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:

Disposition Integration Web (DIW) Program - Parent for RTD, ETID, Compliance Application

2. DOD COMPONENT NAME:

Defense Logistics Agency (DLA)

3. PIA APPROVAL DATE:

12/08/2025

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in the general public.)

- From both members of the general public and Federal employees

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

- Existing 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.

Disposition Integration Web provides web-based, role-based functionality for 50,000 DLA Disposition Services users and their DLA, military, and external customers, including law enforcement, firefighters, and schools. The requirements include: providing an electronic method for users manually preparing disposal turn-in document (DD1348-1A) and systemically sending the document to DSS (ETID application); providing search and requisition of available DLA Disposition Services inventory to DOD, GSA, and special programs and fulfillment of that requisition via EBS(RTD application); and providing all functionality required by DLA Disposition Services for compliance with Laws, regulations, and Policies (LRPs), including Financial Liability Investigation of Property Loss, Situation Reporting, Compliance Assessment Management, and Corrective Actions.(compliance Application)

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)*

Identification, authentication and verification of users and the property that they are authorized to see and requisition.

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

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.

Users are not provided the option to object to the collection of their PII. Users enter their information into AMPS because this is how they are authenticated.

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

Yes

(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.

Users must read the DLA Privacy Act Statement when accessing AMPS and click OK prior to entering their information into AMPS and before being granted access to DIW/ application customer interface.

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
- Not Applicable

Authority: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; 18 U.S.C. 1029, Access device fraud; E.O. 10450, Security Requirements for Government Employees, as amended; and E.O. 9397 (SSN), as amended.

Principal Purpose(s): Information is used to validate a user's request for access into a DLA system, database or network that has its access requests managed by AMPS.

Routine Uses: Data may be provided under any of the DoD "Blanket Routine Uses" published at http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

Disclosure: Disclosure is voluntary; however, if you fail to supply all the requested information you will not gain access to the DLA - Account Management and Provisioning System (AMPS) database. Your identity / security clearance must be verified prior to gaining access to the AMPS database, and without the requested information verification cannot be accomplished.

Rules of Use: Rules for collecting, using, retaining, and safeguarding this information are contained in DLA Privacy Act System Notice S500.55, entitled "Information Technology Access and Control Records" available at http://dpcld.defense.gov/Privacy/SORNsIndex/tabid/5915/Category/11156/defense-logistics-agency.aspx.

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

Shared	Within the DoD Component	Specify.	DLA Disposition Services;
Shared	Other DoD Components	Specify.	Department of the Air Force; Department of the Army; Department of the Navy/U.S. Marine Corps;
Shared	Other Federal Agencies	Specify.	Department of Education;
Shared	State and Local Agencies	Specify.	County or City Governments; State Government Agencies; Law Enforcement Agencies (LESO) All States, Counties, Cities can have access if they apply
Shared	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.	Contractor: Credence Management Solutions Limited (SP4709-17-D-0034 - SP4709-23-F-0100 expiring 7/31/2025) FAR 52.224-3, Privacy Training (Jan 2017) Contractor: LOGC2 (SP4709-17-D-0019 - SP4709-23-F-0022 expiring 3/31/2026) FAR 52.224-3, Privacy Training (Jan 2017)
Shared	Other (e.g., commercial providers, colleges)	Specify.	None

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

- Individuals
- Existing DoD Information Systems
- Databases

The user inputs their information into AMPS which feeds into Active Directory. Our application retrieves their credentials from the Active Directory to authenticate users.

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

- E-mail
- Information Sharing - System to System
- Website/E-Form (Enter link(s) in box below.)

Users are required to input their information when accessing this site: https://pep1.bsm.dla.mil/.

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)? No

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.

If "Yes," enter the SORN System Identifier

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

Information is collected via AMPS which uses the DLA Privacy Act System Notice S500.55, entitled "Information Technology Access and Control Records.

I. 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.

8180.01; 1000.07; 1405.04; 3020.01; 4200.07; 4200.08; 5010.61; 5010.76; 5300.09; 5300.12; 5300.13; 5300.15; 5300.16; 5300.21

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

(3) Retention Instructions.

-8180.01- File Plan-Office Information Listing: Temporary. Cutoff at end of Event. Event is when superseded.
-1000.07- Reorganization Planning: Destroy after 5 years.

-1405.04 - Position Descriptions (PDs) - Official Record Copy of Position Description: Destroy 2 years after position is abolished or description is superseded.

-3020.01 - Continuity of Operations (COOP) Planning and Related Emergency Planning Files: Destroy/delete when 3 years old or 3 years after superseded or obsolete, whichever is applicable.

-4200.07 - Contracting Officer's Representative (COR) / Contracting Officer's Technical Representative (COTR) Files: Destroy 10 years after final payment or cancellation.

-4200.08 - Contract Files: Destroy 10 years after final payment or cancellation.

- 5010.61 - Strategic Planning - Directorate and Division Offices: Destroy when superseded or no longer needed for reference.

-5010.76 - Interagency and Inter/Intraservice Agreements- Other Office: Temporary. Cutoff at end of CY.

-5300.09 - Meeting Documentation - Destroy no sooner than 1 year or when no longer required, as identified by internal business rules.

- 5300.12 - Office Administrative Records and Routine Correspondence: Destroy when 2 years old, or when no longer needed, whichever is sooner.

- 5300.13 - Office Studies and Analyses - Destroy when 3 years old or 3 years after superseded, as appropriate.

- 5300.15 - Staff Visits - Destroy when 2 years old.

- 5300.16 - Office Time Keeping Records - Destroy after GAO audit or when 3 years old, whichever is sooner.

- 5300.21 - Supervisor's Personnel Files: Temporary- Review annually and destroy superseded or obsolete documents, or destroy file relating to an employee within 1 year after separation or transfer.

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.

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.

No

(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.