



DOD 8140 LEARNING MODULES V2.0

PUBLISHED JULY 2026



Purpose: The purpose of the DoD 8140 Learning Modules is to introduce Department of War (DoW) cyberspace (cyber) workforce concepts and activities to DoW cyber workforce (CWF) management teams, with the goal of applying the DoD 8140 policy consistently across DoW Components.

Change Management: This document consolidates the below listed resources published by the DoW Chief Information Officer (CIO) Workforce Innovation Directorate (WID) from 2024-2025 into one resource via an administrative update. If you have a question, please connect with your supervisor, or contact with one of the mailboxes found in Appendix A.

Module 2, “An Introduction to DoD 8140 Policy” has absorbed the “DoD 8570 IA Program Transition to DoD 8140 Cyber Workforce Qualification Program” Module.

Resource Title
Module 1: An Introduction to DoD 8140 Policy
Module 2: DoD Cyber Workforce Strategy Alignment to DoD 8140
Module 3: An Introduction to Warfighting Acquisition University DCWF Credentials (Learning Playlists)
DoW CIO WID Instructor-Led Training: An Introduction to DoD 8140 Foundational Qualifications

At time of publication, DoW CIO WID Instructor-Led Training on DoD 8140 foundational qualifications is provided to DoW Component CWF management teams virtually via Microsoft Teams and on an as-needed basis to support enduring DoD 8140 CWF reporting activities as described in DoDM 8140.03, “Cyberspace Workforce Qualification and Management Program” (February 15, 2023).

This document is unclassified and was prepared by the DoW CIO WID.

The effective date of this document is July 1, 2026.



Module 1:

An Introduction to DoD 8140 Policy

Historical Background Knowledge: The Department of Defense (DoD) 8140 Cyber Workforce Qualification Program establishes the current framework and standards for cyber workforce management, optimizing technical and management qualifications across the enterprise.

This policy supersedes and replaces the legacy DoD 8570 Information Assurance (IA) Program.

Previously, under DoD 8570, the program's focus was to assure IA compliance regarding the development, operation, management, and enforcement of system functions including detection, reaction, and restoration.

The program's focus was to assure IA compliance regarding the development, operation, management, and enforcement of system functions including detection, reaction, and restoration. DoD 8570 baseline qualifications included:

1. Three functional certification levels (I, II, III) for the IA Technical, IA Management, IA System Architect and Engineer categories indicating scope of responsibilities in an enclave's hierarchy.
 - Level 1: Computing Environment IA
 - Level 2: Network Environment IA
 - Level 3: Enclave and Advanced Network IA
2. Certifications for "Computer Network Defense-Service Provider Specialties" as applicable to IA positions, subsequently re-described as "Cybersecurity Service Provider Specialties" for Analyst, Infrastructure Support, Incident Responder, Auditor, & Service Provider Manager mapped to IA functional levels.
3. Additional computing environment and/or operating system certificates were required based on the particular requirements of a system environment.

