PRIVACY IMPACT ASSESSMENT
Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
Integrated Joint Cybersecurity Center (iJC3)
IM-30 SecOps

Affects Members Of the Public? ☐

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	11/29/2022
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	IM-30 SecOps FedRAMP Package ID F1305072116
Exhibit Project UID	N/A
New PIA ☐ **Update** X	Update due to system name change

	Name, Title	Contact Information Phone, Email
System Owner	Ashton Garrett System Owner Office of the Chief Information Officer (OCIO) Cybersecurity Operations (IM33) Integrated Joint Cybersecurity Coordination Center (iJC3)	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	Paul Abulu (CTR) ISSO, iJC3	Office: 301-903-7701

MODULE I – PRIVACY NEEDS ASSESSMENT

document (e.g. ISSM, CSSM, ISSO, etc.)		
Person Completing this Document	Ashton Garrett iJC3 Manager	301-903-1198 Ashton.garrett@hq.doe.gov
Purpose of Information System or IT Project	The IM-30 SecOps is hosted as a subsystem in the DOE JC3 SNOW ServiceNOW instance. IM-30 SecOps will leverage the JC3 SNOW control inheritance and ATO date. The IM-30 SecOps is a cloud-based web portal which includes tracking, managing, and reporting of: • DOE Cyber Incidents; • Requests For Service (RFS); and • Requests For Information (RFI). IM-30 SecOps is used by site security incident reporters (iJC3-designated cyber points of contact). Authentication is supported via OneID (PIV card), 3rd party multi-factor authentication (Microsoft Authenticator), or EITS RSA token. iJC3-designated cyber points of contact have separate accounts in IM-30 SecOps. IM-30 SecOps is built on the FedRAMP-approved (SaaS) ServiceNow platform. iJC3 has implemented the Security Incident Response (SIR) application (which is a part of the larger Security Operations suite offering (from ServiceNow). The information collected depends on the ticket type (Service Request, Request for Information, or Incident Report). Attachments may be added. For ***Service Requests***: 1. Service Request information (type and description) 2. Submitter Contact information (name and email) 3. Reporting Office information (program office; site; POC; email; name; phone) 4. Depending on service request type (beneficiary's name and email) For ***Requests for Information***: 1. Submitted Information (name and email) 2. Reporting Office information (program office; site; POC; email; name; phone; description)	

MODULE I – PRIVACY NEEDS ASSESSMENT

	For ***Incident Reports*** *(Attrition, Impersonation Spoofing, Removable Media, Other, Phishing, Unknown, Loss or Theft, Improper Usage, and Web)*: 1. Submitter's name and work email address is collected at the site level on behalf of the site 2. Reporting Office information (Program Office, site, POC, email, name, business phone) 3. Incident details (date and time of incident; internal tracking number; name, email, and phone number of impacted user; existing iJC3 ticked number (if applicable); confirmation of spillage event (Y or N); incident description; and confirmation of whether confidentiality, integrity, and/or availability of information systems has been affected (Y or N) 4. Functional Impact information (functional impact definition; characterization of observed activity at its most severe level; # users impacted; # systems impacted; location (defined by levels 1-7) at which activity was observed 5. Whether PII Exists? (Y or N) 6. Impacted Operating Systems (name and version of impacted O/S); function of system affected 7. Informational Impact (description of known informational impact from incident; confirmation of if incident is considered to be a breach that must be reported to Congress w/in 30 days in accordance w/ OMB guidance (Y or N); confirmation of if incident is considered to be a "major incident" per OMB guidance (Y or N) 8. Technical Information (incident detection method; netflow (if available); CVE-ID (if available) 9. Indicators of Compromise (email address; IP address; domain; port; protocol 10. Recoverability / Mitigation (recoverability ability; details regarding recoverability) 11. Resolution (confirmation of readiness to close incident (Y or N); resolution details)
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 [X] Name, Phone, email address ☐ Criminal History ☐ Name, Phone, Address ☒ Other – See Purpose section
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.*	The system contains PII.
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 (see above). Basic contact information will be collected from the submitter at the site level during initial reporting of an incident on behalf of the site. Incident information will be collected.
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?	[**X**] Federal Employees [**X**] 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. • 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 threats. In general, CISA authorizes the sharing of cyber threat indicators and defensive measures: ○ For a "cybersecurity purpose," defined to mean "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability." Id. §102(4); ○ Consisting of information that meets the definition of a "cyber threat indicator" or "defensive measures." (See frequently asked question (FAQ) #7 for a discussion of "cyber threat indicators" and "defensive measures."); ○ Following the review and removal of any personal information of a specific person or information that identifies a specific person that the sharer knows is not directly related to a cyber threat. Id. § 104(d)(2); and ○ In compliance with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicators or defensive measures.

