



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Army Training Information Architecture - Learning Management System (ATIA - LMS)
U.S Army Training and Doctrine Command (TRADOC)

### **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
- 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

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.

10 U.S.C. 3013, Secretary of the Army; Army Regulation 350-1, Army Training and Leader Development; and E.O. 9397 (SSN), as amended.

**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 ATIA LMS is a Learning Management System (LMS), which manages the student administration, student participation, printing and distribution of the Army's approximately 1600 sub courses and 325 courses in support of the Army's non-resident training – the Army Correspondence Course Program (ACCP). The system supports 26 army schools and provides service to a worldwide student load of approximately 500,000 military and civilian personnel. The system supports both interactive online training as well as paper based instruction and evaluations. The system is open to personnel from all services and is used by the Army to award promotion points to Active, Reserve, and National Guard enlisted soldiers based upon participation in the ACCP. Information collected: Personal, education and training information.

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

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. The risk associated with providing an individual the opportunity to object or consent is that the individual's personal information can not be maintained, updated or verified.

**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.

Army Staff Principals in the chain of command, Department of the Army Inspector General, Army Audit Agency, U.S. Army Criminal Investigation Command, United States Army Intelligence & Security Command (INSCOM), Provost Marshal General, National Guard Bureau (NGB), and Assistant Secretary of the Army (Financial Management and Comptroller).

**Other DoD Components.**

Specify.

Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General and Defense Criminal Investigation Service.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

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

Specify. RAYTHEON (Prime), CAPSTONE(sub), PROSOFT (sub); in their roles as TSDD contractors will be managing the development, test and production environments. . Contract language: Must maintain information assurance and access controls required to process and maintain sensitive data and data subject to the Privacy Act.

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.

Personal information is already gained through interfaces with other active and reserve AISs, such as the National Guard Bureau (NGB), Reserve Component Automation System (RCAS), Retirement Points Accountability System (RPAS) and the Army Training Requirements and Resources System (ATRRS). Individuals are provided the opportunity to edit and validate personal information at the Reception Battalions (RECBNS). Individuals initially provide PII to the Army during in-processing at recruitment phase and IET for personnel purposes. Personnel are furnished appropriate Privacy statements and given the opportunity to object at that time.

**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.

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

PII is already gained through other in-processing procedures and captured in other system that ATIA LMS interfaces with. When individuals initially provide PII to the Army for personnel purposes they are furnished appropriate Privacy Act Statements and given the opportunity to object/consent at that time. Therefore, all

information is obtained previously and the system-to-system interface does not provide alterations to the user's ability to give/withhold consent during this phase of the lifecycle.

**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.

During inception into the Army (recruitment and IET), individuals provide PII to the Army for personnel purposes. Personnel are furnished appropriate Privacy Act Statements and given the opportunity to object/consent at that time.

**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.**