Top Headlines

- DoD Cyber Workforce Management Update Provided to Members of Congress
- Preparations Underway for DoD 8140 Cyberspace Workforce Annual Report Tasker
- DCWF IT Workforce Element Work Role Refresh Underway
- DCWF Work Role Tool V5.1 Published

DoD Cyber Workforce Management Resource Spotlight

DCWF Work Role Tool V5.1
(New Excel Tool)
Effective Date: July 25, 2025

DoD 8140 Foundational Qualification Matrix V2.0
(Excel)
Effective Date: March 25, 2025

DoD 8140 Cyberspace Workforce Compliance Brief V3.0
Effective Date: June 11, 2025

Figure 1: DoD Cyber Workforce Management Resource Spotlight

Bulletin Appendices

- **A:** DCWF Elements Map: DoD 8140 Cyberspace Workforce Annual Report Focus
- **B:** DCWF IT Work Role Refresh Memo, June 2025
- **C:** DoD CIO IT Privileged User Memo, April 2024
- **D:** An Introduction to DAU DCWF Learning Playlists V2.0, August 13, 2025
- **E:** DoD 8140 Experience Working Group Minutes, July 30, 2025
- **F:** DoD 8140 Academic Accreditation GS-15 Decision Brief Minutes, July 31, 2025

DoD Cyber Workforce Management Roadshow Sprint

Bulletin Overview

- In accordance with DoDD 8140.01, "Cyberspace Workforce Management" (October 5, 2020), this bulletin provides updates from the DoD CIO WID to DoD Components regarding implementation of the DoD 8140 Cyber Workforce Qualification Program.
- Information regarding broader DoD cyber workforce operations and management activities are also noted in this edition.
- The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense (DoD) of the linked websites, or the information, products or services contained therein. The DoD does not exercise any editorial, security, or other control over the information you may find at these locations.

DoD Cyber Workforce Management Roadshow Sprint

Summary

The DoD CIO team recently briefed DoD cyber workforce management updates at several engagements to showcase recent successes of the DoD cyber workforce in alignment with national defense priorities. Of note, Mr. Mark Gorak, Director DoD's Cyber Academic Engagement Office (CAEO), provided an update to U.S. House Representatives Ms. Betty McCollum (D) and Mr. Brad Finstad (R) from Minnesota. This update focused on the DoD cyber workforce vacancy rate, DCWF work role coding, and DoD 8140 qualifications. The DoD CIO WID has also published a DoD Cyber Service Academy (CSA) testimonial. These engagements helped raise awareness on DoD cyber workforce initiatives and CAEO's efforts to build a cyber talent pipeline to support the warfighter.

Associated video and article links can be found on the next page.

Mark Gorak | Director | DoD Cyber Academic Engagement Office
DoD Cyber Workforce Management Update at the National Cybersecurity Workforce Showcase
Defense.gov | Author: Matthew Olay | Date: June 25, 2025
Link: *https://www.defense.gov/News/News-Stories/Article/Article/4225669/senior-official-promotes-bolstering-dod-cyber-workforce/*

Mark Gorak | Director | DoD Cyber Academic Engagement Office
DoD Cyber Workforce Management Update at Hammercon | June 2025
Video posted by the Military Cyber Professionals Association
Link: *https://www.youtube.com/watch?v=NgSJpaaaRt8*

Patrick Johnson | DoD CIO WID | Director
DoD Cyber Workforce Management Update at ISC2 SECURE | June 2025
Linkedin Post provided by the DoD CIO
Link: *https://www.linkedin.com/company/dod-cio; See June 24, 2025 post*

Alfredo Rodriguez | DoD CIO WID | DoD Cyber Workforce Data and Analytics Program Lead
DoD Cyber Workforce Coding and Qualification Brief at Hammercon | June 2025
Video by the Military Cyber Professionals Association
Link: *https://www.youtube.com/watch?v=2TuFKcAZxSI*

Ms. Cathryn Allen | DCWF (CE-341-B) Cyberspace Capability Developer
DoD Cyber Service Academy Testimonial | July 2025
Video by Mr. Miguel La Porte, DoD CIO WID
Link: *https://www.dvidshub.net/video/969236/dod-csa-alumnus-testimonial-series-ms-cathryn-allen*

Figure 2: DoD Cyber Workforce Management Roadshow Sprint

DoD CIO WID Prepares for Release of DoD 8140 Cyberspace Workforce Annual Report Qualification Collection Tasker

Summary

The DoD CIO WID has taken steps to ready the DoD cyber workforce for its next DoD 8140 Cyberspace Workforce Annual Report, with the official tasker scheduled to be released in the Fall of 2025. This report will ingest DoD 8140 foundational qualification data for the DCWF cybersecurity (CS), information technology (IT), and cyber enabler (EN) workforce elements, along with DoD 8140 residential qualification data reporting for the DCWF CS workforce, excluding work role (CS-462) Control Systems Security Specialist. This data will measure the readiness of the DoD cyber workforce and is scheduled to be briefed at a future DoD Cyber Workforce Management Board.

DCWF IT Workforce Element Work Role Refresh Underway

Summary

The DCWF IT workforce element work role refresh is underway and will allow Services and Components to provide input on knowledge, skill, ability, and task modifications for each IT workforce element work role.

CATMS Tasker Reference:
CIO000448-25-240625-XQ4M

Figure 3: DCWF Seal

List of Impacted DCWF IT Work Roles

(IT-411) Technical Support Specialist: Provides technical support to customers who need assistance utilizing client level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable).

(IT-421) Database Administrator: Administers databases and/or data management systems that allow for the storage, query, and utilization of data.

(IT-431) Knowledge Manager: Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

(IT-441) Network Operations Specialist: Plans, implements, and operates network services/systems, to include hardware and virtual environments.

(IT-451) System Administrator: Installs, configures, troubleshoots, and maintains hardware, software, and administers system accounts.

(IT-632) Systems Developer: Designs, develops, tests, and evaluates information systems throughout the systems development lifecycle.

(IT-641) Systems Requirements Planner: Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

(IT-651) Enterprise Architect: Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

(IT-661) Research and Development Specialist: Conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

(IT-671) System Testing and Evaluation Specialist: Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

DoD 8140 Cyber Academic Alignment Team Update

Summary

In coordination with the DoD Cyber Academic Engagement Office (CAEO), the DoD CIO WID collaborated with 75 U.S. academic institutions from across the country to deliberate and enhance the DoD 8140 foundational qualification matrix for education, related to DCWF IT work roles. This activity was a success for the DoD cyber workforce, adding an additional 53 IT-related degree disciplines into the DoD 8140 foundational qualification matrix. At time of document publication, the final report and matrix update is pending final approval by the DoD CIO WID.

Figure 4: DoD 8140 Qualification Approval Process for Education

The DoD CIO WID plans to re-engage with U.S. academic institutions in the Winter of calendar year 2026 to review and align cybersecurity-related degree disciplines; Additional guidance to follow. Collaboration with U.S. academic institutions is and will be another important focus area to support DoD cyber workforce management activities.

At time of publication, a documented process outlining the steps required to review and approve degrees, along with documenting DoD 8140 quality standards, for DoD 8140 foundational qualification matrix inclusion is in development by the DoD CIO WID.

DoD Cyber Workforce Management Update Briefed at DoD Cyber Service Academy Bootcamp

Summary

The DoD CIO WID provided an update on the DCWF, DoD 8140 qualifications, and the DoD 8140 Cyber Academic Alignment Team initiative to 30 U.S. academic institutions at this year's DoD Cyber Service Academy (CSA) Bootcamp, hosted at George Washington University in Washington, D.C.

The event served as a two-day orientation for students selected through the highly competitive DOD CSA scholarship program, which supports their academic and professional journey toward becoming the next generation of cyber defenders. Nearly 30 professors from designated National Centers of Academic Excellence in Cybersecurity institutions were also in attendance.

Administered by the DoD Chief Information Officer, the DoD CSA, formerly the DoD Cyber Scholarship Program, was established over 20 years ago to help recruit and retain skilled cyber professionals capable of securing the nation's critical infrastructure.

This brief echoed senior leader priorities on championing the DoD CSA to prepare the next generation of cyber talent for the DoD cyber workforce. Check-out the article below for more information!

Cyber Scholars Converge on Washington, Prepare to Defend the Nation's Digital Frontlines

Defense.gov | Author: DoD CIO | Date: July 24, 2025

Link: *https://www.defense.gov/News/News-Stories/Article/Article/4254688/cyber-scholars-converge-on-washington-prepare-to-defend-the-nations-digital-fro/*

DoD Cyber Workforce Management Resource Spotlight

DON Cyber Workforce Program Manager's Desk Guide v1

Published on April 17, 2025, this guide provides a comprehensive framework for understanding and executing the responsibilities of a Department of the Navy Cyber Workforce Program Manager by leveraging available tools and resources. This guide was prepared by:

- OPNAV N2N6D4, *NavyCWF@us.navy.mil*
- USMC IDI Team, *IDI_Team@USMC.mil*

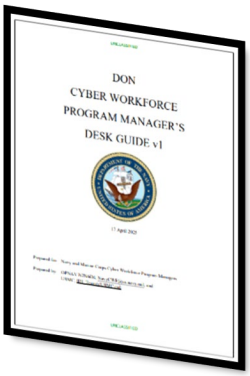


Figure 5: DON CWF PM Guide

Figure 6: DON & USMC Web Logos

Updated DAU DCWF Learning Playlist Module V2.0

This new resource updates the DCWF work role alignment to available Defense Acquisition University (DAU) Learning Playlists, and serves as supporting documentation to the DoD 8140 Foundational Qualification Matrix V2.1, pending final approval by the DoD CIO WID at time of document release. Playlist removals, modifications, and updates will be communicated to the DoD cyber workforce via DAU and DoD CIO WID.

