Department of Energy
DOE Continuous Mitigation Diagnostic (CDM) Agency Dashboard

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT		
Date	07/3/2023	
Departmental Element & Site	IM-30	
Name of Information System or IT Project	Continuous Mitigation Diagnostic (CDM) Agency Dashboard	
Exhibit Project UID		
New PIA [ ] **Update** [X]	Updated to reflect changes in sensitivity and architecture. See Purpose and Impact sections for more details.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Michael Byers 202-586-4687 Michael.byers@hq.doe.gov IT Program Manager	202-586-4687 Michael.byers@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson Privacy Management and Compliance Officer / DOE IM-42	202-287-5786 Brooke.dickson@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Toni Kelley ISSO	757-724-7105 Toni.kelley@hq.doe.gov
Person Completing this Document	Michael Byers CDM system owner	202-586-4687 Michael.byers@hq.doe.gov
Purpose of Information System or IT Project	The CDM Agency Dashboard is a security system built on the Elastic Search and Kibana and is known as Layer C in the CDM architecture. It receives data from a co-located CDM Enterprise Splunk instance. The CDM Agency Dashboard is a reporting platform that will initially provide access to a 30-day view of DOE Asset Management data and metrics	

MODULE I – PRIVACY NEEDS ASSESSMENT	
	associated with this data. It identifies hardware, software, and security configurations as well as vulnerabilities associated with monitored assets. The dashboard provides a security posture scoring capability for each system, site, and overall, for DOE. Summary data is then sent to CISA to a federal level dashboard. In addition to the summary data, CISA will leverage the Cross Cluster Search (CCS) capability in Elastic to directly connect to the DOE CDM Elastic Instance and perform direct queries against the DOE CDM Dashboard. The CDM Enterprise Splunk serves as the top tier of the multi-tier known as Layer B in the CDM architecture. Splunk is where sensor tool data is collected and prepared for the CDM Agency Dashboard. Within DOE, this will entail a Splunk or other similar tool at the site, one potentially at a program office managed convergence point (i.e., IARC), and the Enterprise Splunk instance IM-30 will house in AWS GovCloud. The accreditation boundary for Splunk is the top tier only. The CDM AD system is unclassified. The CDM AD system processes and/or stores non-sensitive administrative Personally Identifiable Information (PII) such as names of individuals associated with the asset (System Owner, AO, AODR, etc.) and asset Management Data including IP addresses, system names, misconfigurations, system or asset vulnerabilities, software titles, and software versions. The data for the CDM Agency Dashboard will be focused on the asset management data described above. Over time, with additional services received from DHS, the data may grow and expand to include additional cybersecurity data. When it becomes necessary to address this additional data, the proper steps will be taken and the PIA updated to include this data in the CDM Agency Dashboard. Splunk Enterprise will help DOE aggregate, correlate, and analyze terabytes of CDM data and enable the creation of a Master Device Record (MDR). A MDR compiles the data from an agency's hardware, software and configuration management, and vulnerability management tools and brings it into a single, holistic view to provide full visibility into network activities and endpoint behaviors. Additionally, Splunk Enterprise will fully integrate endpoint, user behavior, and event management data and provide an enterprise view for leaders to monitor critical networks, systems, and assets. **Change in Dashboard Architecture** Subsequent to the prior version of the PIA, DOE began working with CISA to establish an ISA to set up what is called "Cross-Cluster Search" or CCS. This is a move for CISA to obtain object level data visibility in the Agency dashboard in addition to and eventually replacing the current summary data push they receive from the dashboard at DOE. CCS is a capability within the Elastic software that the dashboard runs on and requires a direct connection between the Federal Dashboard and the DOE Agency Dashboard allowing CISA to directly query the data in the DOE Dashboard remotely from the Federal Dashboard.
Type of Information Collected or Maintained by the System:	☐ SSN ☐ Medical & Health Information

MODULE I – PRIVACY NEEDS ASSESSMENT	
	☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☐ Name, Phone, Address ☒ Other Authorizing Official, Authorizing Official Designated Representative, System Owner Names. Asset Management Data including names, IP addresses, system names, misconfigurations, vulnerabilities, software titles, and software versions.
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)	N/A
Threshold Questions	
1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	Non-sensitive PII.
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?	☒ Federal Employees ☒ Contractor Employees

