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:

Cyber Workforce Compliance Management System

2. DOD COMPONENT NAME:

Defense Logistics Agency (DLA)

3. PIA APPROVAL DATE:

12/08/2025

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- From both members of the general public and Federal employees

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

- New 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.

DLA 8140 Certification Tracking tool will identify requirements, track status, and report on Cyber Space Workforce Requirements (8140) for DLA Enterprise-wide for government civilians, contracting support, and military personnel. A privacy overlay is required due to required PII elements for the system. Overall privacy risk impact level is low.

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)*

Verification, identification, authentication, data matching, mission-related use, and administrative use.

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

Yes

(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.

User accepts via a consent option prior to application entry.

f. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes

(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.

User accepts via a consent option prior to application entry.

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

Please select your DoD PIV/Authentication certificate to access the application.

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.
● At any time, the USG may inspect and seize data stored on this IS.
● Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USGauthorized purpose.
● This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
● Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

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:

Full Statement

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

Shared	Within the DoD Component	Specify.	D-Staff (Director/Vice Director/Staff); DLA Human Resources (J1); DLA Information Operations (J6);
Not Shared	Other DoD Components	Specify.	
Not Shared	Other Federal Agencies	Specify.	
Shared	State and Local Agencies	Specify.	No information will be shared with any state, county, city, for foreign governments.
Shared	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.	CyberSTAR...Shall not publish or disclose without KO's written consent...Safeguard against threats and hazards to security, integrity, and confidentiality of Government data...If any new or unanticipated hazards are discovered, shall bring attention to parties involved.
Shared	Other (e.g., commercial providers, colleges)	Specify.	PII is not shared with any other entities

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- Individuals
- Existing DoD Information Systems
- Other Federal Information Systems

Input into CWCMS and info obtained from DCPDS (for civilians).

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

- Information Sharing - System to System

direct input and uploads into CWCMS

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)? Yes

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.

If "Yes," enter the SORN System Identifier DoD 0005; 5 U.S.C. Chapter 41; 5 CFR part 410; E.O. 11348; E.O. 12107; 10 U.S.C. 113; 10 U.S.C. 136;

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Officer for additional information or http://dpcld.defense.gog/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 (DPCLD). Consult the DoD Component Privacy Officer 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.

I. 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.

3110.04-Professional Development Certification

Temporary. Cutoff at end of Event. Event is when employee transfers or is no longer needed. Destroy/delete when no longer needed or if employee transfers, forward to gaining organization required.

DAA-0361-2021-0018-0003

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

(3) Retention Instructions.

3110.04-Professional Development Certification

Temporary. Cutoff at end of Event. Event is when employee transfers or is no longer needed. Destroy/delete when no longer needed or if employee transfers, forward to gaining organization required.

DAA-0361-2021-0018-0003

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.

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.

No

(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.