This resource was developed by the DoD CIO WID in collaboration with DAU.

This document is pending upload to the DoD Cyber Exchange.

Figure 7: An Introduction to DAU DCWF Learning Playlists V2.0

Effective Date: August 13, 2025

DoD 8140 Qualification Seminar Announcement

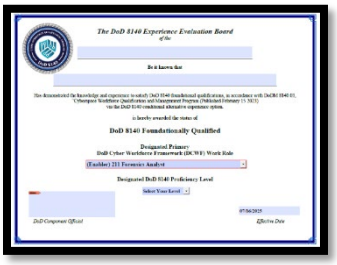
The DoD CIO WID is pleased to host a new DoD 8140 seminar for the DoD cyber workforce: *An Introduction to DoD 8140 Foundational Qualifications.* This seminar will provide an in-depth review of DoD 8140 foundational qualifications, including the submission requirements and ingestion process. Seminar attendance is reserved for DoD civilians, Service members, and DoD contract support personnel, and will be held virtually (MS Teams) on Tuesday September 23, 2025, 1400-1500 Eastern. To register, please contact the DoD CIO WID at the email below.

DoD 8140 Key Point of Contact
Mr. Cameron Myette, DoD CIO WID Contract Support
cameron.r.myette.ctr@mail.mil
Email Subject Line: DoD 8140 Seminar

Publication of Updated DoD 8140 Experience Qualification Process Certificate V3.0

Summary

The DoD CIO WID has updated the DoD 8140 Experience Qualification Process Certificate, which addresses an error regarding DCWF work role number 641 not being reflected properly. This certificate is now labeled V3.0 with an effective date of July 16, 2025. This document was distributed to the DoD cyber workforce via the August 2025 DoD 8140 Readiness Forum, and is pending upload to the DoD Cyber Exchange. The DoD 8140 Experience Qualification Process guide is also being updated through a DoD working group. Please standby for updated guidance.


The DoD 8140 Experience Evaluation Board

DoD 8140 Foundationally Qualified

Figure 8: DoD 8140 EQP Certificate

Effective Date: July 16, 2025

DCWF Cyber Enabler Qualification Governance Deep Dive

Summary

DoDD 8140.01 "Cyberspace Workforce Management" defines the DCWF Cyberspace Enabler (EN) workforce element as: *"Personnel who perform work roles to support or facilitate the functions of cyber IT, cybersecurity, cyberspace effects, or intelligence workforce (cyberspace) work roles. This includes actions to support acquisition, training and leadership activities."*

Through feedback and coordination with DoD Components, the DoD CIO WID concluded that DoD 8140 foundational qualification options that align to a designated DCWF CS or IT work role code and one of the three DoD 8140 proficiency levels satisfies DoD 8140 foundational qualification requirements for all DCWF EN work role codes at all three DoD 8140 proficiency levels. This governance decision allows for the encumbered DCWF EN workforce to leverage their current qualifications to achieve DoD 8140 foundational qualification compliance without the need to enroll in additional training, in this case, Cyber 101.

DoD 8140 Cyber Enabler Qualification Governance Information

Additional Information to Support June 2024 DoD CIO Memo "DoD 8140 Foundational Qualification Options for the Cyber Enabler Workforce Element"

- Attain a DoD 8140 approved degree discipline & associated degree level from an Accreditation Board for Engineering and Technology (ABET) accredited or National Center of Academic Excellence in Cybersecurity (NCAE-C) designated institution within the past 5 years, unless continuous work in the relevant cyber discipline can be demonstrated.
- Attain a DoD 8140 approved DoD training course within the past 5 years, unless continuous work in the relevant cyber discipline can be demonstrated.
- Complete the Cyber 101 (CY101) training course, which can be found on the DoD Cyber Crime Center, https://www.dc3.mil/. DoD civilians and military service members that currently hold a non-cyber related functional community qualification must complete the CY101 training course.
- Complete a cyber-related certification found in the DoD 8140 qualification repository and maintain that certification according to its requirements.

Scenario: A DoD civilian coded to a DCWF (EN-801-A) Program Manager has maintained an active personnel certification that aligns to a DCWF CS or IT work role, at a designated DoD 8140 proficiency level. Does this employee need to successfully complete the DC3 CTA Cyber 101 training course?

Answer: No, in this case, this employee may use the active personnel certification to satisfy DoD 8140 foundational qualification requirements.

DCWF Cyber Enabler (EN) Foundational Qualification Governance Principle

A DoD 8140 approved foundational qualification option aligned to a DCWF CS or IT work role and associated DoD 8140 proficiency level satisfies DoD 8140 foundational qualification compliance for all DCWF EN work roles at all three DoD 8140 proficiency levels.

Figure 9: DCWF EN Foundational Qualification Governance Principle

Proposed Removals of DoD 8140 Foundational Qualification Options

DoD Cyber Workforce Pre-Coordination Announcement

The DoD CIO WID is excited to collaborate with DoD Components on the proposals to remove the following DoD 8140 foundational qualification options for DCWF CS, IT, and EN work roles. If the decision is made to remove these options from the matrix, an enterprise announcement will be provided to DoD Components by the DoD CIO WID. Please standby for additional guidance.

Focus Area	Subject Name	Applicable DCWF Work Roles	Status
(-) Degree Discipline Removal	ABET/NCAE-C B.S. in Data Science	All DCWF IT Work Roles	Pending DoD Coordination
(-) Degree Discipline Removal	ABET/NCAE-C B.S. in Software Engineering	(IT-441-B-I) (IT-451-B-I) (IT-661-B-I)	Pending DoD Coordination
(-) Degree Discipline Removal	ABET/NCAE-C B.S. in Information Systems	(IT-451-B-I) (IT-632-B-I) (IT-641-B-I) (IT-661-B-I) (IT-671-B-I)	Pending DoD Coordination
(-) Degree Discipline Removal	ABET/NCAE-C B.S. in IT	(IT-632-B-I) (IT-661-B-I)	Pending DoD Coordination
(-) Degree Discipline Removal	ABET/NCAE-C B.S. in Computer Science	(IT-641-B-I)	Pending DoD Coordination
(-) Conditional Alternative (Experience)	-	All DCWF CS, IT, EN work roles	Pending DoD Coordination CS: 31DEC2027 IT/EN: 31DEC2028

Frequently Asked Questions

DCWF (IT) 451 System Administrator Implementation

Question: Since the Summer 2025 DoD Cyber Workforce Advisory Group, has there been guidance published by the DoD CIO WID regarding DCWF (IT-451) System Administrator (SA)?

Answer: At time of document publication, an authoritative memo outlining guidance for DoD Components is pending DoD CIO principal level signature. At a high level, mandatory workforce upskilling in response to this circumstance (knowledge, skill, and ability (KSA) modifications) will be covered by DoD Component residential qualifications/training. This will allow DoD Components to ensure that personnel coded to this work role can successfully perform the required work in a timely manner. Upgrades to related DoD 8140 foundational qualifications is anticipated to take place once final guidance is promulgated.

The DoD CIO WID is pursuing options via a designated DoD training provider to support future training mandates in response to potential DCWF KSA modifications, which will allow timely and cost-effective training opportunities to be introduced to the DoD cyber workforce, when applicable.

Once this guidance has been finalized, the DoD CIO WID will communicate this information to DoD Components. Thank you for your patience.

Validation of the Performance of Cyberspace Work

Question: How exactly can a DoD 8140 Experience Evaluation Team validate the performance of cyberspace work? Is additional guidance available?

Answer: The DoD CIO WID is working on the next update of the DoD 8140 Experience Qualification Process (V1.2), which will provide additional clarification on cyberspace work validation, to include instances when personnel use the education or training option to meet DoD 8140 foundational qualifications when the degree or training has been achieved beyond the five year window.

DCWF (SE-461) Systems Security Analyst

Question: Which DCWF workforce element is work role 461 located in?

Answer: DCWF (SE-461) Systems Security Analyst is a part of the DCWF Software Engineering workforce element. This work role transitioned from the DCWF CS workforce element to the DCWF Software Engineering (SE) workforce element on January 13, 2023, per the Cyber Workforce Management Board.

IT Privileged User

Question: Is there additional information available regarding IT privileged users?

Answer: The DoD 8570 to DoD 8140 Info Sheet, page 3 states: *"Privileged Access: DoD 8140 does not specify Privileged Access requirements (i.e., those with access to elevated control functions of systems & networks). Cyber Workforce positions with Privileged Access should be*

coded with appropriate work role code(s). Components may apply additional requirements for training and tracking purposes."
The DoD CIO memo, "Suspension of Information Technology Privileged User Designation Reporting Requirements," signed April 2024, suspends reporting requirements under DoD 8140 policy but *"does not release Components from requirements to identify, train, qualify, manage, track, and report positions and personnel that require IT Privileged User status in accordance with applicable Federal, DoD, Component, and organization policies."*

Privileged Access/Elevated Rights administrative and training requirements are subject to governing organizational policies. For example, IT Privileged User access may be granted for both the Navy and the National Security Agency (NSA) at the same time, but with differing requirements for each type of access and security level. These requirements may be attached to an employee's position (PD/job duties) and/or DCWF work role assigned which means that the training may be part of the job expectations or included in a work role's DoD 8140 residential training program (which may run concurrently with DoD 8140 foundational training).