MODULE I – PRIVACY NEEDS ASSESSMENT	
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?**	P.L. 106-65, "National Defense Authorization Act [Section 3212(d)], enacted October 1999; Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. Seq.; Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C.
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)?**	The system contains non-sensitive PII used to protect DOE assets and systems. Use of this PII is a requisite of employment and use of DOE systems. Refusal would preclude access to DOE systems.
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 design, development, and maintenance of CDM. Privacy Act compliance clauses are included in all contractor agreements. These require contractors to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The CDM AD system is unclassified. The CDM AD system processes and or stores non-sensitive administrative Personal Identified Information (PII) such as names of individuals associated with the asset in various ways (System Owner, AO, AODR, etc.) asset Management Data including IP addresses, system names, misconfigurations, vulnerabilities, software titles, and software versions. Unauthorized access to this system could allow an adversary to identify targets within the department for potential attack and access to business-related PII to aid an adversary in targeting key individuals associated with these assets through phishing or other similar attacks. The CDM AD system does not intentionally process or store classified information. **Upgrade from Moderate to High** It was assessed that when the CDM dashboard was fully operational and receiving data from the Departmental Elements that higher protections would be needed to address the risk of having all the Department's data aggregated in a single system. However, as IM-30 was pushing to get the dashboard up and running and approved to operate a decision was made by the system owner to start with Moderate, the current assessment level for the previous dashboard, given that there were only two sources of data in the current dashboard at the time and the aggregation argument did not apply yet. The data that is of concern is Asset Management data. Asset data including IP addresses, system names, misconfigurations, vulnerabilities, and software titles and versions. This would allow an adversary the ability to identify targets within the department for potential attack should this system become compromised itself. The change in risk assessment to High reflects the additional sensitivity of data aggregation. **Upgrade of PII from none to non-sensitive PII** When the dashboard was first assessed it was identified that there was no PII that would exist while the system was collecting only Asset Management data. There is a move to collect data for Ongoing Assessment and this would collect Names of individuals within DOE who are associated with the asset in multiple ways. System Owner, AO, AODR, etc. This and the change in focus to identify systems that collect any PII data, even non-sensitive PII, triggered the PIA update. Furthermore, DOE is preparing to begin working on Identity and Access Management which would collect more business associated PII within the dashboard. The system observes the Fair Information Practice Principles (FIPPs) to mitigate risk. As a security system, the core function of CDM AD is to protect data and reduce the opportunities and probability of information compromise in furtherance of data quality and security. The system implements role-based access and technical controls to prevent unauthorized access to further protect data in systems across DOE. The system contains only the (non-sensitive) PII necessary for its purpose in furtherance of data minimization and purpose specification. PII is not used for unauthorized purposes in furtherance of use limitation.

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.**	Queries are focused on assets, not individuals.
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*.**	N/A
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?	The CDM AD system processes and or stores non-sensitive administrative Personal Identified Information (PII) such as names of individuals associated with the asset in various ways (System Owner, AO, AODR, etc.) asset Management Data including IP addresses, system names, misconfigurations, vulnerabilities, software titles, and software versions.
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 elements are described as part of the system's assessment for FISMA High ATO authorization
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	Non-sensitive PII including names of individuals associated with assets (e.g., System Owner, AO, AODR, et al) is contained in the system for ongoing assessment to maintain the security and integrity of DOE assets and systems.
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?**	Meta data includes cyber security related information used for security purposes as previously described. Non-sensitive PII related to assets relevant to cyber security is included.
13. With what other agencies or entities will an individual's information be shared?	The information is provided by DOE Departmental Elements sending the data and may be viewed by authorized individuals within DOE and CISA via cross cluster search.
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Data summary reports for ongoing assessments.
15. What will be the use of these reports?	Reports are used for security posture scoring and are sent to CISA for a Federal-level dashboard.
16. Who will have access to these reports?	Authorized system administrators and security personnel.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system is focused on assets and monitors security data accordingly.
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?	All baseline security controls have been implemented and tested as appropriate to its FIPS categorization in accordance with the Senior DOE Management Program Cyber Security Plan (PCSP) and DOE directives.
DATA MANAGEMENT & MAINTENANCE	

MODULE II – PII SYSTEMS & PROJECTS	
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.	DOE Departmental Elements will maintain data currency through local processes. DOE OCIO will validate data currency via periodic reviews.
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 operates according to DOE cyber security policies and procedures.
RECORDS MANAGEMENT	
22. Identify the record(s).	CDM-AD implements a federal dashboard queriable by CISA and DOE as a reporting platform that provides a holistic view of asset management data and metrics. It identifies hardware, software and security configurations as well as vulnerabilities associated with monitored assets. The dashboard includes a cybersecurity posture score for each system and site. GRS 4.2, item 030; requests (either first-party or third-party) GRS 6.5, item 020; customer/client records GRS 3.2, item 020; narrative reports GRS 3.2, item 036;Cybersecurity event logs
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. □ Unscheduled X Scheduled *(cite NARA authority(ies) below)* GRS 4.2, item 030, DAA-GRS-2016-0002-0002 GRS 6.5, item 020, DAA-GRS-2017-0002-0002 GRS 3.2, item 020, DAA-GRS-2013-0006-0001 GRS 3.2, item 036, DAA-GRS-2022-0005-0002
24. Records Contact	Faiad Shaban faiad.shaban@hq.doe.gov (M) (571) 239-8726 Steve Arauz Steve.arauz@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Administrative controls prevent unauthorized access to the system. Technical controls including specialized triggers ensure that only relevant security data is monitored.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	Authorized system administrators and cyber security personnel.
27. How is access to PII data determined?	Access is granted based on job function.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Many information systems interconnect and share data with this system via Interconnection Security Agreements (ISAs) held by this system. The CISA managed Federal Dashboard also connects to this system for query actions on the data within this system.
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?	Interconnection Security Agreements (ISA) outline the responsibilities and expectations associated with system interconnection. ISAs specify security requirements and controls necessary for interconnection and compliance.
30. Who is responsible for ensuring the authorized use of personal information?	Data Owners are responsible for the information contained in their systems. The System owner is responsible for the authorize use of data in this system.
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	**Michael Byers** _____ **(Signature)**	_____
Local Privacy Act Officer	_____ **(Signature)**	_____
Ken Hunt **Chief Privacy Officer**	_____ **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2024.04.19 08:53:44 -04'00' _____ **(Signature)**	_____