PRIVACY IMPACT ASSESSMENT (PIA)

For the

Distance Learning System (DLS)
Defense Threat Reduction Agency (DTRA)

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 9327

☐ **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 007-000001815

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 HDTRA 014, Student Records

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 (request is pending)

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
5 U.S.C. 4103, Establishment of Training Programs
10 U.S.C. 1701 Management Policies
E.O. 11348, Providing for the further training of Government employees
5 CFR part 410, Office of Personnel Management-Training
E.O. 9397 (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.

This commercial-off-the-shelf application tracks and maintains an individual student training history and provides a platform for on-line training and in-residence on-line training registration for civilian, military, and contractor students. Retained data includes name, social security number, occupational series, grade, and supervisory status, registration, student development curriculums, and training data, including start and completion dates, course descriptions, and related data. Where training is required for professional licenses, certification, or recertification, the file may include proficiency data in one or more skill areas. Electronic records may contain computer log-on data and personal emergency contact information. Statistical data, with all personal identifiers removed, are used to compare training completion data and service agency and organization quota reports. The system prepares student roster lists for class instructors.

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

The privacy risk is primarily unauthorized disclosure to persons without a need to know. Technical and administrative controls are in place to reduce the risk of unauthorized disclosure. System users receive periodic training on information security and PII handling requirements.

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. Manually, to track, manage, and report on mandatory training requirements and certifications and for screening and selecting candidates for training or developmental programs sponsored by the agency.

☒ **Other DoD Components.**

Specify. Manually, to DoD components to track, manage, and report on mandatory training requirements and certifications and for screening and selecting candidates for training or developmental programs sponsored by the agency.

☒ **Other Federal Agencies.**

Specify. Manually, to Federal agencies and oversight entities to track, manage, and report on mandatory training requirements and certifications and for screening and selecting candidates for training or developmental programs sponsored by the agency.

☒ **State and Local Agencies.**

Specify. Manually, to 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. Manually, to public and private sector educational, training, and conferencing entities for participant enrollment, tracking, evaluation, and payment reconciliation purposes.

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.

Individuals can object to the collection of information in an identifiable form about themselves before completing the appropriate DNWS DLS New Student Data form. On-line submittal of this form indicates consent. Information on individuals' training completion is automatically updated for on-line courseware and obtained from the class roster for in-residence instructor-led courses. All forms and databases used have a Privacy Act Statement on them. Documentation for non-DTRA-provided training is provided by the individual. Failure to provide information may result in the individual being unable to participate in or receiving credit for the involved 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.

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

Failure to provide information may result in the individual being unable to participate in or receiving credit for the involved training.

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.	A Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), is provided on DTRA/SCC-WMD Form 34, "DTRA/SCC-WMD Defense Nuclear Weapons School Course Registration" when personal data is collected. The Statement provides the following: Federal Statute(s) and/or Executive Order(s) that authorizes the collection of personal information; the purpose for collecting the information; external disclosures and uses of the information; the voluntary nature of the program and the fact that no consequences accrue for those who choose not to participate. The Statement is included on paper and/or electronic collection forms.

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.