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:

Defense Health Headquarters (DHHQ) SIPRNet

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

04/30/24

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
- [x] Existing DoD Information System
- [ ] 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 Defense Health Agency Headquarters (DHHQ) Secure Internet Protocol Router Network (SIPRNet) is a closed system (not public facing) and allows for a secure communications capability for the transmission and reception of sensitive/Secret information. The enclave includes user interfaces such as workstations, laptops, telecommunication devices, and office automation software. DHHQ SIPRNet provides the infrastructure/network and hosting services that include but are not limited to, server virtualization, Active Directory services, Information Assurance, file servers, print servers, and network monitoring. DHHQ SIPRNet does not collect, maintain, process, or disseminate Personally Identifiable Information (PII). However, hosted systems and applications within the enclave can and may have PII on documents stored on file servers and shared drives.

DHHQ SIPRNet currently hosts only one application, and/or electronic collections system: - Medical Situational Awareness Theater (MSAT). MSAT has an inherent ATO and PIA.

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)*

DHHQ SIPRNet does not collect, maintain, process, or disseminate Personally Identifiable Information (PII). However hosted systems and applications within the enclave can and may have PII on documents stored on file servers and shared drives. The process of collection, purpose, and the intended use of collected PII is specific to a system component and is addressed in the hosted system's PIA.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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.

DHHQ SIPRNet does not collect, maintain, process, or disseminate Personally Identifiable Information (PII). However hosted systems and applications within the enclave can and may have PII on documents stored on file servers and shared drives. The opportunity for individuals to object to the collection of PII is specific to the method used to collect PII in the respective hosted system component and is addressed in the hosted system's PIA.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

DHHQ SIPRNet does not collect, maintain, process, or disseminate Personally Identifiable Information (PII). However hosted systems and applications within the enclave can and may have PII on documents stored on file servers and shared drives. The opportunity for individuals

to consent to the collection of PII is specific to the method used to collect PII in the respective hosted system component and is addressed in the sub-system's PIA.

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 ☒ Not Applicable

DHHQ SIPRNet does not collect PII directly from an individual to be stored in a system of records, a Privacy Act Statement or Privacy Advisory is not required.

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)*

☒ Within the DoD Component	Specify.	PII may be shared with personnel with a need-to-know, proper clearance, and current authorized access to the enclave.
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	N/A
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	N/A
☐ State and Local Agencies	Specify.	N/A
☐ 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.	N/A
☐ Other *(e.g., commercial providers, colleges).*	Specify.	N/A

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

☐ Individuals ☐ Databases

☐ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

Not applicable for the enclave; the source of the PII collected is specific to the information system component and is addressed in the sub-system's PIA.

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

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*

☐ In-Person Contact ☐ Paper

☐ Fax ☐ Telephone Interview

☐ Information Sharing - System to System ☐ Website/E-Form

☐ Other *(If Other, enter the information in the box below)*

Not applicable for the enclave; the source of the PII collected is specific to the information system component and is addressed in the sub-system's PIA.

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.

☐ Yes ☒ No

If "Yes," enter SORN System Identifier

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.

A system of records notice ("SORN") is not required because DHHQ SIPRNet does not collect or store information in a system or records. Further, there appears to be no actual retrieval of records by an individual's name or other personal identifier.

However, information systems (e.g., Medical Situation Awareness in Theater ("MSAT")) are hosted on DHHQ SIPRNet. Those

information systems may require a SORN as those information systems appear to collect, store, and actually retrieve information by an individual's name or other personal identifier. However, those information systems (e.g., MSAT) are separately assessed and SORN requirements are addressed in the privacy impact assessments ("PIA") for those systems.

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. Not Applicable

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

(3) Retention Instructions.

The LAN/Enclave itself does not have a NARA approved, pending, or GRS authority and retention instructions applied as a whole. Refer to NARA approved, pending, or GRS authority and retention instruction specific to the systems, applications, electronic collections, file servers, and share drives contained within the LAN/Enclave

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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. Ch. 4, Office of the Secretary of Defense; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 142, Chief Information Officer; 40 U.S.C. 11315, Agency Chief Information Officer. For additional authorities, refer to the authorities as addressed in the respective sub-system's privacy impact assessment ("PIA").

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.

According to the IMCO SME Information is retrieved from other systems, therefore the DHHQ SIPRNET is not the initial point of entry of the information. The information collected in this system is for the diagnosis and treatment of medical disorders and does not collect PHI/PII directly from individuals.