There was no intent for DoD 8140 policy to "soften" these requirements, only to allow DoD Components the flexibility to tailor them to address specific needs of the security level, enclave/environment, technology parameters, operational mandates, etc.

DAU DCWF Learning Playlists

Question: Do any DAU DCWF learning playlists require on-site attendance?
Answer: Bottom line: No DAU DCWF learning playlists require on-site attendance. All learning assets in DAU playlists are designated as "online" or "ILT/VILT". Online means all content is accomplished by the student without any instructor interactions. The ILT/VILT assets have both VILT (virtual) instructor led training and classroom instructor led training options. Some individuals prefer the classroom environment over the virtual environment. Due to high demand, DAU is now also offering "asynchronous" cyber training range options where students receive a short, virtual instructor led orientation and then students have a set period (one or two weeks) to complete the cyber range curriculum in a self-paced mode.

Quick Case Study: (IT-651) Enterprise Architect: The iCatalog link related to this work role takes you to the concept card for the CYB 5640 course. If you select "apply for this course" in the top right, it will bring you to the course registration page. From there you can surf through the available offerings to find the one right for you. In the description for each offering it includes whether the offering is virtual instructor led, in person classroom or virtual asynchronous, start and end times, time zones, dates and any other pertinent information.

Another registration option is to use the playlist website. Go to the intermediate playlist at *https://www.dau.edu/playlists/dcwf-wrc-651-enterprise-architect-intermediate-proficiency-level-playlist-0*

From here, you can then select "request" to register for each learning asset. The same registration process is used for Virtual Instructor Led (VILT) or for online (no instructor) courses.

Advanced Degree Disciplines for DCWF CS Work Roles

Question: When will options pertaining to the education element for DCWF CS work roles at the DoD 8140 advanced proficiency level become available?

Answer: The DoD CIO WID anticipates holding a DoD 8140 Cyber Academic Alignment Team, with a focus on degree options for DCWF CS work roles, in calendar year 2026. In the interim, please anticipate the advanced level for these work roles to reflect the status of "Under Future Evaluation."

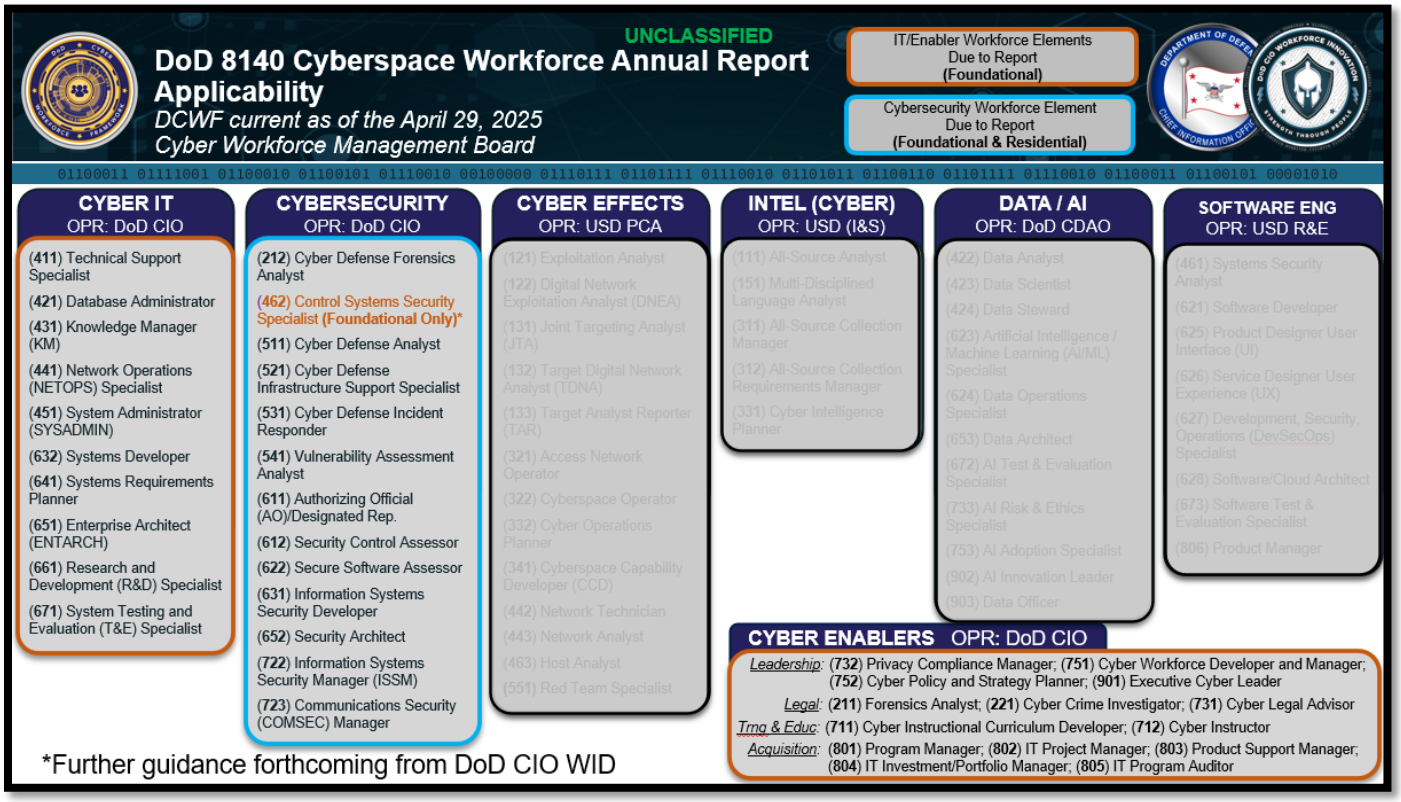
Cyber 101 Enrollment

Question: How long does an DoD cyber workforce member have to complete DC3's Cyber 101 course? Can Cyber 101 be taken virtually?

Answer: Upon the start of enrollment, a DoD cyber workforce member has three weeks to complete the Cyber 101 course. This course can be completed at your own pace, virtually, and will take 40 hours to complete.

APPENDIX A

DCWF Elements Map: DoD 8140 Cyberspace Workforce Annual Report Focus


UNCLASSIFIED
DoD 8140 Cyberspace Workforce Annual Report Applicability
DCWF current as of the April 29, 2025
Cyber Workforce Management Board
IT/Enabler Workforce Elements Due to Report (Foundational)
Cybersecurity Workforce Element Due to Report (Foundational & Residential)
01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010
CYBER IT
OPR: DoD CIO
(411) Technical Support Specialist
(421) Database Administrator
(431) Knowledge Manager (KM)
(441) Network Operations (NETOPS) Specialist
(451) System Administrator (SYSADMIN)
(632) Systems Developer
(641) Systems Requirements Planner
(651) Enterprise Architect (ENTARCH)
(661) Research and Development (R&D) Specialist
(671) System Testing and Evaluation (T&E) Specialist
CYBERSECURITY
OPR: DoD CIO
(212) Cyber Defense Forensics Analyst
(462) Control Systems Security Specialist (Foundational Only)*
(511) Cyber Defense Analyst
(521) Cyber Defense Infrastructure Support Specialist
(531) Cyber Defense Incident Responder
(541) Vulnerability Assessment Analyst
(611) Authorizing Official (AO)/Designated Rep.
(612) Security Control Assessor
(622) Secure Software Assessor
(631) Information Systems Security Developer
(652) Security Architect
(722) Information Systems Security Manager (ISSM)
(723) Communications Security (COMSEC) Manager
CYBER EFFECTS
OPR: USD PCA
(121) Exploitation Analyst
(122) Digital Network Exploitation Analyst (DNEA)
(131) Joint Targeting Analyst (JTA)
(132) Target Digital Network Analyst (TDNA)
(133) Target Analyst Reporter (TAR)
(321) Access Network Operator
(322) Cyberspace Operator
(332) Cyber Operations Planner
(341) Cyberspace Capability Developer (CCD)
(442) Network Technician
(443) Network Analyst
(463) Host Analyst
(551) Red Team Specialist
INTEL (CYBER)
OPR: USD (I&S)
(111) All-Source Analyst
(151) Multi-Disciplined Language Analyst
(311) All-Source Collection Manager
(312) All-Source Collection Requirements Manager
(331) Cyber Intelligence Planner
DATA / AI
OPR: DoD CDAO
(422) Data Analyst
(423) Data Scientist
(424) Data Steward
(623) Artificial Intelligence / Machine Learning (AI/ML) Specialist
(624) Data Operations Specialist
(653) Data Architect
(672) AI Test & Evaluation Specialist
(733) AI Risk & Ethics Specialist
(753) AI Adoption Specialist
(902) AI Innovation Leader
(903) Data Officer
SOFTWARE ENG
OPR: USD R&E
(461) Systems Security Analyst
(621) Software Developer
(625) Product Designer User Interface (UI)
(626) Service Designer User Experience (UX)
(627) Development, Security, Operations (DevSecOps) Specialist
(628) Software/Cloud Architect
(673) Software Test & Evaluation Specialist
(806) Product Manager
CYBER ENABLERS OPR: DoD CIO
Leadership: (732) Privacy Compliance Manager; (751) Cyber Workforce Developer and Manager; (752) Cyber Policy and Strategy Planner; (901) Executive Cyber Leader
Legal: (211) Forensics Analyst; (221) Cyber Crime Investigator; (731) Cyber Legal Advisor
Trng & Educ: (711) Cyber Instructional Curriculum Developer; (712) Cyber Instructor
Acquisition: (801) Program Manager; (802) IT Project Manager; (803) Product Support Manager; (804) IT Investment/Portfolio Manager; (805) IT Program Auditor
*Further guidance forthcoming from DoD CIO WID

