Department of Energy

MODULE I – PRIVACY NEEDS ASSESSMENT		
Date	10/30/2023	
Departmental Element & Site	Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33), Integrated Joint Cybersecurity Coordination Center (iJC3) DOE Germantown Campus, Room CA-007	
Name of Information System or IT Project	Analyst1/Automated Indicator Sharing (AIS)	
Exhibit Project UID	CSAM ID: 106	
New PIA [X] **Update** [ ]		
	Name, Title	**Contact Information Phone, Email**
System Owner	Ashton Garrett IT Program Manager (INFOSEC) IM-33	301-903-1198 Ashton.Garrett@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.)	Charlene Kamadeu ISSO	571-435-6603 charlene.kamadeu@hq.doe.gov
Person Completing this Document	Charlene Kamadeu ISSO	571-435-6603 charlene.kamadeu@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Purpose of Information System or IT Project	The Integrated Joint Cybersecurity Coordination Center (iJC3) serves as the coordination and collaboration hub for cyber incidents, information sharing, and reporting for DOE's enterprise cybersecurity program; it falls under the purview of the Chief Information Officer (OCIO). iJC3's objective is to coordinate enterprise cybersecurity efforts, provide common tools, establish methodologies (to address cybersecurity events), and provide a centralized reporting framework for the Department. iJC3 regularly communicates with sites and contacts throughout the DOE. Analyst1, or Automated Indicator Sharing (AIS), is a product purchased by IM-30 and is replacing the Cyber Fed Model (CFM). DOE cyber threat indicators are currently shared through the CFM. CFM is a GOTS solution which DOE has decided to discontinue. Analyst1 is purchased from the vendor Analyst Platform, and it is used to identify malicious cyber activities. Analyst1 is an indicator, countermeasure, threat intelligence, and sensor management tool that enables analysts to collect and analyze evidence of malicious activity. Analyst1 enables authorized users to author, test, implement, and track rules to detect and mitigate malicious activity across multiple host-based and network-based intrusion detection systems. The continually enriched intelligence context establishes a trusted and enhanced knowledge base to quickly identify the current defensive posture against a known threat. This provides a unique ability for information sharing to flow successfully and rapidly and in both directions between the government, strategic partners, and the private sector. Information types processed by Analyst1 include threat intelligence, vulnerability information for sites, public vulnerabilities, and exploits. Analyst1 empowers network defenders to protect and operate networked environments by simplifying the creation, execution, and enforcement of countermeasures more effectively. The system operates defensively and is not focused on individuals. PII is generally limited to administrative PII for authorized users and email addresses and/or IP address associated with security events and related activity data. These data may or may not be linked to individuals; Analyst1 simply blocks access to DOE systems and takes no offensive or investigative action on individuals. Typical kinds of data collected by the system include: 1. Vulnerability reports, indicator lists, RSS feeds: typically includes IP addresses, file names/hashes, domain names, URLs, and email addresses. Some reports include a narrative describing the malicious activity and may include associations to "Threat Actor" profiles. These profiles are typically direct or abstracted names of groups (e.g., hacker groups or nation state sponsored groups) with which these reports and their contents, a general geolocation (country) and patterns of attacks, have been associated.

MODULE I – PRIVACY NEEDS ASSESSMENT

	2. Item names (file, domain, URLs): typically do not include PII. While it is possible that a person's name could be used for a file or domain name or used in a web address, the system does analyze file names to extract individuals' names. 3. Email addresses: Emails associated with email-based cyber threats (such as a phishing attempts) are extracted and indexed. Typically, the email addresses included are the malicious sender email addresses. Occasionally, reports of targeted Federal employees include targeted email address, but those addresses are matched to a whitelist and are not shared out of platform. 4. Use of data: Used for defensive cyber posturing and threat intelligence sharing with the DOE enterprise and with the Department of Homeland Security. Authorized users of the Analyst1 platform and data contained within do not engage in any offensive cyber activities and do not seek to identify or investigate individuals. Analyst1 is accessible from within the DOE network. Access is limited to authorized federal and contractor employees and is controlled by the system administrator. Access is restricted through AWS security groups to approved external endpoints. The system relies on DOE AD repositories containing all system and access information. The primary authentication method is HCE Azure AD federated with OneID for HSPD12 with MFA as an alternative. The rules, controls, and procedures that govern access to the system will be applied consistently, regardless of which physical site the system is accessed from.
Type of Information Collected or Maintained by the System:	☒ Name, Email Address, Organization (for user accounts/administrative use) ☒ Other – Please Specify Information types contain within and processed by Analyst1 include threat intelligence, vulnerability information for sites, public vulnerabilities, and exploits. Typically includes IP addresses, file names/hashes, domain names, URLs, and email addresses associated with malicious activity.
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*	The system contains PII.

