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) - SAP (DML-ES - SAP)

2. DOD COMPONENT NAME:

Defense Health Agency

Program Executive Office (PEO) Medical Systems (J-6)

3. PIA APPROVAL DATE:

08/22/23

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
- [x] 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.

Defense Medical Logistics - Enterprise Solution (DML-ES) - SAP provides a fully integrated automated information system that supports medical logistics functionality including medical supply, equipment maintenance, and assemblage management. The DML-ES is comprised of three (3) components - DML-ES - CORE; DML-ES - LogiCole; and DML-ES - SAP. This Privacy Impact Assessment (PIA) is specifically for DML-ES - SAP.

DML-ES - SAP supports critical medical logistics war-fighter requirements in a net-centric environment. It ties the national, regional, and deployed units into a single business environment. It creates the necessary links for planners, commercial partners, and medical logisticians to accomplish essential care in the theater through a single customer facing portal. It removes disparate data and replaces it with a single instance of actionable data. DML-ES SAP supports today`s modern, non-contiguous battlefield at the regional, Combatant Commands (COCOM), and Service levels by leveraging emerging Medical Materiel Executive Agency and Theater Lead Agent infrastructure concepts to manage the entire medical supply chain from the industrial base to the end user. DML-ES - SAP includes over one hundred business roles that operate within many facets of functional areas pertaining to medical logistics including: production planning, finance, supply chain management, material management, medical equipment maintenance management, assemblage life cycle management and warehouse management.

Users of DML-ES - SAP include military medical logicians; clinical staff working in military Role 3 treatment facilities; combat readiness planners; trainers at Service school houses to include direct contractors and government staff. The categories of individuals the personal information is collected or obtained from electronic systems include: Active Duty, Reserves, and National Guard personnel as well as DOD civilians and contractors across all service components. Users primarily access DML-ES - SAP through the use of a Common Access Card (CAC); there is an accepted deployed user base that may access DML-ES - SAP with UserID and Password (PW) if the situation warrants such. Access credentials are stored using Personal Identity Verification (PIV)/CAC via Single Sign On or UserID and PW.

DML-ES - SAP collects demographic data such as contact information, personal identifier, geographic, and work force information to generate user accounts for system access. The PII data is retained until the user no longer requires access which is validated annually. There is no defined time frame for this business process as it is based on the need. For internal US Government operations, the individuals last name and first initial are electronically transmitted and therefore shared with Defense Logistics Agency (DLA) Information Operations (J6) for use by DOD applications of Procurement Integrated Enterprise Environment (PIEE)/Wide Area Work Flow (WAWF) to support receipt and acceptance of the product in accordance with Federal payment requirements and for business contact purposes.

DML-ES - SAP receives and collects non-PII data to include: Medical, surgical, dental, equipment and pharmaceutical product information and product attributes; equipment maintenance actions, history and maintenance plans; authorized stock and inventory balances; medical assemblage component availability; organizational information.

DML-ES SAP is owned/managed by the Medical Logistics Program Management Office (MEDLOG 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 SAP collects PII for authentication and administrative use. The intended use of PII collected by DML-ES SAP is to support account creation and system access authorization; allow support teams to contact the user in support of issues; audit and transaction execution history; support product receipt and inspection for financial payment.

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 in writing, by declining to provide a completed DD2875 (System Authorization Access Request). However, if an individual chooses to object to the collection of their PII, they will not be authorized to access DML-ES SAP.

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 have the opportunity to consent to specific uses of their PII in writing, by declining to provide a completed DD2875 (System Authorization Access Request). However, if an individual chooses to withhold consent for specific uses of their PII, they will not be authorized to access DML-ES SAP.

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.)*

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

DD Form 2875 (System Authorization Access Request form), Privacy Act Statement. Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
Principal Purpose: 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.
Routines Uses: None.
Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

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.	DHA Military Treatment Facilities (MTF) and other DHA organizations.
[x]	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.	
[ ]	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)*

[x]	Individuals	[ ]	Databases
[x]	Existing DoD Information Systems	[ ]	Commercial Systems
[ ]	Other Federal Information Systems		

Existing DoD Information Systems, Defense Enrollment Eligibility Reporting System (DEERS).

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

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

Official Form: DD2875 (System Authorization Access Request)

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 EDHA 28

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. Nl-330-11-002, Item 1

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

(3) Retention Instructions.

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.

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; 44 U.S.C., Chapter 35, Coordination of Federal Information Policy, Subchapter II – Information Security; 5 U.S.C. 552a, Records Maintained on Individuals (Public Law 93-579, Privacy Act of 1974); 18 U.S.C. 1030, Fraud and Related Activity in Connection with Computers; 10 U.S.C. 4601, Electronic Submission and Processing of Claims for Contract Payments; 10 U.S.C. 1097(a) – (b), TRICARE Prime and TRICARE Program; 32 CFR 199.17, Tricare Program; E.O. 10450, Security Requirements for Government Employment; E.O. 9397 (SSN), as amended; DoD Instruction (DoDI) 5000.75, Business Systems Requirements; and DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property Acquisition.

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 x 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 SAP does not collect new PII information from members of the public. DML-ES SAP collects information from Members of the Armed Forces and Veteran personnel in order to track equipment request approvals and coordinations, medical logistics issued equipment and accountability. Public collection, such as from spouses and dependents of members of the Armed Forces and DoD-affiliated personnel, are not collected.