PRIVACY IMPACT ASSESSMENT (PIA)

For the

DLA Learning Management System (LMS) and DLA Competency Assessment/ Workforce Planning (CA/WP)
Defense Logistics Agency

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	New DoD Information System	☐	New Electronic Collection
☒	Existing DoD Information System	☐	Existing Electronic Collection
☐	Significantly Modified DoD Information System		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	Yes, DITPR	Enter DITPR System Identification Number	6020 (LMS) and 3135 (CA/WP)
☐	Yes, SIPRNET	Enter SIPRNET Identification Number	
☐	No		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐	Yes	☒	No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒	Yes	☐	No

If "Yes," enter Privacy Act SORN Identifier: S335.01

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

5 U.S.C. Chapter 41, The Government Employees Training Act;
10 U.S.C. 1701 et seq., Defense Acquisition Workforce Improvement Act;
E.O. 9397 (SSN);
E.O. 11348, Providing for the further training of Government employees, as amended by E.O. 12107, Relating to the Civil Service Commission and labor-management in the Federal Service;
5 CFR part 410, Office of Personnel Management-Training.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The Learning Management System (LMS) is used to manage and administer DLA's learning programs and to provide a means through which employees may identify, manage, and complete learning requirements on a timely basis. The Competency Assessment/Workforce Planning tool (CA/WP) is part of the LMS application.

Information is used to manage and administer training and development programs; to identify individual training needs; to screen and select candidates for training; and for reporting and financial forecasting, tracking, monitoring, assessing, and payment reconciliation purposes. Statistical data, with all personal identifiers removed, are used to compare hours and costs allocated to training among different DLA activities and different types of employees.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards described in this document. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.
Administrative: Employee records are maintained on servers that are located in a controlled secured area with access limited to authorized personnel. Authorized personnel with a need-to-know are granted physical access to computing facilities. Personnel that process sensitive information or unclassified information have been cleared with background investigations and granted approval for access. Devices that display or output sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information and are located in 24x7 physically secured locked area.
Technical: The links to Learning Management System applications are located on web servers accessible only to internal users.
Physical: Employee records are maintained by the DLA Human Resources Center and DLA Training Center, in a physically secured area and by authorized personnel that receive initial and Annual IA training in the operation of Security policies. Individuals requiring access to sensitive information are processed for access authorization in accordance with DOD personnel security policy.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Employee's supervisor, DLA Human Resources personnel

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. To the Department of Veterans Affairs for inspecting, surveying, auditing, or evaluating apprentice or on-the-job training programs. To the Department of Labor for inspecting, surveying, auditing, or evaluating apprentice training programs and other programs under its jurisdiction. To Federal agencies for screening and selecting candidates for training or developmental programs sponsored by the agency. To Federal oversight agencies for investigating,

reviewing, resolving, negotiating, settling, or hearing complaints, grievances, or other matters under its cognizance.

☒ **State and Local Agencies.**

Specify. To Federal, state, and local agencies and oversight entities to track, manage, and report on mandatory training requirements and certifications.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Data may be provided to public and private sector educational, training, and conferencing entities for enrollment, tracking, evaluation, and payment reconciliation purposes. The DoD 'Blanket Routine Uses' set forth at the beginning of DLA's compilation of systems of records notices apply to this system.

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

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Privacy act statement is on the LMS website. DISCLOSURE IS VOLUNTARY. Providing the requested data is voluntary. However, failure to provide all data requested may result in inability to authorize training.

(2) If "No," state the reason why individuals cannot object.

j. 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.

Privacy act statement is on the LMS website. DISCLOSURE IS VOLUNTARY. Providing the requested data is voluntary. However, failure to provide all data requested may result in inability to authorize training.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

PRIVACY ACT STATEMENT

Purpose: Information about you is collected to manage and administer training and development programs. We will use the data to identify your individual training needs; to screen and select you as a possible candidate for training; and for reporting, financial forecasting, tracking, monitoring, assessing, and payment reconciliation purposes. Your SSN is collected to positively identify you. Statistical data, with all personal identifiers removed, may be used by management for program evaluation and review.

Authority: 5 U.S.C. Chapter 41, The Government Employees Training Act; 10 U.S.C. 1701 et seq., Defense Acquisition Workforce Improvement Act; E.O. 9397 (SSN); E.O. 11348, Providing for the further training of Government employees, as amended by E.O. 12107, Relating to the Civil Service Commission and labor-management in the Federal Service; and 5 CFR part 410, Office of Personnel Management-Training.

Routine Uses: Data may be provided to public and private sector educational, training, and conferencing entities for enrollment, tracking, evaluation, and payment reconciliation purposes. Data may also be disclosed to Department of Veterans Affairs; the Department of Labor; Federal and state safety and environmental agencies; and Federal oversight agencies for screening, evaluation, managerial, review, or investigative purposes. Data may also be disclosed for any of the "Blanket Routine Uses" published by DLA in the "Preamble" to Record Systems Notices subject to the Privacy Act, available at http://www.defenselink.mil/privacy/notices/dla/.

DISCLOSURE IS VOLUNTARY. Providing the requested data is voluntary. However, failure to provide all data requested may result in our inability to authorize training for you.

Rules of Use: Rules for collecting, using, retaining, and safeguarding this information are contained in DLA Privacy Act System Notice S335.01, available at http://www.defenselink.mil/privacy/notices/dla/.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.