APPENDIX B

DCWF IT Work Role Refresh Memo
June 2025

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MEMORANDUM FOR JOINT STAFF DIRECTOR, COMMAND CONTROL, COMMUNICATIONS AND COMPUTERS/CYBER, J6
CHIEF INFORMATION OFFICER, DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER, DEPARTMENT OF THE NAVY
CHIEF INFORMATION DOMINANCE AND CHIEF INFORMATION OFFICER, DEPARTMENT OF THE AIR FORCE
CHIEF INFORMATION OFFICERS, DEFENSE AGENCIES
CHIEF INFORMATION OFFICERS, DOD FIELD ACTIVITIES

SUBJECT: Department of Defense Cyber Workforce Frame Information Technology Element Work Role Refresh

The Department of Defense Cyber Workforce Framework (DCWF) provides a standard cyber workforce lexicon of work roles used for coding positions. Department of Defense Manual (DoDM) 8140.03, "Cyber Workforce Qualification and Management Program," establishes the qualification criteria for each DCWF work role to ensure personnel filling cyber positions are capable of meeting mission requirements. DoDM 8140.03 requires DoD Services and Components to qualify their personnel coded to a DCWF work role. Under the purview of the Cyber Workforce Management Board, the Workforce Innovation Directorate is coordinating with Services and Components to update the Cyber Information Technology (IT) Element work roles. The IT Element refresh requires an update on each of the ten work roles in the element. The refresh will allow Services and Components to provide input on knowledge, skill, ability, and task modifications for each work role. This will be completed via the IT Element Refresh Survey.

Request Services and Components participate in the IT Element refresh by assigning subject matter experts to review and provide input on the content within the work roles via the attached instructions by July 15, 2025.

The point of contact for this matter is Mr. Matthew Isnor, (202) 924-3866, matthew.m.isnor.civ@mail.mil.

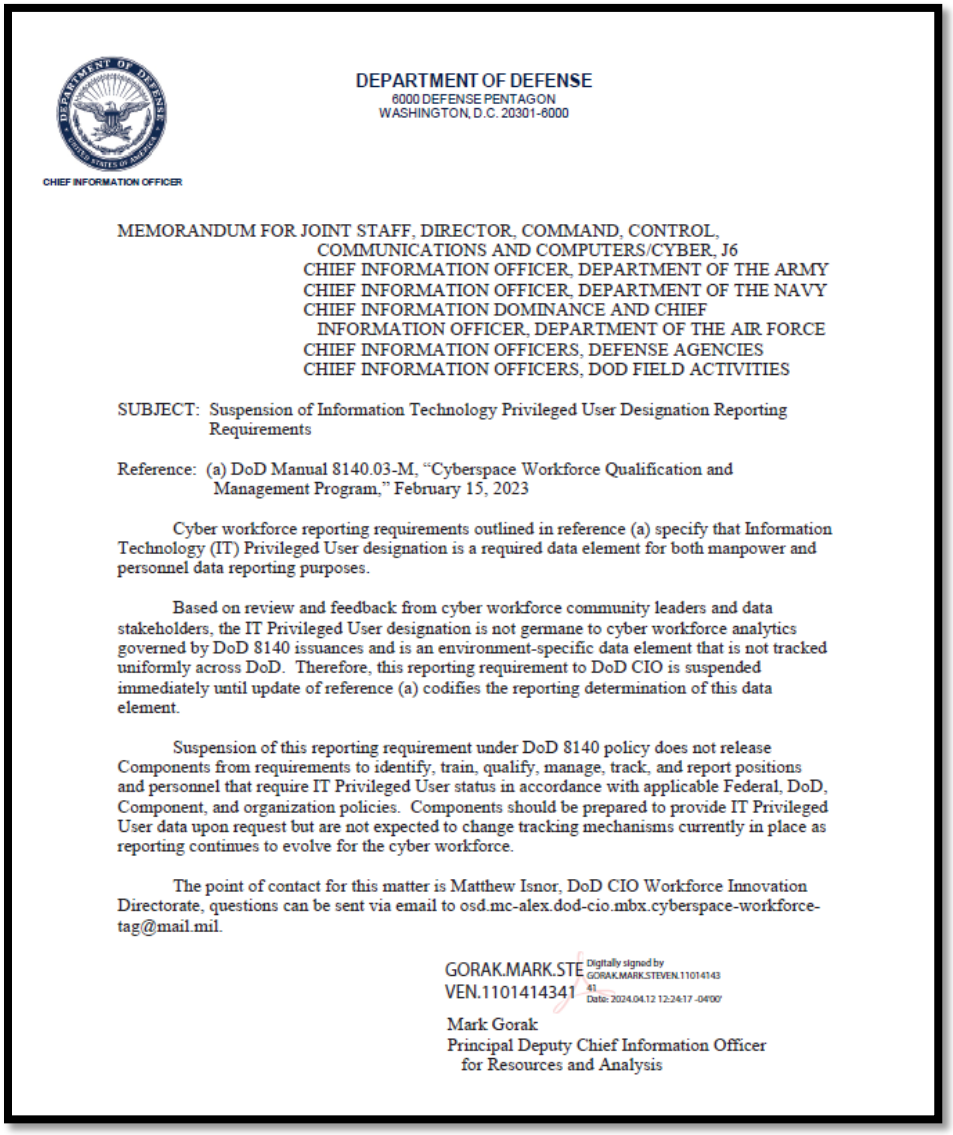
GORAK.MARK.STEVEN.1101414341 Digitally signed by GORAK.MARK.STEVEN.1101414341 Date: 2025.06.25 12:28:12 -04'00'

Mark Gorak
Principal Deputy Chief Information Officer
for Resources and Analysis

Attachment:
As stated

APPENDIX C

DoD CIO IT Privileged User Memo
April 2024



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MEMORANDUM FOR JOINT STAFF, DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS/CYBER, J6
CHIEF INFORMATION OFFICER, DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER, DEPARTMENT OF THE NAVY
CHIEF INFORMATION DOMINANCE AND CHIEF INFORMATION OFFICER, DEPARTMENT OF THE AIR FORCE
CHIEF INFORMATION OFFICERS, DEFENSE AGENCIES
CHIEF INFORMATION OFFICERS, DOD FIELD ACTIVITIES

SUBJECT: Suspension of Information Technology Privileged User Designation Reporting Requirements

Reference: (a) DoD Manual 8140.03-M, "Cyberspace Workforce Qualification and Management Program," February 15, 2023

Cyber workforce reporting requirements outlined in reference (a) specify that Information Technology (IT) Privileged User designation is a required data element for both manpower and personnel data reporting purposes.

Based on review and feedback from cyber workforce community leaders and data stakeholders, the IT Privileged User designation is not germane to cyber workforce analytics governed by DoD 8140 issuances and is an environment-specific data element that is not tracked uniformly across DoD. Therefore, this reporting requirement to DoD CIO is suspended immediately until update of reference (a) codifies the reporting determination of this data element.

Suspension of this reporting requirement under DoD 8140 policy does not release Components from requirements to identify, train, qualify, manage, track, and report positions and personnel that require IT Privileged User status in accordance with applicable Federal, DoD, Component, and organization policies. Components should be prepared to provide IT Privileged User data upon request but are not expected to change tracking mechanisms currently in place as reporting continues to evolve for the cyber workforce.

The point of contact for this matter is Matthew Isnor, DoD CIO Workforce Innovation Directorate, questions can be sent via email to osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil.

GORAK.MARK.STEVEN.1101414341 Digitally signed by GORAK.MARK.STEVEN.1101414341 Date: 2024.04.12 12:24:17 -04'00'

Mark Gorak
Principal Deputy Chief Information Officer
for Resources and Analysis

APPENDIX D

An Introduction to DAU DCWF Learning Playlists V2.0
August 13, 2025

Document Overview

Defense Acquisition University (DAU) DoD Cyber Workforce Framework (DCWF) learning playlists provides courses and workshops that enable the learner to meet the training requirements for identified DCWF work roles. Each level of training builds on the previous level and adds additional training requirements for that level (i.e., Basic, Intermediate, and Advanced DoD 8140 Proficiency Levels).

Figure 1: DAU DCWF Learning Playlists

The courses and workshops contained in these playlists have been evaluated for DCWF knowledge, skill, ability (KSA) and task compliance and meet the foundational qualification minimums for the identified DCWF work role.

DoD cyber workforce supervisors should look to DAU for training as a low/no-cost option for their foundational and/or residential qualification requirements.

These learning playlists are regularly updated as new training curriculum designed to prepare the individual for DCWF work roles is completed. As updates are completed, the training course content is included into the DoD 8140 foundational qualification matrix for identified DCWF work roles.

Consultation with your DoD cyber workforce supervisor is always recommended prior to enrollment in any DoD 8140 foundational qualification option.

At time of document publication, all playlists can be successfully completed virtually; No in-person attendance is required to successfully complete a playlist.

