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:

United States Army Information Assurance Virtual Training Classroom (USAIAVTC)

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

08/25/20

CIO/G6 Cybersecurity Directorate

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] 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.

The U.S. Army Information Assurance Virtual Training Classroom is a hardware enclave and software system that provides hands-on training capabilities to the U.S. Army personnel using web and virtual training machine technology. Specific courses are Cybersecurity-related and all content is delivered over the web using a secure sandbox environment hosted on the LMS itself. System is a CIO/G6 sponsored project that extends the reach of training on Cybersecurity related topics including proper configuration and use of various Cybersecurity tools. The system can be used as a technical reference/knowledge base for Cybersecurity workforce attempting to accomplish complex tasks and needing to go back and look at the knowledge material in real-time. The system also hosts the Army Training and Certification Tracking System that manages the 8570.01-M inputs automatically upon completion of various courses and certifications. Type of PII include: EDIPI (DoD ID Number), Name, Official duty address/work email address, education information, Official Duty telephone, position/title, rank/grade, personnel security information (i.e. ITI, ITII, ITIII), AKO username

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)*

PII collected for official DOD use to include verification, identification and authentication of administrative and mission-related collected data; selected PII collected from individuals to obtain/access to training and certification data from DoD and other Army systems.

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.

This is controlled through the EAMS-A system. All documents requiring the collection of PII have a Privacy Act Statement that explains why the information is being collected and the user has the option not to provide PII information.

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.

All documents requiring the collection of PII have a Privacy Act Statement that explains why the information is being collected and the user has the option not to provide PII information.

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 ☒ Privacy Advisory ☒ Not Applicable

The System advisory starts with: You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.The Privacy Advisory noted on documents requiring some PII starts with:
DATA REQUIRED BY THE PRIVACEY ACT OF 1974
AUTHORITY: E.O. 10450 and Public Law 99-474, the Computer Fraud and Abuse Act
PRINCIPAL PURPOSE:
ROUTINE USES:
DISCLOSURE:

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

☐ Within the DoD Component	Specify.	None
☐ Other DoD Components	Specify.	We do not share the information with outside agencies
☐ Other Federal Agencies	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.	NACON is the contractor providing support and maintenance for the Army Training and Certification Tracking System and the IAVTC. The NACON developers have access to the production database. The contractor shall implement, and maintain appropriate Cybersecurity management, operational and technical controls and processes to ensure compliance to DOD and DA requirements. The contractor shall ensure appropriate CS controls are implemented to provide for non-repudiation, confidentiality, integrity, and availability of the systems and data. As a minimum, the contractor shall ensure adequate Cybersecurity and surety to include any activities required for system accreditation or certification including Approval to Operate (ATO) and annual security review, Backing up data and maintaining a capability to provide disaster, recovery of capability and data in the event of catastrophic failure, and any other activities required by the Army Cybersecurity Directorate
☐ 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)*

☒ Individuals ☐ Databases
☒ Existing DoD Information Systems ☐ Commercial Systems
☐ Other Federal Information Systems

USAIAVTC (IAVTC & ATCTS)

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

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

Minimal PII information is received from the Enterprise Access Management Service-Army (EAMS-A) system.

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 A0351b TRADOC DoD, Army Training I

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. GRS 2.6, item 30 (DAA-GRS-2016-0014-0003)

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

(3) Retention Instructions.

25-2n - KN. Destroy when superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for business use

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.

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

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.

Per DoD Manual 8910.01, Volume, paragraph 2(b) - this volume does not apply to Component internal information collections that do not collect information from members of the public. Public information is not collected.