DoD 8140 CYBERSPACE WORKFORCE MANAGEMENT

Introduction, Program Background, & Purpose of this Supplemental Guide

Introduction

The Department of Defense (DoD) must offensively and defensively protect and preserve communications and information systems, digital domains, enclaves/networks, and data in order to assure the security and reliability of a wide range of national assets and critical services. A highly skilled DoD cyber workforce that can adapt to the dynamic cyber environment is imperative for mission success.

The new DoD 8140 Cyber Workforce Qualification Program provides structure for standardizing work across the full spectrum of cyber operations, leverages DoD 8140 proficiency levels for performing cyber work roles, shapes training and qualifications to grow cyber workforce capabilities. This program is designed to be:

Flexible → DoD Components can tailor Residential qualification requirements based on mission requirements.

Adaptive → DoD 8140 Qualification Program will continue to evolve for the needs of the DoD cyber workforce.

Responsive → The ability to track DCWF work roles and DoD 8140 proficiency levels allows leaders to assess workforce readiness in a timely manner.

The DoD 8140 Program unifies the overall DoD cyber workforce and organizes work roles into seven **Cyber Workforce Elements**:

- Information Technology (IT)
- Cybersecurity (CS)
- Cyber Effects (CE)
- Intelligence (Cyber)
- Data/Artificial Intelligence (Data/AI)
- Software Engineering (SE)
- Cyber Enablers

The DoD 8140 Program establishes the **DoD Cyber Workforce Framework (DCWF)**:

- An authoritative reference for the identification, tracking, and reporting of DoD cyberspace positions
- A standardized framework that provides a lexicon of work roles including knowledge, skills, abilities, and tasks (KSATs) to support the development of common cyber workforce qualification standards
- 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 **Cyber Workforce Management Board (CWMB)**, in accordance with DoD Directive 8140.01, is chartered to be the principal governance body to manage the DoD's cyber workforce. The CWMB is a Senior Executive (SES)/General/Flag (GO/FO) Officer level decision body that provides recommendations to the appropriate implementation authorities for cyber workforce decisions related to standards, qualifications, training, and compliance.

Program Background

Federal Cybersecurity Workforce Assessment Act (FCWAA) of 2015 (Sections 303 and 304 of Public Law 114-113), requires the identification and coding of Federal positions with that require the performance of "IT, Cybersecurity, or other Cyber-related functions."

Through implementation of FCWAA '15, the DoD transformed its cyberspace workforce focus *from information assurance to a broader view of the cyber workforce* 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.

The FCWAA, coupled with DoD's expanding cyber mission responsibilities, drove the transition from the DoD 8570 Information Assurance (IA) Workforce Improvement Program, which launched in 2005, to the DoD 8140 Cyber Workforce Qualification Program (CWQP) directed in 2020.

DoD 8570 IA Program structured certifications based on hierarchical levels of cybersecurity responsibilities needed for information systems:

- Level 1: Computing environment IA
- Level 2: Network environment IA
- Level 3: Enclave and advanced network IA

DoD 8140 CWQP focuses on qualification of DoD 8140 proficiency levels for performing specific work roles. Qualifications include education, training, and certifications mapped to work roles, as well as other requirements tailored for successful performance of work roles in various mission environments. DoD 8140 CWQP:

- Prescribes standards and assigns responsibilities for the management of the DoD cyber workforce
- Supports work role identification, tracking, qualification, and reporting of the cyber workforce
- Facilitates professional development through work role expertise applied to cyber operations and/or organizational objectives

DoD 8140 policies & standards include:

DoD Directive (DoDD) 8140.01 5 October 2020, "Cyberspace Workforce Management"	Establishes a definition for the DoD cyber workforce, introduces the DoD Cyber Workforce Framework (DCWF) as an authoritative reference, and outlines component roles and responsibilities for the management of the DoD cyber workforce.
DoD Instruction (DoDI) 8140.02 21 December 2021, "Identification, Tracking, and Reporting of Cyberspace Workforce Requirements"	Establishes the identification, tracking, and reporting of the DoD cyber workforce in accordance with the DCWF and supports enterprise strategic workforce planning efforts.
DoD Manual (DoDM) 8140.03 15 February 2023, "Cyberspace Workforce Qualification and Management Program"	Prescribes and implements the qualification criteria for DCWF work roles to ensure personnel filling cyber positions are capable of meeting mission requirements.
DoD Cyber Workforce Framework (DCWF) Military & Civilian Workforce Identification & Coding Guide, 29 July 2024 (Ver. 1.3)	Provides supplemental guidance for DoD cyber workforce coding efforts in accordance with Federal and DoD policies.

Purpose of this DoD 8140 Supplemental electronic Guide (eGuide)

This supplemental guidance supports the DoD Cyber Workforce issuances (DoD 8140 policy series) by clarifying implementation and promoting consistent application of policy tenets for standardization across DoD. This guide is not prescriptive, nor infringes on the authorities and responsibilities of DoD Components stipulated in the DoD 8140 issuances. It is intended as a resource to expedite implementation of DoD 8140 requirements and fully leverage its utility in supporting human capital objectives that advance the 2023-2027 DoD Cyber Workforce Strategy.

This guide has been compiled to address frequently asked questions (FAQs) and other comments and inquiries received by the DoD Chief Information Officer Workforce Innovation Directorate (DoD CIO WID). The content of this guide is organized by topic "modules" for utility; the guide will continue to evolve with subsequent versions incorporating feedback from cyber workforce stakeholders based on lessons learned and best practices. Content updates are indicated by the date in the header at the top of the page in each module so that modules may be modified independently in a timely manner as needed.

Submissions for content additions, changes, or general inquiries for this guide may be sent to the DoD CIO WID customer service email at:

osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil

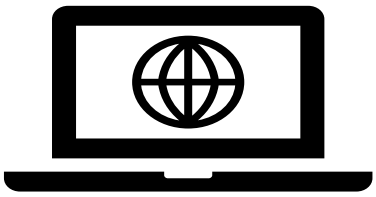
Cyber Workforce members are encouraged to contact their command/organization's DoD Cyber Workforce Program representative in order to obtain particular guidance regarding DoD Component implementation (e.g., Services, Joint Staff/Combatant Commands, 4th Estate agencies).

References and Information

More information can be found on the **DoD Cyber Exchange**, an official site that provides access to compiled information, policy, guidance and training for DoD cyber professionals; it consists of three web portals:

- **Public** (https://public.cyber.mil), which is accessible to all Internet users; all information has been cleared for public use, including commercial vendors.
- **NIPR** (https://cyber.mil), which requires Public Key Infrastructure (PKI) credentials for access to Non-classified Internet Protocol Router Network (NIPRnet); common access card (CAC)-enabled; can host Unclassified and Controlled Unclassified Information (CUI).
- **SIPR** (https://cyber.smil.mil), which can only be accessed from the Secret Internet Protocol Router Network (SIPRnet) with a proper security clearance and token.

DoD 8140 Cyber Workforce Program references are primarily hosted on the Public and NIPR web portals under the "DoD Workforce Innovation Directorate (WID)" main menu which contains links to the DoD 8140 document repository, DoD Cyber Workforce Framework (DCWF), DoD Cyber Excepted Service (CES) repository, and other cyber workforce information. DoD cyber users should use the NIPRnet sites for research which contain expanded reference libraries.



NIPR (CAC-enabled) links:

DoD 8140 Cyber Workforce Program on the DoD Cyber Exchange:

https://cyber.mil/wid/

DoD Cyber Workforce Framework (DCWF) Tool:

https://cyber.mil/wid/dcwf/

Public web sites:

DoD 8140 Cyber Workforce Program on the DoD Cyber Exchange:

https://public.cyber.mil/wid/dod8140/documents-library/

DoD Cyber Workforce Framework (DCWF) Tool:

https://public.cyber.mil/wid/dcwf/