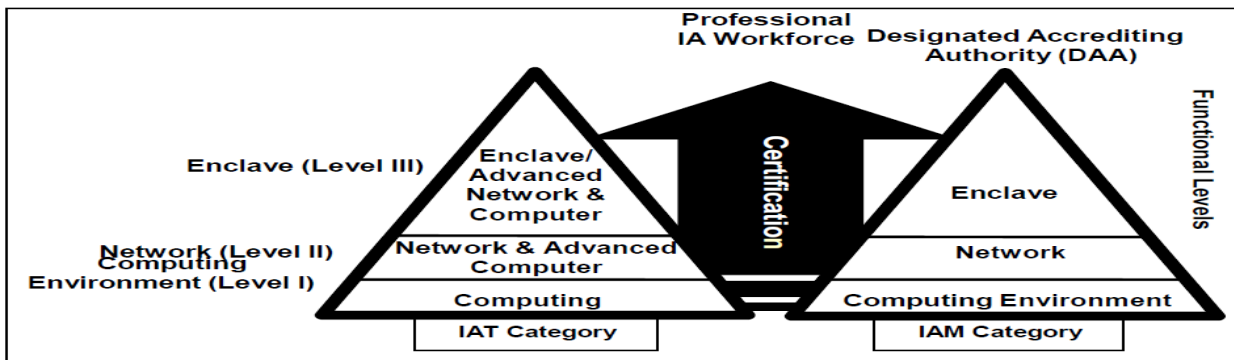


Figure 2: DoD 8570 IA Program

Federal Cybersecurity Workforce Assessment Act (FCWAA) of 2015: Congress introduced the requirements of the identification and coding of Federal positions requiring the performance of “information technology (IT), cybersecurity (CS), or other cyber-related functions through the implementation of the FCWAA of 2015 (Sections 303 and 304 of Public Law 114-113), transforming the DoD’s cyber workforce (CWF) focus from information assurance to a broader view of the CWF comprising personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources, conduct related intelligence activities, enable future operations, and project power in or through cyberspace.

Transition Period: The Department of War (DoW) formally began its transition period from the DoD 8570 Information Assurance (IA) Workforce Improvement Program upon release of the DoD Manual, DoDM 8140.03, “Cyberspace Workforce Qualification and Management Program” on February 15, 2023, transforming an IA compliance-based approach to a focus on the demonstration of knowledge and capability.

DoD 8140 Foundational Knowledge: The information documented throughout the rest of this module provides a high-level overview of DoD 8140 policy tenants and benefits when applied properly, and can be used to develop DoD 8140 training sessions and talking points.

- ✓ The DoD 8140 Cyber Workforce Qualification Program (CWQP) leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).



- ✓ The DoD 8140 CWQP unifies the overall DoW CWF and organizes the DCWF into seven elements:
 1. Information Technology (IT)
 2. Cybersecurity (CS)
 3. Cyber Enablers (EN)
 4. Cyber Effects (CE)
 5. Intelligence (Cyber)
 6. Data/Artificial Intelligence (Data/AI)
 7. Software Engineering (SE)
- ✓ The DoD 8140 CWQP is designed to be:
 - **Flexible:** DoW Components can tailor DoD 8140 residential qualification requirements based on the mission and environment.
 - **Adaptive:** The DoD 8140 CWQP will continue to evolve to meet the needs of the DoW CWF.
 - **Responsive:** The ability to identify and track DCWF work roles and measure DoW CWF qualification at three different proficiency levels allows senior leaders to assess DoW CWF readiness in a timely manner.
- ✓ The DoD 8140 CWQP addresses the scope of expertise needed for all cyber disciplines, using a comprehensive approach for CWF talent management.
- ✓ The DoD 8140 policy governs all cyber positions and personnel across the DoW, regardless of personnel or pay system (e.g., General Schedule (GS), Cyber Excepted Service (CES), Defense Civilian Intelligence Personnel System (DCIPS), Acquisition Demonstration (AcqDemo)).

DoW Cyber Workforce Management Board: In accordance with DoD Directive 8140.01, the DoW Cyber Workforce Management Board (CWMB), is chartered as the Senior Executive Service (SES)/General/Flag Officer (GO/FO) level decision body on behalf of DoW Components. The CWMB Tri-Chairs are 1) The Under Secretary of War for Personnel and Readiness (USW P&R), 2) The Principal Cyber Advisor (PCA), and 3) the DoW Chief Information Officer (CIO).

Position Coding: See the DoW CIO Workforce Innovation Directorate (WID)'s guidance on *DCWF Workforce Identification and Coding Guidance* (updated annually) for additional information.



Proficiency Levels: See the DoW CIO WID's guidance on *DoD 8140 Proficiency Levels* (August 2024) for additional information.

