



CLEARED
For Open Publication

Mar 28, 2024

Unclassified 12 March 2024

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD 8140 CYBER WORKFORCE QUALIFICATION PROGRAM (CWQP) *DoD 8570 Information Assurance (IA) Program Transition to DoD 8140 CWQP*

Overview

DoD transitioned 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 15 February 2023 in accordance with the DoD 8140-policy series. The DoD 8570 IA Program prescribed baseline certifications and qualification requirements for *broad system-focused responsibilities*. The DoD 8570 and DoD 8140 programs are not structured the same and there is no "crosswalk" of qualifications between them, however, an individual's certifications may carry over from 8570 to 8140 dependent on the work role(s) and proficiency level(s) assigned to their position.

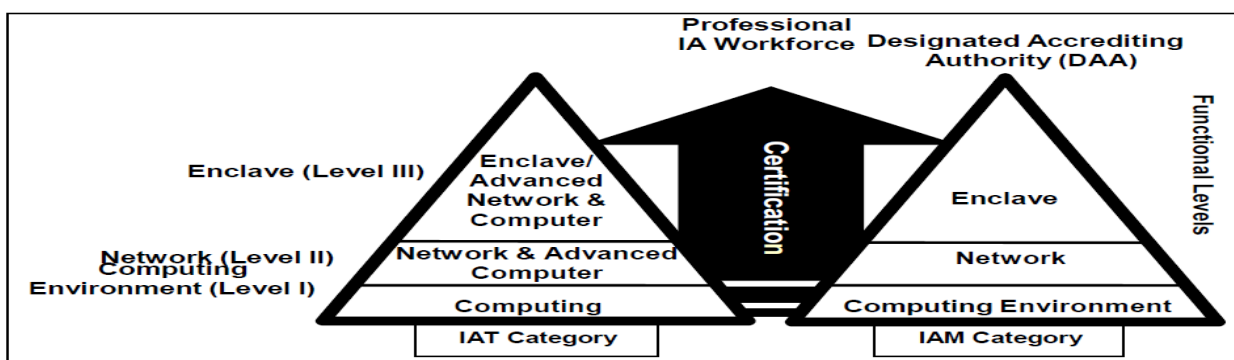
The DoD 8140 Cyber Workforce Qualification Program (CWQP) addresses the scope of expertise needed for all cyber disciplines, using a comprehensive approach for cyber workforce talent management. The DoD 8140 CWQP is designed for individual flexibility by allowing options to obtain knowledge and capability to perform *skills-based work roles*, while empowering organizations to levy additional requirements based on operational needs. DoD 8140 policy governs all cyber/cybersecurity positions and personnel across DoD, regardless of personnel/pay system (e.g., General Schedule (GS), Cyber Excepted Service (CES), Defense Civilian Intelligence Personnel System (DCIPS), Acquisition Demonstration (AcqDemo)).

DoD 8570 Information Assurance (IA) Program

DoD's 8570 IA Program established a defensive posture for the protection of DoD networks through standardized information security technical and management qualification levels. 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:

- Three functional certification levels (I, II, III) for the Information Assurance Technical (IAT), IA Management (IAM), IA System Architect and Engineer (IASAE) categories indicating scope of responsibilities in an enclave's hierarchy.
- Certifications for Computer Network Defense-Service Provider (CND-SP) specialties as applicable to IA positions, subsequently redescribed as Cybersecurity Service Provider (CSSP) specialties for Analyst (A), Infrastructure Support (IS), Incident Responder (IR), Auditor (AU), & Service Provider Manager (SPM) mapped to IA functional levels.
- Additional Computing Environment and/or Operating System (CE/OS) certificates were required based on the particular requirements of a system environment.

Figure 1: DoD 8570 IA Program





Unclassified 12 March 2024

DoD 8140 Cyber Workforce Qualification Program (CWQP)

The DoD 8140 CWQP leverages *granular work roles* for performing defensive, offensive, and other cyber mission responsibilities in addition to the “traditional” IA type roles. DoD 8140 CWQP addresses the growing need for qualified expertise across the full spectrum of varied cyber operations (e.g., network maneuverability, cyber effects, cyber intelligence, data mining, artificial intelligence) which encompass myriad work roles. The DoD 8140 CWQP transitions the workforce from an IA compliance-based approach to a focus on the demonstration of capability.

Key Components of DoD 8140 CWQP:

Work Roles. DoD Cyber Workforce Framework (DCWF) work roles comprise core and additional knowledge, skills, abilities, and tasks (KSATs) that are continually evolving to combat dynamic cyber threats, whereas 8570 focused on functions to fulfill system responsibilities.

