



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Distributed Learning System (DLS) Incr. 1-3 v3.0

Program Executive Office, Enterprise Information Systems - Office of the Assistant
Secretary of the Army for Acquisition, Logistics, and Technology

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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 0626 - DA01315
- 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 007-21-02-42-02-0688-00

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 Covered under ATRRS SORN (A0351 DAPE) per OSD

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. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army and 4301; and E.O. 9397 as amended (SSN).

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.

DLS provides the infrastructure for delivery/management of training, in support of individual, group/collective task training. Benefits include increased training effectiveness/efficiency, improved readiness, and increased training for customers. DLS Objective: streamline/automate training, training support, training management tasks for the Army using commercial technologies; support Training Mission Area (TMA). Key customers: Soldiers (Active, National Guard, and Reserve), Army Civilians. Key stakeholders: Army Training and Doctrine Command, Forces Command, Army Materiel Command, Program Executive Officer – Enterprise Information Systems, Army General Staff.

DLS provides the following capabilities using Commercial-Off-The-Shelf (COTS) solutions: (1) Digital Training Facilities (DTF): electronic classrooms at fixed locations, capable of delivering multimedia courseware, so that students can perform self-paced training or participate in group training events. (2) Enterprise Management Center (EMC): centralized system management of the DLS information resources. (3) Army Learning Management System (ALMS): A web-based information system for centralizing, standardizing, and optimizing training, training management, and training delivery functions under a single system containing all the necessary TMA capabilities and ingredients for mission success. (4) Deployed Digital Training Campuses (DDTC) (in testing) electronic mobile classrooms, capable of delivering multimedia courseware, so that students can perform self-paced instruction or participate in group training events in a deployed location, (5) Army e-Learning: web-based commercial information technology training products for use by Soldiers and civilians to acquire and sustain business, information technology or language skills.

As a whole, DLS facilitates the TMA mission to teach technical and tactical proficiency, develop military occupational specialty (MOS) skills, develop Leaders, support Army Training Transformation, promote self-development, and sustain individual and unit combat skills.

PII collected is personal and military information.

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

The security countermeasures employed mitigate the risk to PII rather than increase or enhance any inherent risks. DLS Incr. 1-3 v3.0 is a Mission Assurance Category II/ Sensitive system that employs FIPS 140-2 encryption standards and enforces Public Key Infrastructure authentication among many other technical security safeguards that protect the integrity of the information it stores/processes/transmits.

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.

The information will only be shared within Department of the Army, and will only be used to identify valid students within the DLS/ATRRS/AKO architecture. Army organizations sharing information are with Army Personnel Systems: Army Human Resources Command G-1 (ATRRS), US Army

Reserve (RPAS), and USA National Guard (RCAS).

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify.

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

Specify.

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.

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

PII is not collected from the individuals, but extracted from AKO via an encrypted LDAP query. Since the information is extracted from AKO, the user has already consented to use.

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.

[Empty light blue box]

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

PII is not collected from the individuals, but extracted from AKO via an encrypted LDAP query. Since the information is extracted from AKO, the user has already consented to use.

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.

[Empty light blue box for describing applicable formats]