Foundational Qualifications: DoD 8140 foundational qualification options (education, training, personnel certifications, and the conditional alternative (experience)) are tailored to each DCWF work role and DoD 8140 proficiency level. DoW CWF personnel who achieve DoD 8140 foundational qualification within the first nine months of assignment to a DCWF work role demonstrate 70% or more of the knowledge required for the applicable DCWF work role, which is measured by core task and KSA alignment. DoW-provided training options include, but are not limited to, the Warfighting Acquisition University (WarU) DCWF Credentials (Learning Playlists) detailed in Module 3.

Policy Fundamentals:

1. The nine-month foundational qualification timeline begins for a DoW CWF member (MIL/CIV) when they are coded to a DCWF work role at the assigned proficiency level.
2. DoW CWF members must complete any one of the foundational qualification options to satisfy the foundational portion of qualification. DoW Components may dictate more stringent requirements in addition to the options found in the DoD 8140 foundational qualification matrix published by the DoW CIO.
3. Training and personnel (industry) certifications must cover 70% of core task and knowledge, skill, and ability content of the DCWF work role appropriate for the applicable proficiency level before being approved as a foundational qualification option.
4. A DoD 8140 approved training or degree may be used to satisfy foundational qualification as far back as continuous cyber work can be verified.

Residential Qualifications: DoD 8140 residential qualifications (on-the-job & environment specific) are developed and implemented by the DoW Component and provide the opportunity for DoW CWF personnel to demonstrate capability in a mission environment against the assigned DCWF work role and DoD 8140 proficiency level. DoW CWF personnel must complete their DoW Component's DoD 8140 residential qualification requirements within twelve months of a DCWF work role and proficiency level assignment.

Continuous Professional Development: Upon attainment of both DoD 8140 foundational and residential qualification, DoW CWF personnel are required to complete 20 hours of continuous professional development per fiscal year. This requirements begins after the CWF member has satisfied both DoD 8140 foundational and residential qualification requirements.



IT Privileged Access: DoD 8140 does not specify IT privileged access requirements (i.e., those with access to elevated control functions of systems & networks). DoW CWF positions with privileged access should be coded with appropriate DCWF work role code(s). DoW Components may apply additional requirements for training and tracking purposes.

		Basic	Intermediate	Advanced
Foundational Qualification Options – Demonstration of Knowledge	Education	Option	Option	Option
	Training (DoD & Commercial)	OR Option	OR Option	OR Option
	Personnel Certification	OR Option	OR Option	OR Option
	Experience	Conditional Alternative	Conditional Alternative	Conditional Alternative
Residential Qualification – Demonstration of Capability	On-the-Job Qualification	Always Required	Always Required	Always Required
	Environment Specific Requirements	Component Discretion	Component Discretion	Component Discretion
Maintain Currency	Continuous Professional Development	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.

Figure 3: Sample DCWF Work Role Qualification Matrix



Module 2:

DoD Cyber Workforce Strategy Alignment to DoD 8140

Historical Background Knowledge: The Department of Defense (DoD) Cyberspace Workforce Strategy (DCWS) was originally published in December 2013 as overarching enterprise guidance for the DoD cyberspace (cyber) workforce. The DCWS initiated DoD cyber workforce (CWF) management tenets, advocated for the expansion of hiring and retention authorities, and introduced cyber-threat awareness for all DoD personnel. This strategy also launched the effort for creation of the Department Cyber Workforce Framework (DCWF). Notably, the first focal area of the DCWS stated:

“Establish a cohesive set of DoD-wide cyberspace workforce management issuances. A single set of DoD policies and directives will be established, reconciled with existing Information Technology/Information Assurance (IT/IA), Intelligence and Operations policies and directives, for building a qualified and adaptable cyberspace workforce. This is a key strategic point required to set the cyberspace workforce standards and guide the Department; by identifying cyberspace work roles, the required qualifications, and parameters for managing the workforce.”

This Strategy builds upon DoW CWF management efforts developed over the past 20 years, while moving forward with specific actionable and measurable outcomes.