MODULE I – PRIVACY NEEDS ASSESSMENT

data, and including any other personal information that is linked or linkable to a specific individual.	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	NA

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?	Yes (X) Threat intelligence IOCs may contain email addresses which may be linked or linkable to members of the public.
4. Is the information about DOE or contractor employees?	(X) Federal Employees (X) Contractor Employees

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

MODULE II – PII SYSTEMS & PROJECTS

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.; The Cybersecurity Information Sharing Act of 2015 (CISA) requires the Director of National Intelligence and the Departments of DHS, Defense, and Justice to develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities under threat.
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)?**	Individuals have two opportunities to decline to provide information: 1) All visitors to the portal will see the following system use / warning banner, which clearly states that logging in is equivalent to providing consent. An individual may choose not to log into the system. ****WARNING**WARNING**WARNING**WARNING**** This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY. ****WARNING**WARNING**WARNING**WARNING**** 2) In Analyst1, users have the option to upload attachments. User uploads are not mandatory and may be declined.

MODULE II – PII SYSTEMS & PROJECTS

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 Analyst1. 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 DOE requirements.

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed Analyst1 as a moderate-risk system according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity, or availability be compromised. Analyst1 contains PII including contact information for users. The unauthorized disclosure of PII is expected to have a minimal adverse effect on individuals. If PII maintained in this system were disclosed to unauthorized parties, the moderate sensitivity thereof could compromise the trust between employees and the employer. Should information identifying an individual's email address as related to malicious activity be compromised, it could cause significant privacy harm to the individual including personal, professional, legal, and social harm and embarrassment. Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of Analyst1 from being compromised in contemplation of the Fair Information Practice Principles (FIPPs). 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. Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access based on user responsibility and job function. These controls are defined in the system security plan. The system is not focused on individuals and collects the minimum PII required in observance of data minimization. PII is used only for expressly authorized purposes in observance of purpose specification and use limitation. Importantly, Analyst1 is expected to provide a net benefit to the privacy of individuals by securing data and improving on how privacy and "data spillage" incidents are communicated and resolved at DOE. The system is designed to improve communication and workflows between cybersecurity resources throughout DOE and between DOE cybersecurity resources and all other (non-cyber) DOE resources. Analyst1 automatically categorizes content to include Cyber Kill Chain and the MITRE ATT&CK Framework. Additionally, the system's reporting and analytic capabilities may provide new insight into trends regarding DOE privacy incidents. Analyst1 empowers network defenders to protect and operate networked environments by simplifying the creation, execution, and enforcement of countermeasures more effectively.

MODULE II – PII SYSTEMS & PROJECTS	
	Analyst1 is not a public-facing system. Even within the DOE community, its use will be restricted to only those who can access the EITS internal network.
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.**	All threat intelligence indicators are indexed in Analyst1. The threat intelligence will include email addresses, which are retrievable from the threat indicator database. However, Analyst1 operates in a strictly defensive posture. Email addresses are not typically related to real individuals and are irrelevant to the threat indicator as well as the system's response, which is to block access related to all malicious activity. The information may not constitute PII if not tied to individuals and its use by the system bears no relation to individuals, investigative or otherwise.
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*.**	A SORN is not required; see answer to previous question.
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
8. What are the sources of information about individuals in the information system or project?	1) Administrative purposes for users – email, name, organization provided by users and/or managers. 2) Incident reports such as spoofed email addresses or victim email addresses reported to iJC3 from DOE sites/labs or threat intelligence reports. The threat intelligence reports come from a mix of open source, paid, and government entities from approximately 150 providers.

