PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

SIEM (Security Information Event Manager) SaaS (Software as a Service)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

07/16/24

PEO-Cyber ID6 Cyber Analytics and Awareness Division

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees
- [ ] from both members of the general public and Federal employees
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [x] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Security Information and Event Management (SIEM) SaaS Pilot was created to assist in building an effective automated security capability within DISA and its facilities to help detect, categorize, identify, and prioritize computer intrusions near real-time. This technology provides value added flexibility to a constantly evolving infrastructure and improves DoD security. The types of personal information that is collected includes: Name(s), DoD ID Number, Rank/Grade, Official Duty Telephone Phone, Work E-mail Address, and Official Duty Address.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The PII collected will be used for user authentication into the system as well as role and privilege assignment.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individuals can object to the collection of their PII by not completing and submitting the information required.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Individuals can object to the specific uses of their PII by not completing and submitting the information req

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

- [ ] Privacy Act Statement
- [ ] Privacy Advisory
- [x] Not Applicable

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X]	Within the DoD Component	Specify.	DISA/JFHQ-DODIN/JSP
[X]	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	ARMY Cyber
[ ]	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
[ ]	State and Local Agencies	Specify.	
[ ]	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
[ ]	Other *(e.g., commercial providers, colleges)*.	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [ ] Individuals
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

1. PII is collected from ICAM GFUD and stored in SIEM SaaS
2. PII is collected from sensor, network devices, endpoints, etc. from across the DODIN and stored in SIEM SaaS

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] In-Person Contact
- [ ] Fax
- [X] Information Sharing - System to System
- [ ] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Paper
- [ ] Telephone Interview
- [ ] Website/E-Form

1. All information is collected and correlated from existing DoD Information Systems, specifically from DISA Identity, Credential, and Access Management (ICAM) Global Federated User Domain (GFUD)
2. All information is collected from sensor, network devices, endpoints, etc. from across the DODIN and stored in SIEM SaaS

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier DoD-0015

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-GRS-2013-0006-0002

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

The authority below allow SIEM/SaaS to collect the following data:
- 10 U.S.C. Chapter 8-Defense Agencies and Department of Defense Field Activities;
- DoD Directive (DoDD) 5105.19 Defense Information Systems Agency (DISA);
- DoD Directive 1000.25; DoD Personnel Identity Protection (PIP) Program
- DoD Personnel Identity Protection (PIP) Program;
- DoD Enterprise User Data Management Plan for Persons and Personas, August 11, 2010;
- DoD Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS), March 11, 2009;
- DoDI 5200.46-DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC) ;
- DoDI 8520.03-Identity Authentication for Information Systems
- DoD Directive 5105.19, Defense Information Systems Agency (DISA)
- DoD Chief Information Officer Memorandum for Director, Defense Information Systems Agency (DISA)
- Mandating the Use of Department of Defense Enterprise Directory Services (EDS), 31 Mar 2019

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ Yes ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB Control Number: 0704-0415; Expiration Date: None