODULE I – PRIVACY NEEDS ASSESSMENT

<p>Has there been any attempt to verify PII does not exist on the system?</p> <p><i>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.</i></p>	<p>NO</p>
--	-----------

<p>If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)</p>	
---	--

Threshold Questions

<p>1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?</p>	<p>Administrative PII only.</p>
<p>2. Is the information in identifiable form?</p>	<p>NO</p>
<p>3. Is the information about individual Members of the Public?</p>	<p>NO</p>
<p>4. Is the information about DOE or contractor employees?</p>	<p><input type="checkbox"/> Federal Employees <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.



MODULE I – PRIVACY NEEDS ASSESSMENT

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

<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>42 USC 7101</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>Information provided is not voluntary but part of the condition of employment. All employees are required to read and sign the Rules of Behavior in which they consent to ... "no expectation of privacy on any information entered, stored, or transferred through CHBWW computers, host systems or networks."</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>NO</p>
<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>The system poses a very low privacy risk in light of the limited administrative data contained within. Should the data be compromised, it would not likely cause harm to individuals. The system observes controls to mitigate risk in observance of the FIPPs.</p>



MODULE II – PII SYSTEMS & PROJECTS

<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>The system contains only administrative PII including names and department. There is no other PII to retrieve.</p>
<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>N/A</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>
<p>DATA SOURCES</p>	
<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>The only PII in the system includes name and department pulled from HR-maintained organizational chart data.</p>
<p>9. Will the information system derive new or meta data about an individual from the information collected?</p>	<p>NO</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>10. Are the data elements described in detail and documented?</p>	<p>NO</p>
<p>DATA USE</p>	
<p>11. How will the PII be used?</p>	<p>The PII (person's name) is used to organize and manage software tracking.</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>N/A</p>
<p>13. With what other agencies or entities will an individual's information be shared?</p>	<p>Information may be shared during the course of assessment conducted with a corporate partner and/or other entity authorized by DOE. .</p>
<p>REPORTS</p>	
<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>Specialized reports may be generated in response to specific data call. Or, generic reports would be produced based on pre-established report query criteria. The report would the software custodian and information regarding the software.</p>
<p>15. What will be the use of these reports?</p>	<p>Data reporting and tracking.</p>
<p>16. Who will have access to these reports?</p>	<p>WVDP Managers and Supervisors, and auditors (internal and external),</p>
<p>MONITORING</p>	
<p>17. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>No, the data is not used to identify, locate or monitor individuals..</p>
<p>18. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>N/A.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>19. Are controls implemented to prevent unauthorized monitoring of individuals?</p>	<p>Access to the database tables/data is restricted to those individuals that have a need to utilize the data for job functions. User authentication is utilized for access to the application.</p> <p>Furthermore, the server housing the data and client workstations are also part of the CHBWV GSS. All security controls for the CHBWV GSS also apply.</p> <p>Access to all information systems (i.e. servers and workstations) which are part of the CHBWV are logged and monitored via a combination of the TripWire product (baseline monitoring) and SolarWinds (log monitoring).</p> <p>Finally the CHBWV GSS has undergone a Mission Information Protections Plan (MIPP) review on an annual basis and has obtained an Authorization to Operate at CHBWV until December 21st, 2023.</p>
---	---

DATA MANAGEMENT & MAINTENANCE

<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>PII information is maintained and updated by Human Resources.</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>The system is operated within only the CHBWV GSS accreditation boundary.</p>

RECORDS MANAGEMENT

<p>22. Identify the record(s).</p>	<p>Information is Documented for the internal department</p> <p>Example Documentation ID: WVNS-SCM-090</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 checked="" type="checkbox"/> <i>Unscheduled</i> <input type="checkbox"/> <i>Scheduled (cite NARA authority(ies) below)</i></p>



MODULE II – PII SYSTEMS & PROJECTS

<p>24. Records Contact</p>	<p>Paul Contreras 716-942-4450 Paul.contreras@chbvw.com</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>CHBWW has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management RMAIP and DOE Directives.</p> <p>Access to the database table/data is restricted to those individuals that have a need to utilize the data for job functions. User credentials are utilized to authenticate to the database. Managers are only given a 1-2 week window to access system to input their recommendations.</p> <p>Access to information systems (servers and workstations) which are part of the CHBWW GSS are logged and monitored through SolarWinds Log and Event Manager.</p> <p>The System Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. CHBWW GSS has undergone a Mission Information Protections Plan (MIPP) review on an annual basis and has obtained an Authorization to Operate until December 21st, 2023. The MIPP audit found CHBWW to have mitigated risk to an acceptable level.</p>
<p>26. Who will have access to PII data?</p>	<p>Persons authorized to access the database will have ability to access the data. Personnel access authorization involves the persons manager, database owner, and ISSM (Form 1626).</p>
<p>27. How is access to PII data determined?</p>	<p>Access is determined through Account Access procedure (CP-115) and is limited/restricted to data needed by individual. Access is controlled both at the application level and network authentication level. Management, Data Owner, and ISSM must approve all requests</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>



MODULE II – PII SYSTEMS & PROJECTS

<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 CHBWW Information System Security Manager (ISSM) and the Quality Assurance Manager. All the access controls listed in CP-115 (account access procedure) have been implemented. This includes the following access controls: AC-1, AC-2, AC-3, AC-5, AC-6, and AC-17.</p> <p>These controls were defined in RMAIP-February2014_EXEC-2013-008183_4. The versions of the controls are provided in Appendix A in RMAIP-February2014_EXEC-2013-008183_4.</p>

END OF MODULE II



SIGNATURE PAGE

	Signature
System Owner	<hr/> <i>Paul Contreras</i> <hr/> (Print Name)
	<hr/> <i>Paul W Contreras</i> <hr/> (Signature)
Local Privacy Act Officer	Michelle Farris <hr/> (Print Name)
	<hr/> <i>Michelle Farris</i> <hr/> (Signature)
Ken Hunt Chief Privacy Officer	<hr/> (Print Name)
	<hr/> (Signature)