Department of Energy

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	5/2/2023
Departmental Element & Site	OCIO IM-30
Name of Information System or IT Project	Endpoint Detection and Response (EDR)
Exhibit Project UID	
New PIA [X] **Update** [ ]	

	Name, Title	Contact Information Phone, Email
System Owner	Michael Byers 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	brooke.dickson@hq.doe.gov 240-805-8278
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Primary ISSO: Quam Onigbanjo Secondary ISSO: Charlene Kamadeu IM-30 ISSO	Primary ISSO Contact: (609) 947 -5275 Quam.Onigbanjo@hq.doe.gov Secondary ISSO Contact: 571-435-6603 charlene.kamadeu@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Quam Onigbanjo & Charlene Kamadeu	Quam Onigbanjo Contact: (609) 947 -5275 Quam.Onigbanjo@hq.doe.gov Charlene Kamadeu Contact: 571-435-6603 charlene.kamadeu@hq.doe.gov
Purpose of Information System or IT Project	Endpoint Detection Response (EDR) is an IM-30 system that leverages CrowdStrike Falcon Platform, a FedRAMP approved Software-as-a-Service (SaaS) solution. EDR identifies unknown malware, detects zero-day threats, identifies advanced adversaries, and prevents damage from targeted attacks in real-time. Furthermore, EDR is able to identify indicators of comprise and potential attacks to notify DOE EDR administrators and users. Agents will be installed on end-user machines, ensuring availability of network connections so the agents can send event information, adding and/or requesting access to user interfaces and reviewing events through the user interface. EDR will enable DOE EDR administrators and users to monitor security events detected by CrowdStrike Falcon Platform through the web-based user interfaces. DOE EDR administrators and user can also extract event data for incident investigations through Falcon Forensics Collector (FFC); this allows users to review trends, examine a high-level view of telemetry, and gather and analyze multiple artifacts for a single system and timeframe. EDR is not focused on individuals or their personal information. The system monitors event data for covered systems based on security triggers. While the system monitors systems, not individuals, a covered system may be linkable to an individual users based on username if the username contains all or part of the individual's name. The system contains administrative PII for authorized users and administrators including username, work email, and work phone.	
Type of Information Collected or Maintained by the System:	☐ SSN ☐ Medical & Health Information ☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☐ Name, Phone, Address ☒ Other –The EDR system will leverage systems logs with event data which can contain usernames. Work email may also be present.
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.*	NO
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?	NO
4. Is the information about DOE or contractor employees?	☒ 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)?**	The individual may choose not to use the Government system that is being monitored by EDR, but use of certain systems may be a requisite of employment depending on job function.
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 and yes.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	In observance of data minimization, EDR does not contain sensitive PII on individuals and therefore presents a low privacy risk. The system monitors government systems, not individuals, and contains event data for security purposes. EDR poses a privacy risk less than or equal to virtually any government system, as all government systems use EDR or a similar cyber security tool for security purposes. While systems may be linkable to individuals, compromise of the data contained in EDR would not pose significant privacy harm to individuals because it is limited to standard, non-sensitive cyber security data used for the purpose of preventing malware and cyber attacks which is not related to authorized users. Moreover, the business purpose of the system is to mitigate risk of data breach or compromise and therefore poses a net benefit to individuals' privacy interests.
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.**	Log data tied to government systems is used for security purposes as with other IT systems. PII is not retrieved by individual identifier or used for business purposes.
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

MODULE II – PII SYSTEMS & PROJECTS

DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Individual-provided Federal agency issued work contact information.
9. Will the information system derive new or meta data about an individual from the information collected?	Potentially. Meta data would be tied to threat indicators identified by the EDR solution.
10. Are the data elements described in detail and documented?	Yes. See Falcon Events Data Dictionary.
DATA USE	
11. How will the PII be used?	Security-related event data is used to prevent malware and cyber attacks. Administrative PII is used for system access.
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?**	Any meta data derived by the EDR solution would be threat or risk based information associated with government systems. The individual does not have an "individual record" in the EDR system data set.
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?	Reports may be generated relating to a security incident being monitored, tracked, and responded to. Event data is related to government systems but may be linkable to individuals via username.
15. What will be the use of these reports?	Reporting and documenting the Cyber Security Indicators of Compromise and associated incidents.

MODULE II – PII SYSTEMS & PROJECTS	
16. Who will have access to these reports?	Authorized cyber security personnel.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system monitors security event data tied to government systems.
18. What kinds of information are collected as a function of the monitoring of individuals?	Individuals are not monitored, but event data may be linkable to individuals via username.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Administrative controls prevent unauthorized access to the system. Technical controls including specialized triggers ensure that only relevant security data is monitored.
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.	The system does not contain records about individuals. Security event data tied to government systems is tracked for security purposes.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A
RECORDS MANAGEMENT	
22. Identify the record(s).	Public Customer Service Records: GRS 6.5 Customer/client records, item 020 Schedules of Daily Activities: GRS 5.1, item 010 Privacy Act Requests Files: GRS 4.2, item 020

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	☐ Unscheduled ☒ Scheduled GRS 4.2, item 020 DAA-GRS-2016-0002-0001 GRS 5.1, item 010; DAA-GRS-2016-0016-0001 GRS 6.5, item 020; DAA-GRS-2017-0002-0002
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.
26. Who will have access to PII data?	Authorized 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.	No.
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?	N/A
30. Who is responsible for ensuring the authorized use of personal information?	System owner.

MODULE II – PII SYSTEMS & PROJECTS

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) Michael W. Byers Digitally signed by Michael W. Byers Date: 2023.06.29 23:05:56 -04'00' (Signature)	
Local Privacy Act Officer	(Print Name) Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2023.06.28 16:14:34 -04'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.06.22 15:29:48 -04'00' (Signature)	