Defense Acquisition University

Headquarters: 9820 Belvoir Road, Fort Belvoir, VA 22060

Acquisition.cyber@dau.edu

Helpdesk: (703) 382-1450 / (866) -568-6924

Figure 2: Defense Acquisition University

DoD 8140 Foundational Qualification Matrix V2.1 Authoritative Qualification Options

Effective Date: Pending Publication

The alignment of DAU DCWF Learning Playlists to the DoD 8140 Foundational Qualification Matrix for CS, IT, and EN work roles has been validated by the DoD CIO WID. This document serves as supporting documentation to the DoD 8140 Foundational Qualification Matrix V2.1, which is pending publication at time of document release. Playlist removals, modifications, and updates will be communicated to the DoD cyber workforce via DAU and DoD CIO WID.

Change Management Log

The below playlists have been added to this document since the publication of version 1.0 in May, 2025.

DCWF Work Role	DoD 8140 Basic	DoD 8140 Intermediate	DoD 8140 Advanced
(CS-541) Vulnerability Assessment Analyst			✓
(IT-441) Network Operations Specialist	✓	✓	
(IT-451) System Administrator	✓	✓	
(IT-671) System Testing and Evaluation Specialist	✓	✓	✓

DAU DCWF Search Menu Walkthrough

This section briefly walks the user through the DAU DCWF Learning Playlist website and provides additional information, including web links.

A list of DAU DCWF learning playlists can be found at the following link: *https://www.dau.edu/playlists*

Search "DCWF" in the search tab at the top of the menu to find learning playlists that correspond to your DCWF work role.

Additional cyber courses are available through the iCatalog at *https://icatalog.dau.edu/* and the DAU Learning search menu. For questions or concerns regarding the DAU DCWF learning playlists, please connect with DAU at *acquisition.cyber@dau.edu*

Please see the next page.