Module 3 Overview: The DoD Cyber Workforce Strategy (2023-2027) sets the foundation for how the DoW will foster a CWF capable of executing the Department’s complex and varied cyber missions and provides a unifying direction for DoW CWF management activities. The DoD CIO released the DoD Cyber Workforce Strategy Implementation Plan in August 2023 to carry out actions and initiatives to achieve the strategic goals that build and strengthen the Nation’s most valuable cyber asset: our highly skilled workforce.

This Strategy outlines four overarching goals supported by 22 objectives and 38 initiatives that specify activities, targets, milestones, and key performance indicators (KPIs) to measure progress and evaluate the effectiveness of each objective. Four human capital pillars provide the Strategy’s foundation. Data-driven metrics are utilized to assess status of the pillars, as well as forecast future trends, for talent management.



DoW Cyber Workforce Vision

To drive the development of the workforce that supports the Department's cyber mission, making it the most capable and dominant force in the world.

GOAL 1: Identify requirements to stay ahead of force needs. Execute consistent capability assessment and analysis processes.

GOAL 2: Develop people and capabilities to address current and future requirements. Establish an enterprise-wide talent management program to better align force capabilities with requirements.

GOAL 3: Facilitate a cultural shift to optimize human capital management activities and decisions based on data-driven metrics.

GOAL 4: Foster partnerships and collaboration for development of capabilities, operational effectiveness, and career broadening experiences.



Figure 2: DoD Cyber Workforce Strategy Overview

This Strategy highlights actions for human capital strategic planning informed by DoW CWF analytics garnered from DoD 8140 requirements. Successful execution of the Strategy and achieving these goals will enable the DoW to close CWF development gaps, apply resources for CWF initiatives, stay at the forefront of technological advances, securely and rapidly deliver resilient systems, and assess CWF readiness using data analytics.



ACTIONS FOR BUILDING A CAPABLE AND DOMINANT DoW CYBER WORKFORCE

IDENTIFICATION: Determine workforce requirements through accurate work role coding of positions.

RECRUITMENT: Identify and attract talent with skills needed for missions by leveraging all Federal and DoD processes and HR authorities.

DEVELOPMENT: Promote advancement of skills with developmental programs

RETENTION: Target incentives for desired skills and abilities.

CWF Strategy Goal 1: Execute consistent capability assessment and analysis processes to stay ahead of force needs.

Objective 1.3: Utilize advanced analytic capabilities to increase the speed, accuracy and efficiency of capability and requirement reviews.

Initiative 1.3.1: Implement a DoD 8140 Qualification Program data maturity roadmap to drive the DoD toward enterprise-wide CWF analytics. This roadmap supports data-driven talent management of critical skillsets and CWF analytics capability to deliver data in a timely manner for recruitment, development, and retention decision-making.

Figure 3: DoD 8140 Alignment to DoD CWF Strategy



Module 3:

An Introduction to Warfighting Acquisition University DCWF Credentials (Learning Playlists)

Module Overview: The Warfighting Acquisition University (WarU) offers a suite of targeted courses, workshops, and credentials (formerly learning playlists) designed to meet the standards of the DoD 8140 Cyber Workforce Qualification Program.

Specifically, the WarU Department Cyber Workforce Framework (DCWF) Credentials (Learning Playlists) outlined in this module are formally approved to satisfy the DoW training foundational qualification option for DCWF cybersecurity (CS), information technology (IT), and cyber enabler (EN) work roles at the designated proficiency level.

By completing a designated WarU DCWF Credential, cyber workforce (CWF) members can meet the foundational qualification requirement for their assigned DCWF work role, often at little to no cost to their command. These credentials provide a structured, DoW-provided alternative to education, commercial training or personnel certifications.

At time of document publication, additional WarU DCWF training opportunities have been developed to support DoD 8140 continuous professional development, but these trainings do not satisfy DoD 8140 foundational qualification requirements.

It is recommended that supervisors of CWF members consider WarU for training as a low/no-cost option for their DoD 8140 foundational and/or residential qualification requirements.

