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 Medical Logistics - Enterprise Solution (DML-ES) Amazon Web Services (AWS)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

05/20/2026

Program Executive Office (PEO) Medical Systems (J6)

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 Defense Medical Logistics - Enterprise Solution (DML-ES), operating in the Defense Health Agency (DHA) Amazon Web Services (AWS) cloud environment, delivers a full line of integrated Medical Logistics (MEDLOG) business and operational capabilities to end-users at the Department of Defense (DoD), Veterans Affairs (VA), and other Federal agencies. DML-ES supports DHA Military Treatment Facilities (MTFs) by providing consumable and durable supplies, equipment, and facilities to Military Health System (MHS) beneficiaries as well as forward depot positioning of materiel and support for deployed operational medical forces across a joint environment. DML-ES also delivers a fully integrated medical logistics functionality from the industrial base to end-users for medical supply, equipment maintenance, property and facility management, and assemblage management; provides full financial integration with the DHA, Services, and VA; enables compliance with Federal regulations, DoD, U.S. Food and Drug Administration (FDA), Drug Enforcement Administration (DEA), and Joint Commission standards; and provides inventory and management integration with the Shelf-Life Extension Program (SLEP).

The types of personally identifiable information (PII) collected by DML-ES include personal descriptors, identification numbers (including DoD ID Numbers), and employment information.

PII is collected from the following categories of individuals: Members of the Armed Forces, Veterans, DoD civilians, and DoD contractors.

DML-ES is owned and managed by the Medical Logistics IT Program Management Office (MEDLOG IT PMO)/Solution Delivery Division (SDD)/Program Executive Office (PEO) Medical Systems (J-6)/Defense Health Agency (DHA).

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)*

DML-ES collects PII for authentication and administrative use. The intended use of PII collected by DML-ES is to support system access authorization, audit, and transaction execution history; support product receipt and inspection for financial payment; facilitate end-user support; and positively account for government property issued to an authorized direct contractor, beneficiary (retired or service-connected disability veteran), and government staff.

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.

Individuals can object to the collection of their PII in writing, by declining to provide a completed DD2875 (System Authorization Access Request) or hand receipt for equipment issuance. However, if an individual chooses to object to the collection of their PII, they will not be authorized to access DML-ES or receive government-issued property.

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.

Individuals have the opportunity to consent to specific uses of their PII in writing, by declining to provide a completed DD2875 (System Authorization Access Request) or hand receipt for equipment issuance. However, if an individual chooses to withhold consent for specific uses of their PII, they will not be authorized to access DML-ES or receive government-issued property.

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

AUTHORITY: 5 U.S.C § 552a (Pub.L. 93-579, Privacy Act of 1974); 10 U.S.C § 4601 - Electronic Submission and Processing of Claims for Contract Payments; 18 U.S.C § 1029, Fraud and Related Activity in Connection with Access Devices; 18 U.S.C § 1030, Fraud and Related Activity in Connection with Computers; 5 U.S.C § 301 - Departmental Regulations; 44 U.S.C § 3541 (Pub.L. 107-347, Federal Information Security Management Act of 2002); E.O. 10450 (Security Requirements for Government Employment); 32 CFR § 199.17 - TRICARE Program; Defense Federal Acquisition Regulation Supplement (DFARS) Procedures, Guidance, and Instructions (PGI) 232.70 and 252.232-7003; DoD Instruction (DoDI) 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property; and Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors.

PRINCIPAL PURPOSE(S): To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USE(S): These records may specifically be disclosed outside the DoD as a routine use pursuant to 5 USC § 552a(b)(3) to appropriate Federal agencies or entities when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm; and to Federal, state, or local agencies or professional organizations or associations, maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, or administrative or disciplinary information, or disciplinary records related to suspended or revoked licenses, if necessary to obtain information relevant to a DoD component or agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit. For a full listing of the Routine Uses, please refer to the applicable SORN.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of your access request.

APPLICABLE SORN: DoD-0019, Information Technology Access and Audit Records (ITAAR) (September 1, 2023; 88 FR 60442). https://www.federalregister.gov/documents/2023/09/01/2023-18682/privacy-act-of-1974-system-of-records

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.	DHA MTFs and other DHA Organizations
☒	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Defense Logistics Agency (DLA) Information Operations (J-6); Departments of the Army, Navy, and Air Force
☒	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Department of Veterans Affairs (VA)
☐	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 ☐ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☒ Other Federal Information Systems

Existing DoD Information Systems: Defense Enrollment Eligibility Reporting System (DEERS); Defense Information Systems Agency (DISA) Identity, Credential, and Access Management (ICAM) Solution.

Other Federal Information Systems: VA Electronic Health Record (EHR) provides internal control numbers (ICNs); VA information system responsible for Personal Identity Verification (PIV) certificate authentication.

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
- ☒ 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

Official Form: DD2875: System Authorization Access Request (SAAR)); DD1150: Request for Issue/Transfer/Turn-In (completed by individuals requesting government property); Service-specific Hand Receipt Form(s); DD250: Material Inspection and Receiving Report; DD1155: Order for Supplies or Services; and DD1348-1A: Issue Release/Receipt Document.

Information Sharing – System to System: DEERS; DISA ICAM Solution; VA EHR; VA information system responsible for PIV certificate authentication.

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 DoD-0019

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.

Mission Schedules:
- N1-330-11-002, item 1

Other Schedules:
- System Access Records: GRS 3.2, item 030 (DAA-GRS-2013-0006-0003),
- Data Administration and Documentation: GRS 3.1, item 051 (DAA-GRS-2013-0005-0003)

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

(3) Retention Instructions.

Mission Schedules:
FILE NUMBER: 911-12
FILE TITLE: Defense Medical Logistics Support System (DMLSS) Medical Logistics Master Files
DISPOSITION: Temporary. Cut off annually. Destroy 3 years after cutoff.

Other Schedules:

FILE NUMBER: 1601-02
FILE TITLE: System Access Records - Systems not requiring Special Accountability for Access
DISPOSITION: Temporary. Cut off and destroy when business use ceases.

FILE NUMBER: 1601-12
FILE TITLE: Data Administration and Documentation - Temporary Systems
DISPOSITION: Temporary. Cut off after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system. Destroy 5 years after cutoff.

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 § 552a (Pub.L. 93-579, Privacy Act of 1974); 10 U.S.C § 4601 - Electronic Submission and Processing of Claims for Contract Payments; 18 U.S.C § 1029, Fraud and Related Activity in Connection with Access Devices; 18 U.S.C § 1030, Fraud and Related Activity in Connection with Computers; 5 U.S.C § 301 - Departmental Regulations; 44 U.S.C § 3541 (Pub.L. 107-347, Federal Information Security Management Act of 2002); E.O. 10450 (Security Requirements for Government Employment); 32 CFR § 199.17 - TRICARE Program; Defense Federal Acquisition Regulation Supplement (DFARS) Procedures, Guidance, and Instructions (PGI) 232.70 and 252.232-7003; DoD Instruction (DoDI) 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property; and Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors.

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.

DML-ES collects information from Members of the Armed Forces and Veterans to track medical equipment requests and issuances and ensure accountability for government property. DML-ES does not conduct information collection(s) from members of the general public as defined by DoDM 8910.01, Volume 2.