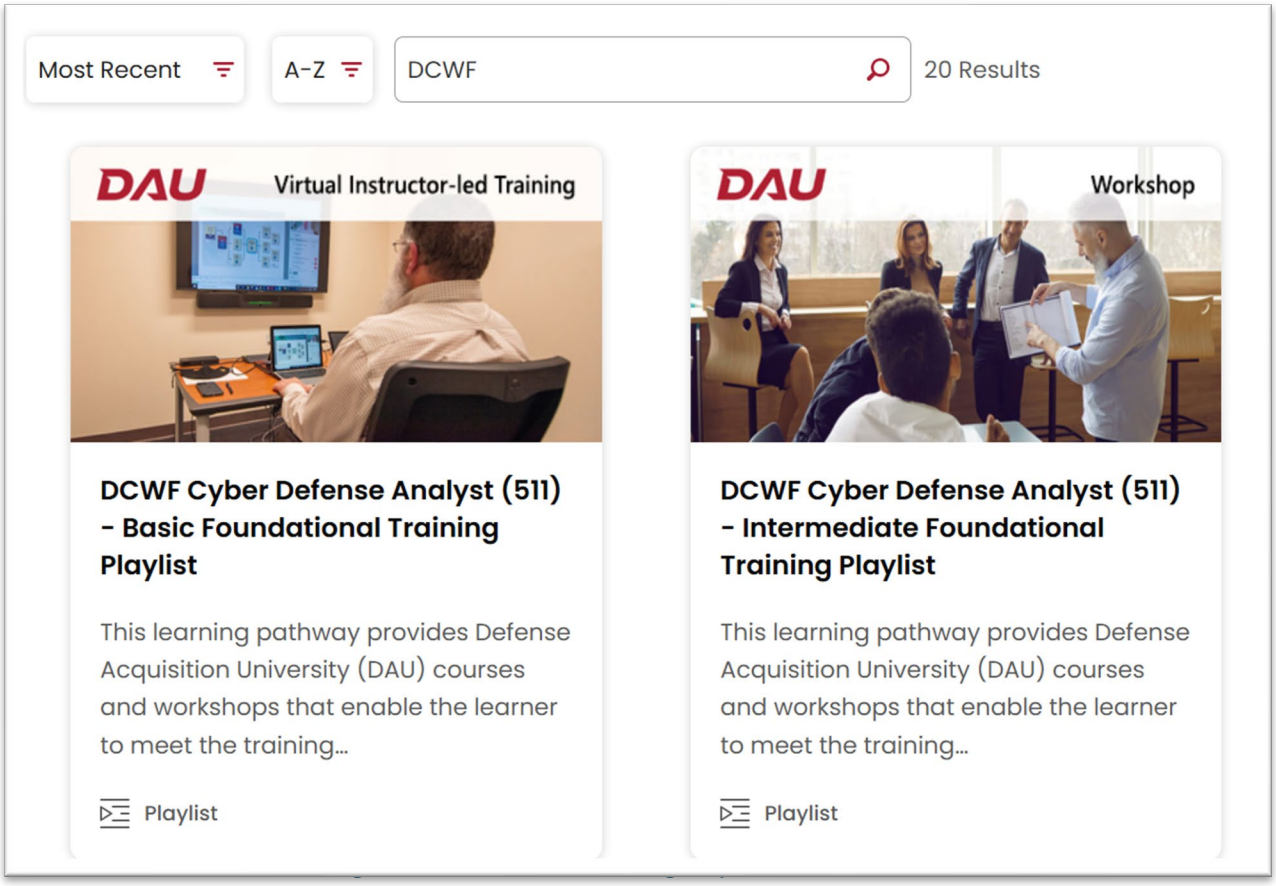


Figure 4: DAU DCWF Learning Playlist Search Menu

Finding Your DAU User ID and Troubleshooting

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

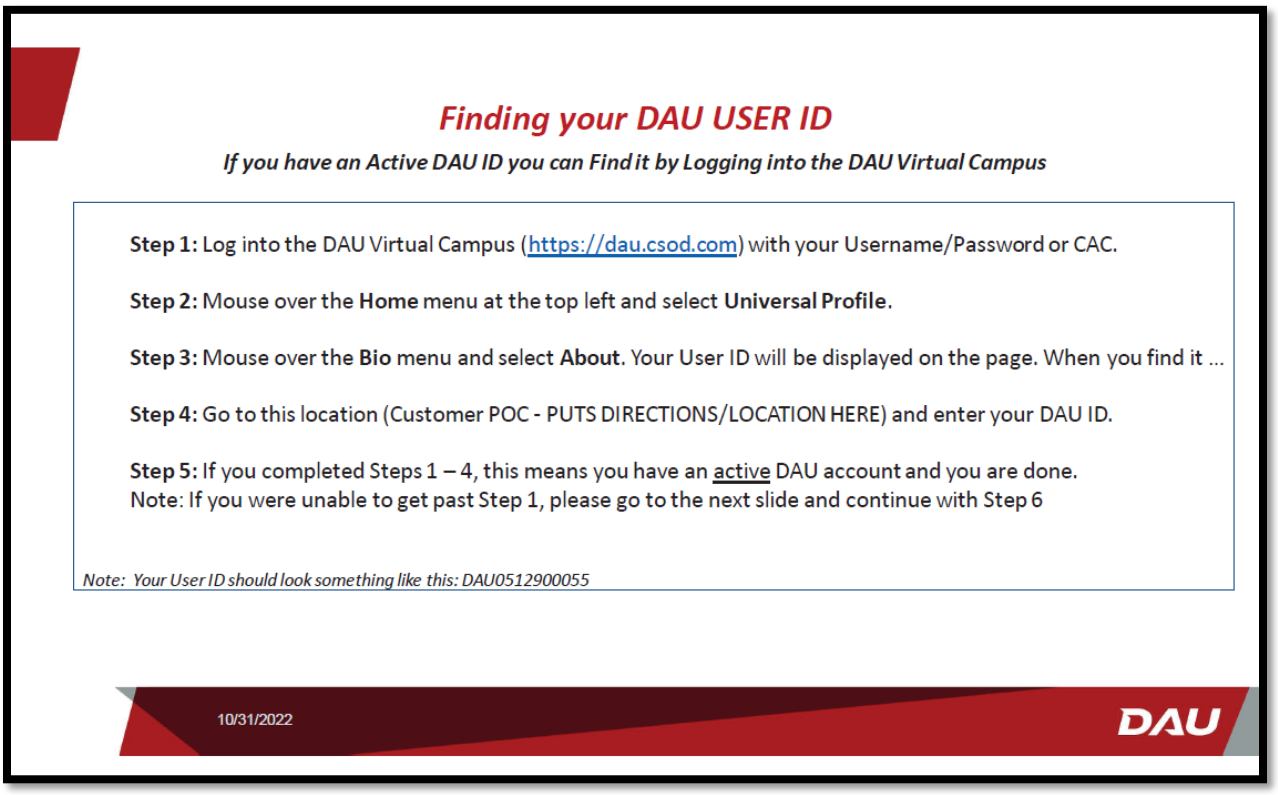


Figure 5: Finding your DAU User ID

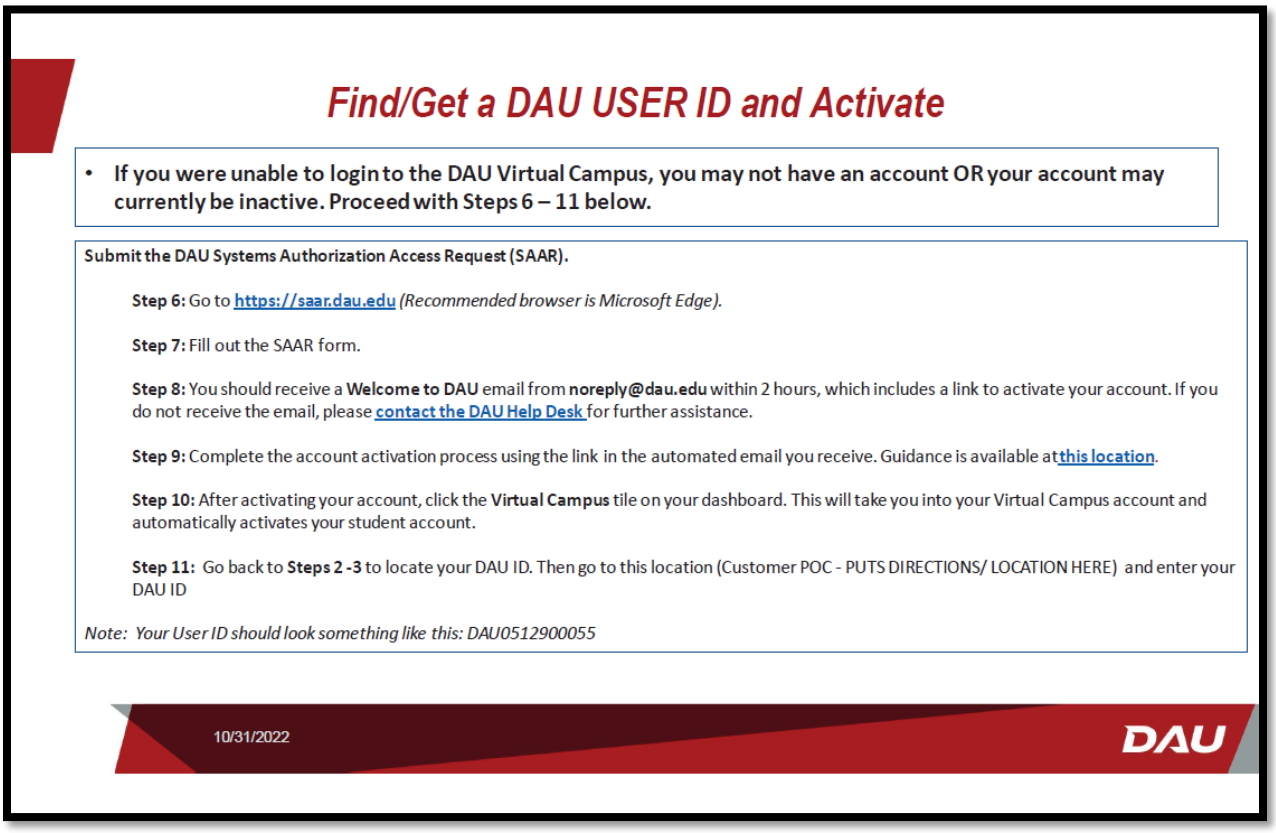


Figure 6: Find/Get a DAU User ID and Activate

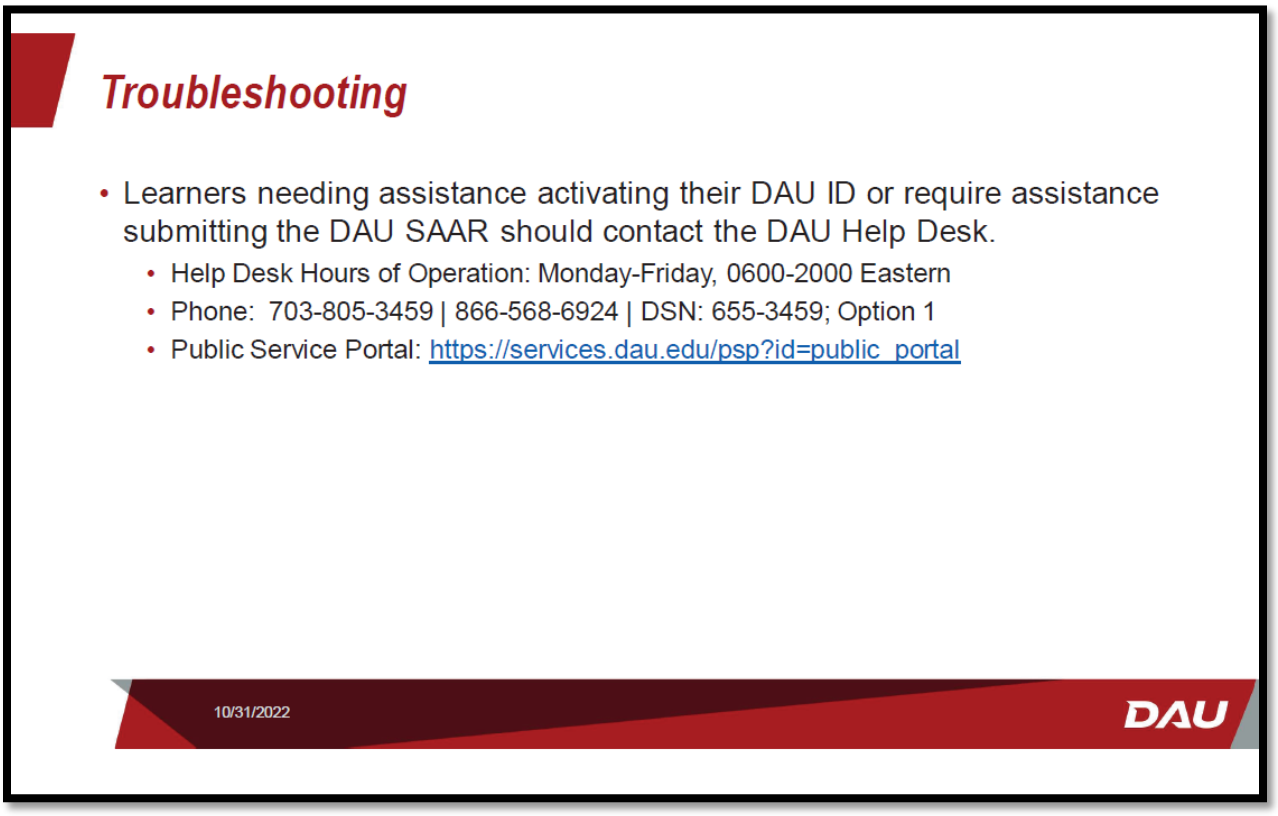


Figure 7: Troubleshooting

DAU DCWF Learning Playlist Coverage

The below tables outline the alignment of DAU DCWF Learning Playlists to associated DCWF work roles (Cybersecurity (CS), Information Technology (IT), and Cyber Enablers (EN)) and DoD 8140 proficiency levels.

DAU 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 1: DAU DCWF Learning Playlist Coverage for DCWF Cyber Enabler Workforce (Acquisition Workforce)

DAU	DCWF Information Technology (IT) Work Roles		
DCWF Work Role	**DoD 8140 Basic**	**DoD 8140 Intermediate**	**DoD 8140 Advanced**
(IT-411) Technical Support Specialist	✓	✓	✓
(IT-431) Knowledge Manager	✓	✓	✓
(IT-441) Network Operations Specialist	✓	✓	
(IT-451) System Administrator	✓	✓	
(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 2: DAU DCWF Learning Playlist Coverage for DCWF Information Technology (IT) Work Roles

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

Table 3: DAU DCWF Learning Playlist Coverage for DCWF Cybersecurity (CS) Work Roles

DoD 8140 Individual Development Plans & Qualification Timelines

It is recommended that individual development plans are developed with the employee, the employee's supervisor, the organization's training officer, and the organization's human resources department to ensure the employee can complete the assigned playlist within the DoD 8140 qualification timeline.

DoD 8140 Continuous Professional Development

Once a DoD cyber workforce team member satisfies DoD 8140 foundational and residential qualification requirements via a DAU DCWF learning playlist (or other applicable option), the employee is required to successfully complete 20 hours of continuous professional development or education activities per fiscal year, to maintain and enhance competence. DoD 8140 continuous professional development is as defined in DoDM 8140.03 (February 15, 2023) Section 3.2 "DoD Cyberspace Workforce Qualification and Management Program."

APPENDIX E

DoD 8140 Experience Working Group Minutes
July 30, 2025

Background

- The DoD CIO WID collaborated with DoD Components on enhancing the DoD 8140 Experience Qualification Process (EQP), including addressing concerns and challenges proposed by the DoD cyber workforce.

Main Discussion Points

- Addressed current challenges on how to validate the performance of cyberspace work.
- Discussed signature authorities.
- Discussed leveraging this process to validate experience when an employee is satisfying DoD 8140 foundational qualifications via education or training.
- Discussed DoD Component reciprocity.