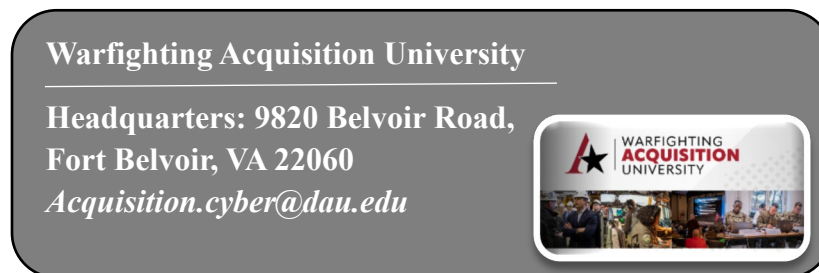
These credentials are regularly updated as new training curriculum is designed to prepare learners for their DCWF work role. As updates are completed, the training course content is updated on the associated WarU DCWF Credential webpages.

Consultation with your supervisor is always recommended prior to enrollment in any DoD 8140 foundational qualification option to verify current requirements.



At time of document publication, all WarU DCWF Credentials can be successfully completed virtually; no in-person attendance is required.

This module was prepared by the DoW CIO WID and coordinated with WarU.



*Figure 1: Warfighting Acquisition University
DCWF Learning Playlist Visual*

Change Management Log: The below menus have been modified since the publication of WarU DCWF Credential alignment (August, 2025), to reflect current offerings.

In accordance with the Office of the Secretary of War, the Defense Acquisition University has been re-named to Warfighting Acquisition University (WarU).

With the update from “Learning Playlists” to “Credentials,” WarU has introduced completion certificates at the completion of this training. Maintaining this certificate in the appropriate authoritative systems of record is critical to verify CWF personnel have met DoD 8140 foundational qualification requirements through this training option.

This document serves as an extension of the DoD 8140 foundational qualification matrix, which is updated on a regular basis. WarU DCWF Credential removals, modifications, and updates may occur at any time. If you have a question, please connect with your supervisor.



DCWF Work Role	DoD 8140 Basic	DoD 8140 Intermediate	DoD 8140 Advanced
(IT-441) Network Operations Specialist	<i>External Content; DCWF DISA Training</i>	<i>External Content; DCWF DISA Training</i>	<i>No Coverage; Consider a different option</i>
(IT-451) System Administrator	<i>External Content; DCWF DISA Training</i>	<i>External Content; DCWF DISA Training</i>	<i>No Coverage; Consider a different option</i>

Table 1: Change Management Log

WarU DCWF Credential Search Menu Walkthrough: This section briefly walks the user through the WarU DCWF Credential webpages and provides additional information, including web links.

A list of WarU DCWF Credentials can be found at the following link:

https://www.waru.edu/playlists?field_playlist_last_modified_value=1&sort_by=title&sort_order=ASC&playlist-search=DCWF&items_per_page=25

When you visit the webpage, search your DCWF work role in the search tab at the top of the menu to find approved credentials that correspond to your DCWF coding assignment and proficiency level.

Additional cyber courses are available through the iCatalog at ***<https://icatalog.dau.edu/>*** and the WarU Learning Search Menu. For questions or concerns regarding the WarU DCWF Credentials, please connect with the Warfighting Acquisition University team at ***acquisition.cyber@dau.edu***

Please see the next page.



Most Recent

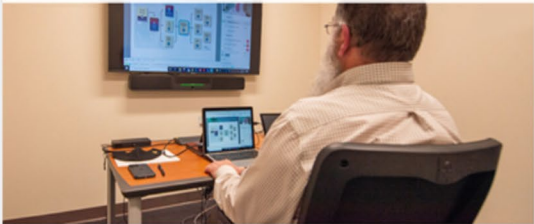
A-Z

DCWF

20 Results

DAU

Virtual Instructor-led Training



DCWF Cyber Defense Analyst (511)
- Basic Foundational Training
Playlist

This learning pathway provides Defense Acquisition University (DAU) courses and workshops that enable the learner to meet the training...