MODULE II – PII SYSTEMS & PROJECTS

9. Will the information system derive new or meta data about an individual from the information collected?	Yes. The system attempts to correlate publicly available security data to develop profiles for threat actors as they are surfaced in threat indicators. This is not intended to discover or index sensitive PII and informs solely defensive posturing in DOE.
10. Are the data elements described in detail and documented?	Data elements to be ingested are described in: 1) The Cybersecurity Information Sharing Act of 2015 ("CISA") 2) The Master Indicator Sharing Agreement with DHS
DATA USE	
11. How will the PII be used?	Email addresses from incident reports are used for threat analysis. If the email address is associated with threat actors or associated with an actual DOE reported incident, it may be shared with the rest of the DOE cyber threat intelligence community and DHS. PII for users (email addresses) may be contained in event logs and sent to network and log analysis tools meant to monitor for unauthorized 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?**	Meta data may be used to help develop profiles for threat actors as they are surfaced in threat indicators. The system does not seek to identify or track individuals, only accounts or email addresses.

MODULE II – PII SYSTEMS & PROJECTS	
13. With what other agencies or entities will an individual's information be shared?	Analyst1 is a threat intelligence platform which automates the collection, correlation, and enrichment of cyber threat information from multiple trusted sources to produce actionable threat intelligence between DOE and sites, labs, and DHS. iJC3 personnel (including Analyst1 system admins) and site designated cyber POCs will be able to see threat reports that have been submitted by people other than themselves. More specifically, site designated cyber POCs will only be able to see reports concerning their respective organization. Some users will need to be able to have visibility at the Program Office level (which encompasses multiple sites) sharing to flow successfully and rapidly and in both directions between the government, strategic partners, and the private sector.
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Per NIST SP 800-53 / 800-37, Analyst1 is required to follow several auditing controls. As a result, audit logs are generated. These contain information such as user email address, user actions (login time, etc.). Analyst1 has not been designed to report on individuals, though accounts or email addresses related to malicious activity may be included.
15. What will be the use of these reports?	The reports generated are all used for auditing/administrative purposes.
16. Who will have access to these reports?	1) Authorized iJC3 system administrators and security personnel will have access to reports from all sites.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. The system operates defensively and does not identify, target, or monitor individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A

MODULE II – PII SYSTEMS & PROJECTS	
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. 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. Technical and administrative controls are in place to prevent the misuse of data.
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.	Via a hybrid of automated quality control and manual review.
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).	1) Data described in Module 1 (Type of Information Collected or Maintained by the System); and 2) User actions that are recorded (for auditing purposes) by the system

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. (X) Scheduled (cite NARA authority below) National Archives Records Administration (NARA) General Records Schedule (GRS) GRS 3.2 Information Systems Security Records. This schedule covers records created and maintained by Federal agencies related to protecting the security of information technology systems and data and responding to computer security incidents. This schedule does not apply to system data or content. Items 010-036 (DAA-GRS-2013-0006-0001; DAA-GRS-2013-0006-0002; DAA-GRS-2013-0006-0003; DAA-GRS-2013-0006-0004; DAA-GRS-2022-0005-0001; DAA-GRS-2022-0005-0002) The Schedules may be found here: https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf
24. Records Contact	Dustin Rice RLO/AERL U.S. Department of Energy Cybersecurity Phone: 301-452-2498 dustin.rice@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The Analyst1 web portal itself can only be reached by DOE and affiliated sites and labs IP addresses. HCE Azure OneID further restricts login to those who have active and approved HCE accounts. Upon login, privileges are determined by membership in role-based groups. Implementation details are described in the System's Security Plan.
26. Who will have access to PII data?	Authorized iJC3 system administrators, security personnel, and designated site POCs.
27. How is access to PII data determined?	Access to data in Analyst1 is restricted and role-based. Authorized iJC3 system administrators and security personnel have different levels of role-based access to reports containing basic contact information within Analyst1.

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes, other information systems have access to data but not user account information. Analyst1 shares incident reports such as spoofed email addresses or victim email addresses with other information systems.
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?	There are ISAs in place with DHS and EM.
30. Who is responsible for ensuring the authorized use of personal information?	Data Owners are responsible for the information contained in their systems.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Ashton Garrett** **(Print Name)** Ashton M. Garrett Jr. Digitally signed by Ashton M. Garrett Jr. Date: 2023.11.16 11:59:15 -05'00' **(Signature)**	
Local Privacy Act Officer	**Brooke Dickson** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.11.15 09:20:51 -05'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**William K. Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.11.15 09:21:03 -05'00' **(Signature)**	