

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:

Security Education Training Environment (SETE)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

10/17/25

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- ☐ From members of the general public ☐ From Federal employees
- ☒ from both members of the general public and Federal employees ☐ Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one.)

- ☐ New DoD Information System ☐ New Electronic Collection
- ☒ 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.

SETE is a Software-as-a-Service (SaaS), Impact Level 4 (IL4) learning delivery platform designed to support the DCSA's Director mission as the DoD functional manager for security education and training, to include the delivery of controlled unclassified information (CUI) designated training materials.

SETE leverages multiple software services offerings such as FedRAMP-Authorized Hosted Learning Management Systems (LMS), System Integration, Student Information Systems & Transcript Management, Agile Solution Development, Cybersecurity Services, COTS & Open-Source Solutions, and Data Analytics & Metrics.

SETE collects information about individuals to track training. System users include DoD enterprise military and civilians, including cleared industry, federal agencies. After the user registers for courses, the Registrar's Office (RO) validates the assignment of course workload/training to ensure user roles align with the courses taken. The RO consists of DCSA Human Capital Management Office (HCMO) government and contractor personnel. SETE is not the system of record for student training records. Training completions will not be stored in SETE but will be sent to the Security Training, Education, and Professionalization Portal (STEPP) repository, which is part of the Federal Learning Enclave (FLE).

User Profile data includes complete contact information including first/last name, email, position title, title/rank, status civ/mil/other, military/GS grade, highest level of education, mailing address, DCSA org code, program area (security specialty area), and supervisor name and contact info. The system does not contain or use social security numbers or date of birth.

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)

To establish and retain a permanent enrollment record of students, course completions, certifications, and academic credits/transcripts.

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

Applicants are provided notice and the ability to consent, in the form of a Privacy Act Statement that is part of the system banner, at the original point of entry into the information system. External DoD users may decline providing their data, however, doing so may result in denial of access into the system.

f. 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.

If individuals choose to consent to the PAS in the system banner then they are consenting to the uses of their PII as outlined in the SORN DoD-0005 and PAS.

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

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. The USG may inspect and seize data stored on this IS at any time. Communications or data stored on this IS are not private and are subject to routine monitoring, interception, search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests, not for your personal benefit or privacy.

By proceeding, you also consent to the following Privacy Act Statement:

(1) Authority: Title 5, United States Code (USC), Section 301; 5 U.S.C. Chapter 41, Training; 5 CFR part 410, Office of Personnel Management-Training; E.O. 11348, Providing for the Further Training of Government Employees, as amended by E.O. 12107; Executive Order 10450. "Security Requirements for Government Employment;" Executive Order 9397, "Numbering System for Federal Accounts Relating to Individual persons;" Executive order 10865, "Safeguarding Classified Information within Industry;" and DoD Directive 5105.42, "Defense Security Service."

(2) Purpose: The Security Education Training Environment (SETE) is a learning delivery platform designed for security education and training, to include the delivery of controlled unclassified information (CUI) designated training materials. The purpose of the requested information is for the Defense Counterintelligence and Security Agency (DCSA) to establish and retain a permanent enrollment record of students, course completions, certifications, and academic credits/transcripts.

(3) Routine Uses: In addition to those disclosures generally permitted under 5 USC 522A (b) of the Privacy Act, Executive Order 0307, System of Records Notice (SORN) DoD 0005 (<https://www.federalregister.gov/documents/2020/12/28/2020-26548/privacy-act-of-1974-system-of-records>), and Public Law 104-134 (April 26, 1996), SETE uses student accounts as numerical identifiers for students and professional certification candidates/holders. It uses PII to respond to requests, provide SETE services, and communicate information and offers about DCSA products, services, and events. SETE will not share data outside of DCSA unless authorized in the published SORN.

(4) Disclosure: Disclosure is voluntary. However, failure to provide the requested information will impede, delay, or prevent further access to SETE.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component?

(Check all that apply)

☒ Within the DoD Component

Specify.

CDSE, OCIO / Federal Learning Enclave (FLE) will manually receive completion information (name, email, grade) upon course completion, which will be uploaded into the Security, Training, Education, and Professionalization Portal (STEPP).

☐ Other DoD Components (i.e. Army, Navy, Air Force)

Specify.

☐ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

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.

Contractor personnel (PowerTrain) must complete the annual Security and Privacy Awareness training as a condition of employment. This training outlines their accountability for safeguarding PII. A contract modification is underway to address privacy requirements within the contract.

☐ 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

Data exchange from STEPP to SETE

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) |
| ☐ In-Person Contact | ☐ Paper |
| ☐ Fax | ☐ Telephone Interview |
| ☐ Information Sharing - System to System | ☒ Website/E-Form |
| ☒ Other (If Other, enter the information in the box below) | |

SETE accounts are created by the Registrar's Office as a part of the CUI enrollment process on STEPP. STEPP will be the system of record and the location for any information about students or registration.

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.dod.mil/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.

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

(3) Retention Instructions.

Enrollment, Registration and Course Completion Records: Maintained for 10 years; Training Division Course Records: Destroy 1 year after; Certification Program Records: Hold certification for 1 year after new certification then destroy

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 statute 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.

Authorities, listed in DoD-Wide Training Records SORN (DoD-0005): 5 U.S.C. Chapter 41, Training; 5 CFR part 410, Office of Personnel Management-Training; 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; 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1746 Defense Acquisition University; 10 U.S.C. 1747, Acquisition Fellowship Program; DoD Instruction 1215.08 Senior Reserve Officers Training Corp Programs; DoD Directive 1322.18, Military Training; DoD

Directive 1322.08E, Voluntary Education Programs for Military Personnel; DoD Instruction 1322.26, Distributed Learning; DoD Instruction 1322.25, Voluntary Education Program; DoD Instruction 1322.9, Job Training, Employment Skills Training, Apprenticeships, and Internships (JTEST-AI) for Eligible Service Members; DoD Instruction 1430.16, Growing Civilian Leaders; DoD Instruction 5132.13, Staffing of Security Cooperation Organizations (SCOs) and the Selection and Training of Security Cooperation Personnel; DoD Instruction 1215.21, Reserve Component (RC) Use of Electronic-based Distributed Learning; Directive-Type Memorandums 13-004, Operation of the DoD Financial Management Certification Program Methods for Training; and DoD Instruction 1015.2, Military Morale, Welfare and Recreation (MWR), DoD Instruction 1300.26, Operation of the DoD Financial Management Certification Program; and E.O. 9397.

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 ☒ 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.

SETE user accounts are created within STEPP and therefore the user data is considered regurgitated information. Therefore, an OMB control number is not needed.