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:

US Army Medical Research Institute of Infectious Diseases Local Area Network (USAMRIID LAN)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

08/15/24

Medical Research and Development Command (MRDC)

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
- ☐ 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
- ☐ 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 US Army Medical Research Institute of Infectious Diseases Local Area Network (USAMRIID LAN) is an Information System (IS) providing network security and network data transport services (local area network communications) for DHA systems. The LAN consists of workstations, servers, printers, and web-based services to provide office automation and associated information distribution capabilities, secure user and network access, technical support, facilitates workflows and processes to maintain data, and provides methods to share and integrate the data with numerous business functions throughout the Organization's workforce. Commercial-Off-The-Shelf (COTS) applications such as Microsoft Word Excel, PowerPoint, and Outlook are utilized to provide administrative support and may process PII.

Personally Identifiable Information (PII) collected, maintained, processed, or disseminated by systems and applications within the HQ USAMRIID LAN or in documents stored on file servers and shared drives includes employee and beneficiary contact information, military information, demographic information, and Protected Health Information (PHI). Categories of persons information is collected are Federal Employees, Active Duty military, Contractors, and emergency contacts for persons working at USAMRIID, which includes, Civilians, Contractors, External Workers, and Military personnel.

The following systems and applications contain electronic collections hosted within the USAMRIID LAN: US Army Medical Research Institute of Infectious Diseases Workforce HR application and Bio-Laboratory Management System (BLMS).

Personally Identifiable Information (PII) processed on listed system components and applications utilize specific administrative, physical, and technical security controls to protect PII confidentiality and are addressed in separate Privacy Impact Assessments (PIA)s available at: https://dodcio.defense.gov/In-the-News/Privacy-Impact-Assessments/.

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 collection of PII is incidental to the USAMRIID LAN security services performed and has no intended use for the PII which may be collected within audit logs captured by the security services. Additional uses of the collected PII specific to an information system are addressed in the system's PIA.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ 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.

The opportunity for individuals to object to the collection of PII is presented by the DHA application the user is interacting with and is addressed in the sub-system's PIA.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☐ 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.

The opportunity for individuals to consent to uses of PII is specific to the DHA application the user is interacting with.

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

The LAN infrastructure does not collect PII directly from individuals.

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.	Headquarters, United States Army Medical Research Material Command; Headquarters, US Army Medical Command Deputy Chief of Staff, Army G-1
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Assistant Secretary of Defense for Nuclear, Biological, Chemical; Assistant Secretary of Defense for Health Affairs
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Federal Bureau Investigation; Center for Disease Control
☐ 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.	All contracts reference Federal Acquisition Regulation (FAR) clauses 52.224-1, Privacy Act Notification (Apr 1984) and 52.224-2, Privacy Act (Apr 1984).
☐ 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 ☐ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

The source for PII collected within the audit logs is any application listed in 1c that utilizes the LAN for transport.

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 the LAN collects PII which already exists within the packet data transported across, and inspected/monitored by protection mechanisms against the threats of malware, malformed packets, and viruses; which may then be collected in the LAN audit data.

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.

The USAMRIID LAN is not a system of records and is not used to retrieve records by personal identifier.

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.

DoD Instruction 8500.01, Cybersecurity, 14 Mar 2014; DoD Joint Information Environment (JIE) Cyber Security Reference Architecture (CS RA) v 4.0 April 15, 2016; Computer Network Defense (CND) Service Provider Program via DoD Instruction 8530.01, March 7, 2016; DoD Instruction O-8530.2: Support to Computer Network Defense (CND), March 9, 2001.

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.

The LAN/enclave does not collect information from members of the public.