MODULE II – PII SYSTEMS & PROJECTS

	CISA provides that, "notwithstanding any other provision of law, a non-federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-federal entity or the Federal Government a cyber threat indicator or defensive measure." CISA, §104(c)(1) (emphasis added).
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)?**	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, of course, choose not to log in to 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) On several screens (when inside IM-30 SecOps) users have the *option* to upload attachments (that would contain additional information). User uploads aren't mandatory.
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 IM-30 SecOps. 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:	IM-30 SecOps is expected to improve how privacy and data spillage incidents are communicated and resolved at DOE. The system is designed to improve communication and workflows between security resources

MODULE II – PII SYSTEMS & PROJECTS

How does this project or information system impact privacy?	throughout DOE. Additionally, the system's reporting and analytic capabilities may provide new insight into trends regarding DOE privacy incidents. The system's purpose and use are consistent with that of Incident Response and Security Coordination Teams. IM-30 SecOps is not a public-facing system. Even within the DOE community, its use will be restricted to only those who can authenticate via OneID. The only PII collected by IM-30 SecOps includes administrative PII pertaining to contact information and clearance. Incident reports will not include sensitive PII, but rather a description of the incident with general reference to any data breached. In addition to the low sensitivity of the PII as well as the controls protecting it, PII is not indexed and cannot therefore be retrieved by unique identifier beyond very narrow administrative retrieval by a small number of privileged personnel. IM-30 SecOps observes a number of protections to protect privacy and via the Fair Information Practice Principles (FIPPs). IM-30 SecOps maintains the minimum PII necessary for its business purpose to mitigate privacy harm. In addition, use of the PII in IM-30 SecOps is limited to clearly defined business purposes furthering privacy interests at DOE. Access to and use of PII in the system is protected by a series of controls including role and permission-based monitoring controls. Access is restricted to authorized users with a need to know and is verified through a series of technical controls. Approved OCIO system administrators have access to the user data. The significant privacy protection facilitated by IM-30 SecOps outweighs the small privacy risk posed by the system. IM-30 SecOps provides a significant privacy net benefit in light of the low sensitivity administrative PII collected by the system weighed against the ability to protect privacy interests the system provides.
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.**	Deliberate, indexed retrieval of PII is not possible for general users. Access to IM-30 SecOps data is restricted to DOE approved users with appropriate security permissions who may retrieve administrative PII (e.g., name, organization, clearance level) for administrative (record keeping and contact) purposes. General users cannot retrieve PII by unique identifier. Moreover, data accessible to the IM-30 SecOps team could not be searched against other data in the system.

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*.**	See answer to Question 4. PII is not indexed and cannot therefore be retrieved by unique identifier beyond very narrow administrative retrieval by a small number of privileged personnel; a SORN is therefore not required.
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?	1) OneID (https://oneid.yc.energy.gov/info/#/idm) and PIV cards will be used to authenticate. IM-30 SecOps users will need to supply their own PIV card. 2) Once inside the system, a user can enter basic contact information about themselves or, if submitting a ticket on behalf of someone else, another individual.
9. Will the information system derive new or metadata about an individual from the information collected?	No. IM-30 SecOps will be collecting the types of data stated in Module 1. Every ticket needs to be associated with at least one person, but IM-30 SecOps does not generate new data or metadata about individuals.
10. Are the data elements described in detail and documented?	Yes. They are described in the FIPS-199 Security Categorization.
DATA USE	
11. How will the PII be used?	IM-30 SecOps is an incident reporting system designed to improve communication between organizations in DOE to further data protection. The system manages incident tickets.
12. If the system derives metadata, how will the new or metadata be used?	N/A.