Playlist

DAU

Workshop



DCWF Cyber Defense Analyst (511)
- Intermediate Foundational
Training Playlist

This learning pathway provides Defense Acquisition University (DAU) courses and workshops that enable the learner to meet the training...

Playlist

Figure 2: WarU DCWF Learning Playlist Search Menu

PLAYLIST

DAU

Virtual Instructor-led Training



Event

CYB 5640V Cyber Training Range

Request

DAU

Workshop



Event

WSS 011 Cyber Training Range – Intermediate

Request

Figure 3: Warfighting Acquisition University DCWF Learning Playlist Search Menu





Finding Your WarU User ID and Troubleshooting: Users can find their WarU User ID by following the steps outlined below. If you have additional questions, or if you require assistance with trouble shooting, please contact WarU at acquisition.cyber@dau.edu

Finding your DAU USER ID

If you have an Active DAU ID you can Find it by Logging into the DAU Virtual Campus

Step 1: Log into the DAU Virtual Campus (<https://dau.csod.com>) with your Username/Password or CAC.

Step 2: Mouse over the Home menu at the top left and select **Universal Profile**.

Step 3: Mouse over the Bio menu and select **About**. Your User ID will be displayed on the page. When you find it ...

Step 4: Go to this location (Customer POC - PUTS DIRECTIONS/LOCATION HERE) and enter your DAU ID.

Step 5: If you completed Steps 1 – 4, this means you have an active DAU account and you are done.

Note: If you were unable to get past Step 1, please go to the next slide and continue with Step 6

Note: Your User ID should look something like this: DAU0512900055

10/31/2022

DAU

Figure 4: Finding Your DAU User ID



Find/Get a DAU USER ID and Activate

- If you were unable to login to the DAU Virtual Campus, you may not have an account OR your account may currently be inactive. Proceed with Steps 6 – 11 below.

Submit the DAU Systems Authorization Access Request (SAAR).

Step 6: Go to <https://saar.dau.edu> (Recommended browser is Microsoft Edge).

Step 7: Fill out the SAAR form.

Step 8: You should receive a **Welcome to DAU** email from noreply@dau.edu within 2 hours, which includes a link to activate your account. If you do not receive the email, please [contact the DAU Help Desk](#) for further assistance.

Step 9: Complete the account activation process using the link in the automated email you receive. Guidance is available at [this location](#).

Step 10: After activating your account, click the **Virtual Campus** tile on your dashboard. This will take you into your Virtual Campus account and automatically activates your student account.

Step 11: Go back to **Steps 2 -3** to locate your DAU ID. Then go to this location (Customer POC - PUTS DIRECTIONS/ LOCATION HERE) and enter your DAU ID

Note: Your User ID should look something like this: DAU0512900055

10/31/2022

DAU

Figure 5: Find/Get A WarU User ID and Activate



Troubleshooting

- Learners needing assistance activating their DAU ID or require assistance submitting the DAU SAAR should contact the DAU Help Desk.
 - Help Desk Hours of Operation: Monday-Friday, 0600-2000 Eastern
 - Phone: 703-805-3459 | 866-568-6924 | DSN: 655-3459; Option 1
 - Public Service Portal: https://services.dau.edu/psp?id=public_portal

10/31/2022

DAU

Figure 6: Troubleshooting



WarU DCWF Credential Coverage: *The below tables outline the alignment of WarU DCWF Credentials to DCWF CS, IT, and EN work roles and corresponding DoD 8140 proficiency levels.*

DCWF Cyber Enabler (EN) Work Roles (Acquisition Workforce)

DCWF Work Role	DoD 8140 Basic	DoD 8140 Intermediate	DoD 8140 Advanced
(EN-801) Program Manager	✓	✓	✓
(EN-802) IT Project Manager	✓	✓	✓
(EN-803) Product Support Manager	✓	✓	✓
(EN-804) IT Investment/Portfolio Manager	✓	✓	✓
(EN-805) IT Program Auditor	✓	✓	✓
All Other Cyber Enabler Work Roles	No Coverage; Consider Cyber 101	No Coverage; Consider Cyber 101	No Coverage; Consider Cyber 101

