Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT		
Date	1/09/25	
Departmental Element & Site	OCIO – IM-30. The Hardened Cloud Enclave (HCE) provides a secure cloud-based hosting option available for IM-30 systems requiring a FISMA High environment. HCE is located within the AWS GovCloud with Identity Provider (IDP) in Microsoft Azure Gov, affiliated with DOE OneID.	
Name of Information System or IT Project	Hardened Cloud Enclave (HCE)	
Exhibit Project UID		
New PIA ☐ **Update** ☒	Periodic update.	
	Name, Title	**Contact Information** **Phone, Email**
System Owner	Lili Cameron	202-586-0008 lili.cameron@hq.doe.gov
Cyber Security Expert reviewing this	Eric Fryson IM-32 ISSO	540-642-3534 eric.fryson@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT		
document (e.g. ISSM, CSSM, ISSO, etc.)		
Person Completing this Document	John Devison HCE System Engineering	703-732-5176 john.devison@hq.doe.gov
Purpose of Information System or IT Project	The Hardened Cloud Enclave (HCE) is a FISMA High accredited parent package that allows other FISMA packages to inherit FISMA High controls and support efficient control assessment activities during the A&A process for each system. This efficiency drives more secure solution implementations for AWS-based solutions. HCE provides a secure cloud-based hosting option available for IM-30 systems requiring a FISMA High environment.	
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. fingerprint, retinal scan □ Mother's Maiden Name □ DoB, Place of Birth □ Employment Information □ Criminal History □ Name, Phone, Address ☒ Other – Please Specify User Account data limited to user account authenticators • name (first/last) • gov't email address (used as account ID) • phone numbers if used to register for OTP or virtual MFA tokens)	

Has there been any attempt to verify PII does not exist on the system?	Yes HCE's operational applications and infrastructure have been reviewed. There are no publicly accessible

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.*	applications where PII might be disclosed. There are no applications designed or expected to capture or process user data beyond user account authenticators (usernames (first/last) account ID and gov't email address and phone numbers) which are strictly administrative in nature and use.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Initial and periodic verification by engineers building/operating each application within the HCE system (not counting FISMA subsystems with separate individual PIA)
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

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. Seq.
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)?**	Limited PII is required to create an account for the information system. Individuals who decline to provide the required information will not have accounts created for access to the Hardened Cloud Enclave. Information provided by individuals for HCE accounts will not be used for other purposes.
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 are involved with the development and maintenance of the HCE. Standard Federal Acquisition Regulation (FAR) contractual privacy compliance language is in place and adhered to for all contracts supporting the HCE system. All contractors are held to the Privacy Act clauses and other protection requirements outlined in the DOE Contractor Requirements Documents (CRDs) and contracts.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	Should PII in the system be compromised, it could result in a moderate impact to individuals in light of the low sensitivity of the PII. This information includes username, email address, and any phone numbers the individual may enter. Should this PII be compromised, it could harm the trust between individuals and their employer(s) but should not result in significant harm to either the individuals or to government operations. The system does not pose a privacy risk to members of the public because their PII is not collected by or maintained in the system.
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.**	Data may be retrieved using Lightweight Directory Access Protocol (LDAP) tools. Individuals are assigned User Objects, which include the following attributes: • Name • Username • Email address • Distributed Unique Identifier (DUID) • user Certificate

MODULE II – PII SYSTEMS & PROJECTS

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*.**	To trigger the SORN requirements of the Privacy Act, PII must be retrieved in actual practice by a unique identifier(s) for a purpose beyond the administration of the system. HCE has limited, role-based retrieval of limited PII purely for the administration of the system itself not including investigatory purposes or the business purpose of the system, which is to grant a set of FISMA/FedRAMP High access controls to other systems to promote efficiency.
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?	PII is provided by the individual and is pulled from DOE OneID.
9. Will the information system derive new or meta data about an individual from the information collected?	Limited metadata for the security and administration of the system will be collected from OneID. The system will not derive new or meta data about individuals relating to the business purpose of the system.
10. Are the data elements described in detail and documented?	Yes. Data elements are described as part of the system's assessment for FISMA High ATO accreditation.

MODULE II – PII SYSTEMS & PROJECTS	
DATA USE	
11. How will the PII be used?	PII will be used to create user accounts to grant individuals access to the system. PII will be used exclusively for the administration of the IT system itself and not for the business purpose of the system.
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?**	Metadata will be collected from the DOE OneID information system for the security and administration of the system. Collected information will be a part of the individuals' user object.
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?	Troubleshooting reports include user account data.
15. What will be the use of these reports?	The system may produce troubleshooting reports used to support the administration and security of the system.
16. Who will have access to these reports?	Only users who are members of the HCE_Admins group for the information system will have access to reports.
MONITORING	

MODULE II – PII SYSTEMS & PROJECTS	
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?	N/A
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Role Based Access Controls are in place to prevent unauthorized use of data by limiting access to the system and all data stored in the system
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.	Information is not collected from any sources other than DOE records. Because the limited PII used to create user accounts is provided by individuals, individuals' bear the responsibility of ensuring that their information is current and accurate. Individuals may request to have administrators of the information system make changes to their information.
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 information system is not operated in more than one site.
RECORDS MANAGEMENT	
22. Identify the record(s).	User account credentials, audit logs, access management records.

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 3.2, items 030/031 - system access records GRS 3.2, item 010 – system and data security records GRS 3.1, items 010 & 011 - information technology development records • GRS 6.3, item 020 – enterprise architecture records
24. Records Contact	Steve Arauz Training Specialist U.S. Department of Energy IM-30 Cybersecurity Phone: 571-279-2677 steve.arauz@hq.doe.gov Faiad Shaban Cybersecurity Senior Analyst U.S. Department of Energy IM-32 Cybersecurity 703-457-4903 faiad.shaban@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Role Based Access Controls are in place to prevent unauthorized use of data by limiting access to the system and all data stored in the system.
26. Who will have access to PII data?	Only users who are members of the HCE_Admins group for the information system will have access to the limited PII used for the administration of the system.

MODULE II – PII SYSTEMS & PROJECTS

27. How is access to PII data determined?	Only users who are members of the HCE_Admins group have access to PII for administrative functions. Access to all data on the information system is limited by roles and policies.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	DOE OneID provides the following to the information system.: • First and Last name - incorporated into our Azure Entra ID account object • gov't eMail (lookup) - incorporated into our Azure Entra ID account object • OneID internal user record DUID - incorporated into our Azure Entra ID account object • status of PIV card - ephemeral for confirmation
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?	An ISA with OneID is pending.
30. Who is responsible for ensuring the authorized use of personal information?	The information System Owner is responsible for ensuring the authorized use of personal information.

END OF MODULE II

MODULE II – PII SYSTEMS & PROJECTS

SIGNATURE PAGE

	Signature	Date
System Owner	**Lili Cameron** **(Print Name)** LILI CAMERON Digitally signed by LILI CAMERON Date: 2025.02.04 16:27:50 -05'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**Ken Hunt** **(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2025.01.22 13:00:02 -05'00' **(Signature)**	