MODULE II – PII SYSTEMS & PROJECTS	
Will the new or meta data be part of an individual's record?	
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?	Per NIST SP 800-53 / 800-37, IM-30 SecOps is required to follow a number of auditing controls. As a result, audit logs are generated. These contain information such as user actions (login time, etc.). Most site-designated cyber POCs will have the ability to generate reports detailing all tickets associated with only their site. Some users will need to be able to have visibility at the Program Office level (multiple sites), however. All other users will be unable to generate reports.
15. What will be the use of these reports?	Audit logs will be used for the security and management of the system. iJC3 produces specific daily, weekly, and monthly operations reports. One example is the Executive Summary Incident Report. The iJC3 must also be able to generate situational reports. PII would not be collected, stored or searchable in these instances. Example: LANL's designated cyber point of contact may call the iJC3 to report an Indicator of Compromise (present on their network). It would be extremely helpful for the iJC3 Analyst to be able to view LANL's past (and any current) tickets (for incidents or IOCs). If an abnormal amount of problems are from one specific user, this information would be vital to properly assessing and resolving the problem. This type of capability is considered standard for security analysts to effectively perform their jobs.
16. Who will have access to these reports?	1) Authorized iJC3 system administrators and security personnel will have access to reports from all sites. 2) Site-designated cyber POCs will be able to view reports that cover only their (respective) sites. 3) Standard end users won't have any report-viewing capability.
MONITORING	
17. Will this information system provide the	IM-30 SecOps is not a monitoring or identification system. Certain user actions are required to be logged for standard system security.

MODULE II – PII SYSTEMS & PROJECTS	
capability to identify, locate, and monitor individuals?	
18. What kinds of information are collected as a function of the monitoring of individuals?	Security log data. Auditable user actions are logged, as IM-30 SecOps is required to meet NIST-defined security controls. The system must be capable of auditing based on a risk assessment and mission/business needs in the DOE Program Cyber Security Policy (PCSP). Audit events include successful and unsuccessful logon, account creation / deletion, changes in account profiles, and error conditions. Further details can be found in the IM-30 SecOps Security Plan.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. Access controls limit the users who can view audit logs.
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.	There is an annual audit review where the ISSO and other stakeholders will review the details included in system audit records and determine if anymore, less, or other details are required.
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. There is only one production instance of IM-30 SecOps, and it is hosted in the cloud. All system users, regardless of their geographic location, will be accessing this instance.
RECORDS MANAGEMENT	
22. Identify the record(s).	• System audit records • Cybersecurity incident reporting • Requests for Cybersecurity services and information
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	☐ Unscheduled ☑ Scheduled *(cite NARA authority below)* • GRS 3.2, item 020 - Computer security incident handling, reporting and follow-up records

MODULE II – PII SYSTEMS & PROJECTS	
	• GRS 3.2, items 030 (or 031) - System access records • GRS 5.6, item 190 - Index to the personnel security case files or GRS 5.6, item 010 - Security administrative records • GRS 5.8, item 010 - Technical and administrative help desk operational records
24. Records Contact	Shannon Hughes, shannon.hughes@hq.doe.gov Dominick Littleton, dominick.littleton@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	As a system designed to further data security, IM-30 SecOps employs a number of technical and administrative controls to protect data. The IM-30 SecOps web portal itself can only be reached by DOE IP addresses. OneID further restricts login to those who have PIV cards. Upon login, privileges are determined by membership in role-based groups. To request privileged access, users are required to follow the iJC3 approval process. Implementation details are described in the system's Security Plan.
26. Who will have access to PII data?	iJC3 system administrators and site-designated POCs will have access to limited administrative PII associated with tickets.
27. How is access to PII data determined?	Access to data in IM-30 SecOps is restricted and role based.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	iJC3 SNOW (SecOps is a subsystem of this system).
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners	N/A.

MODULE II – PII SYSTEMS & PROJECTS	
to ensure the privacy of individuals is protected?	
30. Who is responsible for ensuring the authorized use of personal information?	The IM-30 SecOps System Owner is responsible for ensuring authorized use of personal information. Access control lists are kept by iJC3 IM-30 SecOps System Administrators and audited according to policy.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date (If not digitally signed)
System Owner	**Ashton Garrett** **(Print Name)** Ashton M. Garrett Jr. Digitally signed by Ashton M. Garrett Jr. Date: 2023.05.08 13:32:14 -04'00' **(Signature)**	
Local Privacy Act Officer	**Brooke Dickson** **(Print Name)** Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2023.04.28 09:44:37 -04'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**William K. Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.04.27 09:04:20 -04'00' **(Signature)**	