Table 2: Warfighting Acquisition University DCWF Credential Coverage For DCWF Cyber Enabler Work Roles (Acquisition Workforce)



DCWF Information Technology (IT) Work Roles

DCWF Work Role	DoD 8140 Basic	DoD 8140 Intermediate	DoD 8140 Advanced
(IT-411) Technical Support Specialist	✓	✓	✓
(IT-421) Database Administrator	✓	✓	No Coverage; Consider a different option
(IT-431) Knowledge Manager	✓	✓	✓
(IT-441) Network Operations Specialist	✓	✓	No Coverage; Consider a different option
(IT-451) System Administrator	✓	✓	No Coverage; Consider a different option
(IT-632) Systems Developer	✓	✓	✓
(IT-641) Systems Requirements Planner	✓	✓	✓
(IT-651) Enterprise Architect	✓	✓	✓
(IT-661) Research & Development Specialist	✓	✓	✓
(IT-671) System Testing and Evaluation Specialist	✓	✓	✓

Table 3: Warfighting Acquisition University DCWF Learning Playlist Coverage For DCWF Information Technology (IT) Work Roles



DCWF Cybersecurity (CS) Work Roles

DCWF Work Role	DoD 8140 Basic	DoD 8140 Intermediate	DoD 8140 Advanced
(CS-212) Cyber Defense Forensics Analyst	✓	No Coverage; Consider a different option	No Coverage; Consider a different option
(CS-462) Control Systems Security Specialist	No Coverage; Consider a different option	No Coverage; Consider a different option	✓
(CS-511) Cyber Defense Analyst	✓	✓	✓
(CS-521) Cyber Defense Infrastructure Support Specialist	✓	✓	No Coverage; Consider a different option
(CS-531) Cyber Defense Incident Responder	✓	✓	No Coverage; Consider a different option
(CS-541) Vulnerability Assessment Analyst	✓	✓	✓
(CS-611) Authorizing Official/Designated Rep.	✓	✓	✓
(CS-612) Security Control Assessor	✓	✓	✓
(CS-622) Secure Software Assessor	No Coverage; Consider a different option	No Coverage; Consider a different option	No Coverage; Consider a different option
(CS-631) Information Systems Security Developer	✓	✓	No Coverage; Consider a different option
(CS-652) Security Architect	✓	✓	✓
(CS-722) Information Systems Security Manager	✓	✓	✓
(CS-723) Communications Security Manager	✓	✓	✓

Table 4: Warfighting Acquisition University DCWF Learning Playlist Coverage For DCWF Cybersecurity (CS) Work Roles



Appendix A: Governance & References

Document Title	Web Link
DoDD 8140.01	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf
DoDI 8140.02	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/814002p.PDF
DoDM 8140.03	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/814003p.pdf

Appendix B: DoD 8140 Ask A Question

DoW Component	Web Link
Army	(CIO Policy) usarmy.pentagon.hqda-cio.mbx.policy-inbox@army.mil (CIO SAIS-CSP Policy) usarmy.pentagon.hqda-cio.mbx.sais-csp@army.mil (DCS, G6) usarmy.belvoir.hqda-cio.mbx.training-and-certification@army.mil
Navy	NavyCWF@us.navy.mil
Marine Corps	IDI_Team@usmc.mil
Air Force	(Military) USAF_17X_Career_Field_Manager@us.af.mil (Civilians) SAF.CNSF.Workflow@us.af.mil
OSD, 4 th Estate, Federal Government, Commercial Partners	osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil

If you have additional questions, please contact your local CWF Program Manager, if applicable, and then contact with one of the mailboxes listed above.

Online Resources: The DoD 8140 Home Page serves as the central repository for all authoritative cyber workforce information, including news and announcements, policy, guidance, and training resources. It is available at: <https://www.cyberworkforce.mil/DoD-8140/>