Affects Members Of the Public? X

Department of Energy

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	09/26/24
Departmental Element & Site	OCIO IM-30
Name of Information System or IT Project	Integrated Joint Cyber Coordination Center (iJC3)
Exhibit Project UID	
New PIA X **Update**	

	Name, Title	Contact Information Phone, Email
System Owner	Lili Cameron IT Project Manager	lili.cameron@hq.doe.gov 202-586-0008
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	ISSO: Quam Onigbanjo	ISSO Contact: (609) 947 -5275 Quam.Onigbanjo@hq.doe.gov
Person Completing this Document	Lili Cameron, James Phongsuwan, Frank Stovicek, and Quam Onigbanjo	Lili Cameron Contact: 202-586-0008 lili.cameron@hq.doe.gov James Phongsuwan Contact: 202-306-8447 james.phongsuwan@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

		Frank Stovicek: frank.stovicek@hq.doe.gov Quam Onigbanjo Contact: (609) 947 -5275 Quam.Onigbanjo@hq.doe.gov
Purpose of Information System or IT Project	The Integrated Joint Cyber Coordination Center (iJC3) system provides automation including Sandbox and Mailparser. These tools do not have any public access (available to authorized internal DOE users only). Sandbox is an automated malware detonation. It allows customers to submit files or URLs to be tested. This system is focused on security data, not individuals, and does not investigate individuals or pursue PII beyond user email addresses for administrative purposes. Security-related PII may be submitted in the form of a malicious file name containing PII or a malicious email address sending phishing attempts. For Sandbox, multifactor authentication will be in place utilizing the Hardened Cloud Enclave (HCE) Identity Multifactor mechanism. Types of Data in Sandbox: • User accounts – User accounts require capturing a government issued email address. This information is collected/shared only for administrative purposes. • File/URL submissions – There is no intentional collection of PII. Users may submit files or URLs they deem potentially malicious. • File/URL content – There is no intentional collection of PII. Users may submit files or URLs they deem potentially malicious. Content is extracted which includes screen captures of a virtual machine opening the file/URL. • Extracted indicators/reports - The file/URL may contain malicious IPs, domains, URLs, and email addresses of malicious actors (e.g., sender email address phishing attempts). The above data types are available to the DOE submitter and iJC3 system administrators. The submitter and system administrators may opt to make the data visible to other DOE users of Sandbox and/or submit the data to other DOE systems for further investigation or awareness. The Mailparser tool works on parsing email to provide alerts to sites and labs of cyber hygiene (identified vulnerabilities) from CISA scanning. Mailparser has no users or web interface. Data received from CISA is parsed and sent to BDP for	

MODULE I – PRIVACY NEEDS ASSESSMENT

	reporting to the respective sites/labs. Type of Data in Mailparser: • Vulnerability data – Public vulnerability information paired with system IP addresses. There is typically no PII in this data.
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 – user email addresses, IP addresses, vulnerability data

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

MODULE I – PRIVACY NEEDS ASSESSMENT

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?	The possibility exists that limited PII might be contained in a user submission, but the system does not seek PII on members of the public.
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.

MODULE II – PII SYSTEMS & PROJECTS	
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)?**	User email is a requisite of use of government 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 development and maintenance of iJC3. Standard Federal Acquisition Regulation (FAR) contractual privacy compliance language is in place and adhered to for all contracts supporting the iJC3 system.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The system poses a low privacy risk in light of the limited, low-sensitivity PII contained within. Compromise of PII in this system would have a limited privacy impact, as PII is limited to user email address and potentially low sensitivity PII contained in malicious file names in keeping with data minimization. Use of PII is limited to authorized security and administrative purposes in keeping with use limitation and purpose specification. Role-based access controls protect the integrity of the system and quality of data. The system produces a net privacy benefit by increasing the integrity of DOE systems and data and reducing the possibility of a data compromise.
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.**	The files/URLs containing malicious IPs, domains, URLs, email addresses of malicious actors (e.g., sender email address phishing attempts) can be submitted to Sandbox. Once collected, it is possible that the data described above could be queried for administrative purposes only by administrators. Identifiers: Malicious IPs, domains, URLs, and email addresses.

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*.**	No. This is not a Privacy Act System of Record intended to collect, use and/or retain personal information as a source for accessing PII. Query of data by email address would not produce additional PII.
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?	Users provide their email addresses for administrative purposes. Users may submit suspected malicious files containing limited PII.
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?	No
DATA USE	
11. How will the PII be used?	For the administration 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?**	N/A

MODULE II – PII SYSTEMS & PROJECTS	
13. With what other agencies or entities will an individual's information be shared?	DOE OCIO and Departmental Elements
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Periodic system auditing is performed which lists active users and their system activity.
15. What will be the use of these reports?	System administration.
16. Who will have access to these reports?	iJC3 System Owner, iJC3 System Administrators and other DOE Users as required. (e.g. if a site/lab requests a list of their active users.)
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	This system does not monitor individuals.
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 and Audit log review 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.	The system does not maintain PII beyond Malicious IPs, domains, URLs, and email addresses. Content submitted to the platforms do not contain sensitive PII. All submitted data is stored in the system for historical/auditing and administrative purposes.

MODULE II – PII SYSTEMS & PROJECTS	
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	System Owners and Information owners are responsible for ensuring information is used and managed consistently for its stated purpose in support of the organization. Users are limited by Role Based Access Controls.
RECORDS MANAGEMENT	
22. Identify the record(s).	System access records, cyber security logging records
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 3.2 item 030, 035, 036
24. Records Contact	Faiad Shaban (571) 239-8726 faiad.shaban@hq.doe.gov 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?	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?	Access to data in the iJC3 is restricted and role-based. Authorized and authenticated DOE employees and contractors working as network administrators; security officers, and related security operations center personnel, will have access to data in the iJC3.
27. How is access to PII data determined?	Access to data in the iJC3 is restricted and based on a need to know.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Sandbox extracted Indicators of Compromise and related reports are potentially shared with Analyst1, though no automation currently exists. There is an intention to automate in the future. Mailparser sends all extracted data to BDP.

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?	N/A - Same organization
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	

SIGNATURE PAGE

	Signature	Date
System Owner	_____ **(Print Name)** LILI CAMERON Digitally signed by LILI CAMERON Date: 2024.10.03 15:54:50 -04'00' _____ **(Signature)**	_____
Local Privacy Act Officer	_____ **(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.10.02 15:08:13 -04'00' _____ **(Signature)**	_____
Ken Hunt **Chief Privacy Officer**	_____ **(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.10.02 15:08:42 -04'00' _____ **(Signature)**	_____