Department of Energy

Privacy Impact Assessment (PIA)

Affects Members Of the Public?	

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	CH2M General Support System (GSS) General Purpose Storage (GPS). The GSS consists of several information systems including general storage, database, and general application servers.
Exhibit Project UID	019-60-02-00-01-5013-00
New PIA [X] **Update** [ ]	CH2M General Support System (GSS) General Purpose Storage (GPS).

	Name, Title	Contact Information Phone, Email
System Owner	Paul Contreras	716-942-4450 Paul.contreras@chbwv.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@chbwv.com
Person Completing this Document	Paul Contreras	716-942-4450 Paul.contreras@chbwv.com
Purpose of Information System or IT Project	This PNA is for the Performance Assurance Department general user/departmental files (i.e., excel, access, word, etc.) that reside on General Purpose Storage Servers (GPS) within user home directories (N: drive), shared folders (W: and S: drives), and/or workstations utilized by the department. This data resides in various locations on systems (Servers/Workstations) that could otherwise be deemed part of the CHBWV General Support System (GSS).	
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 – Please Specify - Injury Reports, Performance Assessments, Abestos Certificate	

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

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?**	NO
3. **Is the information about individual Members of the Public?**	NO
4. **Is the information about DOE or contractor employees?**	☒ 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.

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

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	42 U.S.C. 7101
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)?**	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 CHBWV computers, host systems or networks."
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?**	NO
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	Information contained in the GSS is strictly name, phone, address, department, and position only. Information could be used in identity fraud, but risk would be minimal as more PII would be needed.

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.**	GPS contains a mix of excel, word, PDF, and access files. PII is not used to identify files.
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*.**	GPS for Environmental, Health, Safety, and Quality follows our SORN records for our company -wide GSS. DOE-5, Personnel Records of Former Contractor Employees DOE-11, Emergency Operations Notification Call List DOE-14, Report of Compensation DOE-28, General Training Records DOE-38, Occupational and Industrial Accident Reports DOE-52, Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites DOE 55, Freedom of Information Act and Privacy Act Requests for Records DOE-72, The DOE Radiation Study Registry
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?	Source is ESHQ staff members who create data files and place them in general storage areas on the network.

MODULE II – PII SYSTEMS & PROJECTS

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.
DATA USE	
11. How will the PII be used?	The PII is stored from several programs utilized across the ESHQ department. All PII is covered by system-level PIAs which account for their use.
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?	No reports are generated using the GPS
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No, the data is not used to identify, locate, or monitor individuals.

PRIVACY PROGRAM

MODULE II – PII SYSTEMS & PROJECTS

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?	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. 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. 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). 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.
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.	PII is sourced from Human Resources, who are responsible for keeping an accurate record of names.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The system is operated within only the CHBWV GSS accreditation boundary.
RECORDS MANAGEMENT	
22. Identify the record(s).	No physical or electronic records are generated using the GPS.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	N/A

MODULE II – PII SYSTEMS & PROJECTS

24. Records Contact	Mark Rodges 716-942-4303 Mark.Rodges@chbwv.com

ACCESS, SAFEGUARDS & SECURITY

25. What controls are in place to protect the data from unauthorized access, modification or use?	CHBWV has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management RMAIP and DOE Directives. 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. Access to information systems (servers and workstations) which are part of the CHBWV GSS are logged and monitored through SolarWinds Log and Event Manager. 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. CHBWV 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 CHBWV to have mitigated risk to an acceptable level.
26. Who will have access to PII data?	Different users across EHSQ have different levels of access to various data in the GPS. See system-level PIAs for details.
27. How is access to PII data determined?	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
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Information is accessed through various applications.

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?	The GSS accreditation boundary documents cover applications using data stored in GPS.
30. Who is responsible for ensuring the authorized use of personal information?	The CHBWV 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. 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.

END OF MODULE II

SIGNATURE PAGE

	Signature
System Owner	*Paul Contreras* **(Print Name)** *Paul H Contreras* **(Signature)**
Local Privacy Act Officer	Michelle Farris **(Print Name)** *Michelle Farris* **(Signature)**
Ken Hunt **Chief Privacy Officer**	**(Print Name)** **(Signature)**