Meeting Outcomes

- **Challenge Statement #1:** Validation of the Performance of Cyberspace Work
  - *Solutions:*
    - Leverage "Qualifying Documentation" as listed in the guide.
    - It is recommended that DoD Components may leverage this process to validate the performance of cyberspace work when an employee uses the DoD 8140 foundational qualification option of education (degree) or training if the option was achieved beyond 5 years of DCWF work role and DoD 8140 proficiency level assignment.
- **Challenge Statement #2:** Final Signature Authorities
  - *Solutions:*
    - Update "CWF Supervisor" to "CWF Supervisor of the cyberspace workforce employee."
    - Update "DoD Component ISSM" to "ISSM of the DoD Component, Organization, Command, or Activity."
    - Include examples.
- **Challenge Statement #3:** DoD 8140 Experience Reciprocity across DoD Components
  - *Solution:*
    - DoD CIO CATMS Tasker: DoD Component Enrollment in DoD 8140 Experience Reciprocity

Due-Outs

OPR	Action Item	Suspense
Military Services	List of Service-Specific Official Documentation to Support DoD 8140 EQP	Friday August 15, 2025
DoD CIO WID	DoD 8140 Experience Qualification Process (Guide) V1.2	Friday August 29, 2025
DoD CIO WID	DoD 8140 Experience Reciprocity CATMS Tasker	Tuesday September 30, 2025

Additional Notes

- Publication of the DoD 8140 EQP V1.2 will remove the reference to the DoD 8140 EQP workbook. DoD Components are invited to leverage the current version of the DCWF work role tool (excel) for a complete list of work role knowledge units, skills, abilities, and tasks.
- This process provides the baseline requirements for the DoD 8140 EQP. DoD Components have the authority and flexibility to add additional requirements to this process.
- The DoD 8140 EQP Certificate has been updated to V3 with an effective date of July 16, 2025. This document is pending upload to the DoD Cyber Exchange.

APPENDIX F

DoD 8140 Academic Accreditation GS-15 Decision Brief Minutes
July 31, 2025

Overview

- Outcomes from the Summer 2025 DoD 8140 Cyber Academic Alignment Team introduced the need to modify DoDM 8140.03, "Cyberspace Workforce Qualification and Management Program" (Published February 15, 2023) in terms of academic accreditation requirements.
- The DoD CIO WID collaborated with DoD Components for a GS-15 decision brief to address these modifications. Outcomes are listed below.
- The proposed modifications to DoDM 8140.03 listed in this document have been approved at the GS-15 level and are pending DoD Cyber Workforce Management Board (CWMB) final approval prior to DoD cyber workforce implementation.

Decision Brief Outcomes

- Inclusion of "regional accreditation" into policy.
- Introduces mandatory degree discipline accreditation by the **Accreditation Board for Engineering and Technology (ABET).**
  - Web Link: *https://www.abet.org/accreditation/find-programs/*
- Introduces mandatory degree discipline designation by the **National Center of Excellence in Cybersecurity (NCAE-C)** program.
  - Web Link: *https://maps.caecommunity.org/*
- Introduces DoD 8140 Academic Accreditation Implementation Plan.

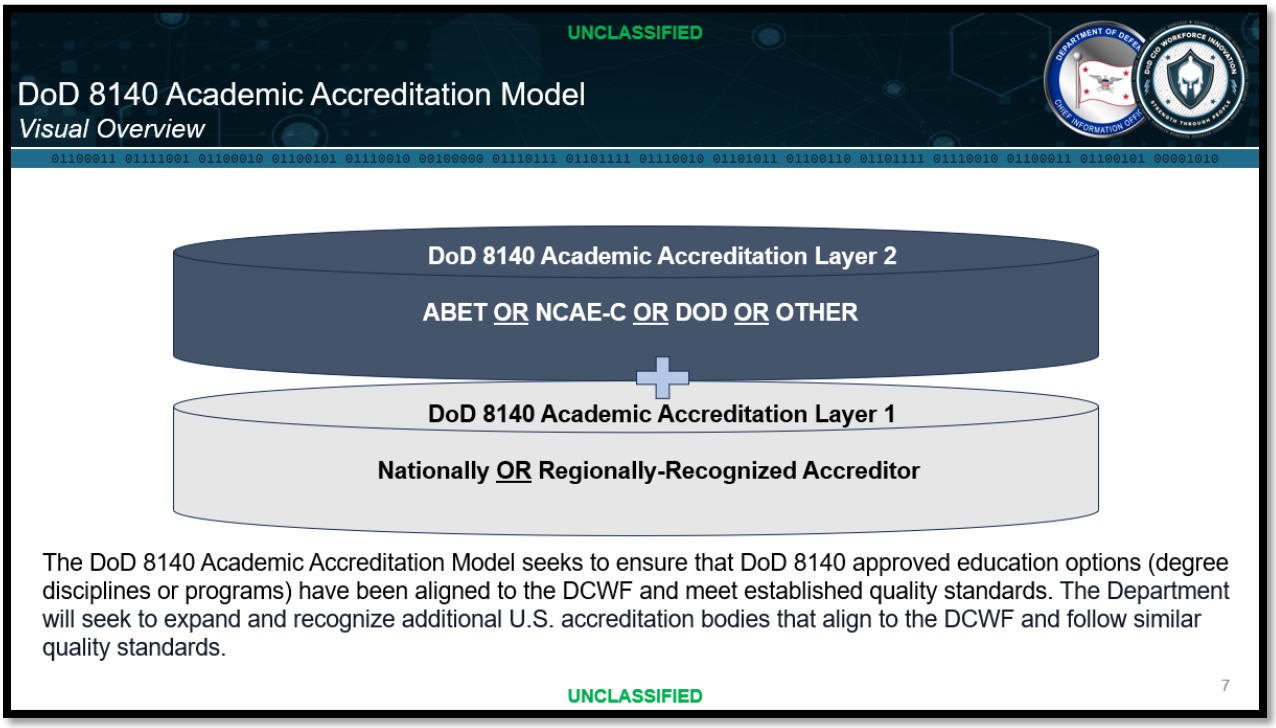
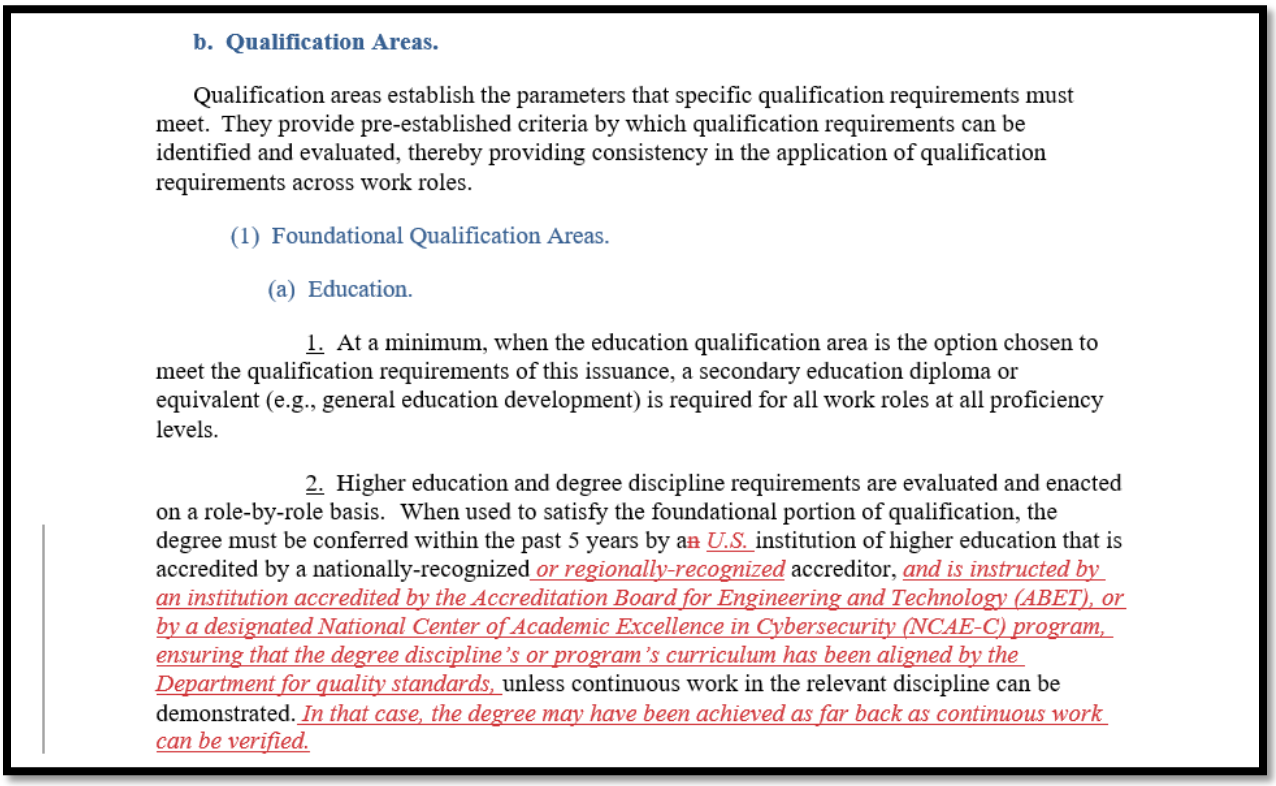


Figure 1: DoD 8140 Academic Accreditation Model

Proposed Modifications to DoDM 8140.03 "Cyberspace Workforce Qualification and Management Program"

Published February 15, 2023

Parts 1,2,3



b. Qualification Areas.

Qualification areas establish the parameters that specific qualification requirements must meet. They provide pre-established criteria by which qualification requirements can be identified and evaluated, thereby providing consistency in the application of qualification requirements across work roles.

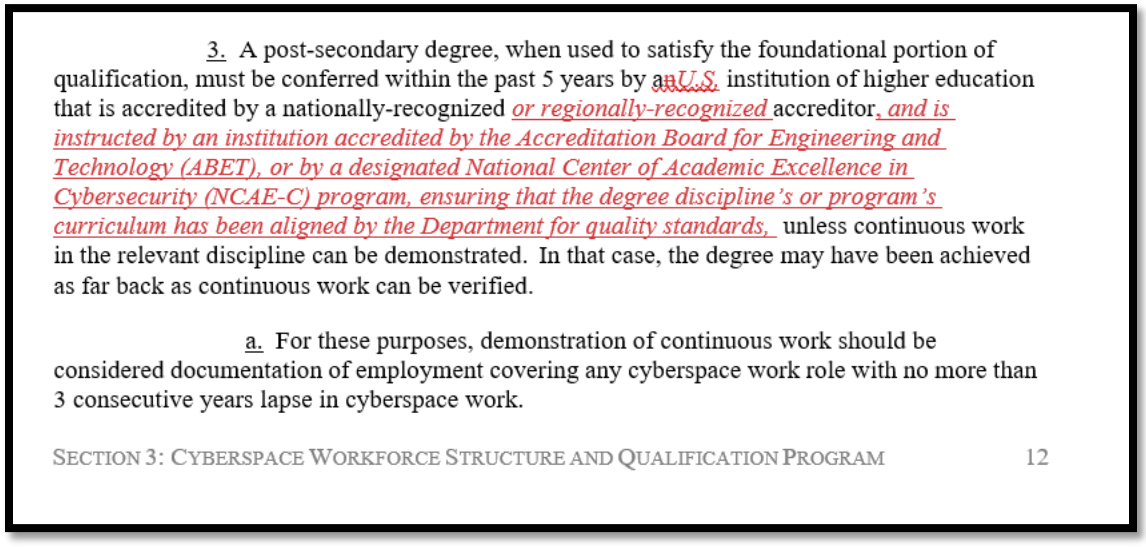
(1) Foundational Qualification Areas.

(a) Education.

1. At a minimum, when the education qualification area is the option chosen to meet the qualification requirements of this issuance, a secondary education diploma or equivalent (e.g., general education development) is required for all work roles at all proficiency levels.

2. Higher education and degree discipline requirements are evaluated and enacted on a role-by-role basis. When used to satisfy the foundational portion of qualification, the degree must be conferred within the past 5 years by a~~n~~ *U.S.* institution of higher education that is accredited by a nationally-recognized *or regionally-recognized* accreditor, *and is instructed by an institution accredited by the Accreditation Board for Engineering and Technology (ABET), or by a designated National Center of Academic Excellence in Cybersecurity (NCAE-C) program, ensuring that the degree discipline's or program's curriculum has been aligned by the Department for quality standards,* unless continuous work in the relevant discipline can be demonstrated. *In that case, the degree may have been achieved as far back as continuous work can be verified.*

Figure 2: DoDM 8140.03 Modification Part 1

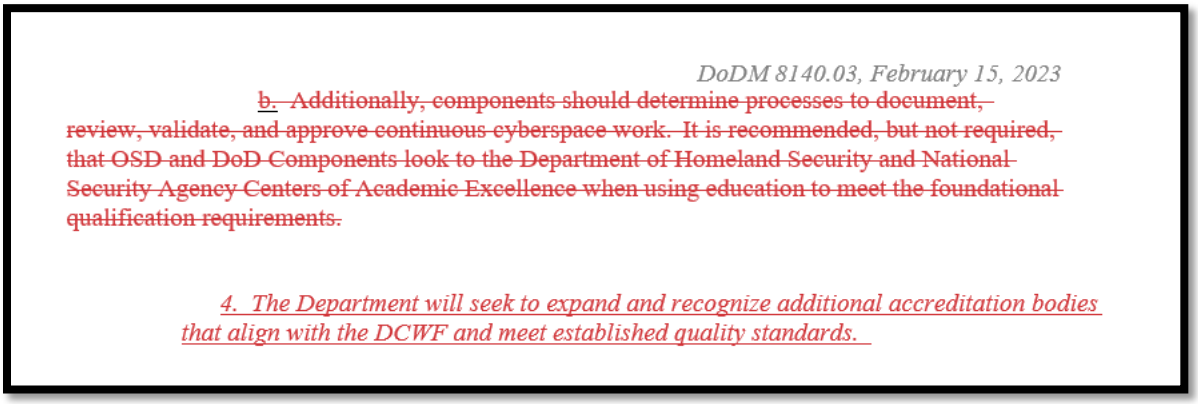


3. A post-secondary degree, when used to satisfy the foundational portion of qualification, must be conferred within the past 5 years by a ~~n~~U.S. institution of higher education that is accredited by a nationally-recognized *or regionally-recognized* accreditor, *and is instructed by an institution accredited by the Accreditation Board for Engineering and Technology (ABET), or by a designated National Center of Academic Excellence in Cybersecurity (NCAE-C) program, ensuring that the degree discipline's or program's curriculum has been aligned by the Department for quality standards,* unless continuous work in the relevant discipline can be demonstrated. In that case, the degree may have been achieved as far back as continuous work can be verified.

a. For these purposes, demonstration of continuous work should be considered documentation of employment covering any cyberspace work role with no more than 3 consecutive years lapse in cyberspace work.

SECTION 3: CYBERSPACE WORKFORCE STRUCTURE AND QUALIFICATION PROGRAM 12

Figure 3: DoDM 8140.03 Modification Part 2



DoDM 8140.03, February 15, 2023

~~b. Additionally, components should determine processes to document, review, validate, and approve continuous cyberspace work. It is recommended, but not required, that OSD and DoD Components look to the Department of Homeland Security and National Security Agency Centers of Academic Excellence when using education to meet the foundational qualification requirements.~~

4. The Department will seek to expand and recognize additional accreditation bodies that align with the DCWF and meet established quality standards.

Figure 4: DoDM 8140.03 Modification Part 3

DoD 8140 Academic Accreditation Implementation Plan

Overview: This implementation plan will guide the DoD cyber workforce in continuously refining DoD 8140 academic accreditation and education options in support of DoD 8140 foundational qualification matrix. Additional guidance will be provided to DoD Components at a later time.

OPR: DoD CIO

OCR: DoD Components

Initiative Number	Initiative Description	Status
1.0	Develop the DoD 8140 Qualification Approval Process for Education, which will document steps and requirements for degree discipline alignment, review, and approval.	In Progress
1.1	Develop an approval pathway for U.S. institutions that do not have authorized accreditation or designation status to submit degree disciplines or programs to DoD for review and approval into the DoD 8140 foundational qualification matrix.	In Progress
1.2	Identify and document qualifying criteria and standards for approved U.S. accreditation bodies for inclusion into the DoD 8140 Qualification Approval Process.	In Progress
2	Introduce a transition period to ensure DoD Component comprehension of new accreditation requirements.	In Progress; Pending DoD cyber workforce coordination
3	Continue to explore and expand U.S. accreditation options that accredit degree disciplines or programs and align to the DCWF for inclusion into the DoD 8140 foundational qualification matrix and DoDM 8140.03.	Ongoing Activity

DoD 8140 Cyberspace Workforce Annual Report

Interim Guidance for Fall 2025 Qualification Data Collection Tasker

Overview: This section provides authoritative interim guidance from the DoD CIO WID regarding DoD 8140 foundational qualifications (education) in support of the anticipated Fall 2025 DoD 8140 qualification data collection tasker. This information will be reflected in the DoD 8140 foundational qualification matrix and DoD 8140 qualification data collection template.

TEMPORARY DEGREE DISCIPLINE/PROGRAM ACCREDITATION SUSPENSION

- The DoD CIO WID has temporarily suspended the mandatory Accreditation Board for Engineering and Technology (ABET) accreditation **OR** National Center of Academic Excellence in Cybersecurity (NCAE-C) designation requirements within the DoD 8140 foundational qualification matrix. In accordance with the DoD 8140 Academic Accreditation Implementation Plan, these requirements will be re-introduced to the DoD 8140 foundational qualification matrix once the DoD-wide transition period is complete.

NATIONALLY OR REGIONALLY-RECOGNIZED ACCREDITOR REQUIREMENT IN EFFECT

- A DoD 8140 approved post-secondary degree must be conferred within the past five years **AND** must be from a U.S. institution of higher education that is accredited by a nationally **OR** regionally-recognized accreditor, unless continuous work in a relevant discipline can be demonstrated. In that case, the degree may have been achieved as far back as continuous work can be verified.

DCWF Cybersecurity (CS) Workforce Element

Basic Proficiency Level: A **B.S.** in Information Technology (IT), cybersecurity (CS), Computer Science, Information Systems, Data Science, or Software Engineering.

Intermediate Proficiency Level: A **B.S.** in Information Technology (IT), cybersecurity (CS), Computer Science, Information Systems, Data Science, or Software Engineering.

Advanced Proficiency Level: Pending DoD validation; Consider an alternative option.

DCWF Information Technology (IT) Workforce Element

Basic Proficiency Level: Please refer to DoD 8140 Cyber Academic Alignment Team Report for DoD 8140 foundational qualification alignment.

Intermediate Proficiency Level: Please refer to DoD 8140 Cyber Academic Alignment Team Report for DoD 8140 foundational qualification alignment.

Advanced Proficiency Level: Please refer to DoD 8140 Cyber Academic Alignment Team Report for DoD 8140 foundational qualification alignment.

DCWF Cyber Enabler (EN) Workforce Element

DCWF Cyber Enabler Foundational Qualification Governance Principle (Education)

A DoD 8140 approved degree discipline or program aligned to a DCWF CS or IT work role and associated DoD 8140 proficiency level satisfies DoD 8140 foundational qualification compliance for all DCWF EN work roles at all three DoD 8140 proficiency levels.