Work Role

Definition:

Describes the purpose of the work role.

Task:

An activity performed on a regular basis to carry out the work role.

Knowledge, Skills, & Abilities (KSAs):

Attributes required for performance of the task.

Core (C) KSAs & Tasks:

Critical for successful performance within a role. Baseline requirements for demonstration of the work role.

Additional (A) KSAs & Tasks:

Somewhat important, or not applicable, for successful performance of the work role.

Example

Definition: *Security Control Assessor (612) conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls.*

Core Task: *Develop methods to monitor and measure risk, compliance, and assurance efforts.*

Core KSAs:

Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.

Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.



Unclassified 12 March 2024

- Position Coding** DoD 8140 policy allows a primary work role code and up to two additional work role codes assigned to a position for a comprehensive description of the cyber work.
- Proficiency Levels** DoD 8140 Work role proficiency levels (i.e., Basic, Intermediate, Advanced) provide the levels of capability to perform the work role successfully and indicate individual readiness.

Example Security Control Assessor (612) work role proficiency level task statements:

Task: *Develop methods to monitor and measure risk, compliance, and assurance efforts.*

Basic: *Demonstrates knowledge of methods to monitor and measure risk, compliance, and assurance efforts.*

Intermediate: *Contributes to developing methods to monitor and measure risk, compliance, and assurance efforts.*

Advanced: *Develops, reviews and/or approves methods to monitor and measure risk, compliance, and assurance efforts.*

- Qualifications** DoD 8140 Foundational Quals are similar to DoD 8570 baseline certifications, however, there are multiple avenues, including DoD skills-based courses and experience, to attain Foundational Quals tailored to individual work roles. Additionally, Residential Quals build upon Foundational Quals through demonstration of work role KSATs in the mission environment.
- Qual Matrix** Work role qualifications map to proficiency levels for Foundational & Residential qualifications according to each work role; emphasis is on attainment of work role proficiency (via alternative paths) vice certifications. Certifications are only one feature of DoD's 8140 CWQP which includes a multifaceted approach for work role qualification.
- 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.
- Letters** DoD 8140 does not require appointing letters or official designations, as the work role coding suffices, but Components may require designation letters, administrative, and other requirements based on assigned work roles and/or organizational duties.
- Certificates** Computing Environment, Operating System, Network Environment (CE/OS/NE) certificates are not required under DoD 8140 policy but may be required by Components for performing certain roles or jobs.
- Governing Policies** Federal and DoD authorities (e.g., OPM, USCYBERCOM, DoD CIO, Services, NSA, DISA) may supplement, but not substitute, DoD 8140 compliance requirements. DoD and Service functional communities (e.g., intelligence, security, financial management, acquisition) may mandate requirements for positions in addition to DoD 8140 work role qualifications.



Unclassified 12 March 2024

Commands/Orgs

Organizations may require functional and position specific conditions of employment including Personnel Qualification Standards (PQS), Job Qualification Requirements (JQR), On-the-Job Training (OJT), training, exercises and other means to satisfy Foundational and Residential qualifications, but not in lieu of requirements contained in an applicable Qual Matrix.

Maintenance

DoD 8140 Residential Qualification requires a minimum of 20 hours per year of Continuous Professional Development (CPD) or continuing education (CE) units annually commencing in the fiscal year after attainment of Residential Qualification. Renewal/maintenance of certifications is dependent on each certification's particular requirements. Courses approved by a certification provider for recertification may also be applied toward Residential Qualification CPD.

Figure 2: Qualification Matrix template

		Basic	Intermediate	Advanced
Foundational Qualification Options – Demonstration of Knowledge	Education	Option	Option	Option
	Training (DoD & Commercial)	OR	OR	OR
	Personnel Certification	Option	Option	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.

Transition Items

- DoD CIO maintains DoD 8570 information on the DoD Cyber Exchange as a reference for transition although the DoD 8570 policy and standards have been superseded by DoD 8140 qualification requirements for military and civilian personnel. There is no direct comparison, or mapping, between 8570 IA functional categories and the DCWF work roles.
- Contractors remain until DoD 8570 policy until update of the Defense Federal Acquisition Regulation Supplement (DFARS) authorizes DoD 8140 implementation for contractor personnel.
- Industry certifications attained under DoD 8570 may carryover to DoD 8140 CWQP depending on their validity and applicability for a particular work role and proficiency level; the certifications must be current per the applicable certifying/governing organization.



Unclassified 12 March 2024

- Waivers may be granted to “grandfather” certifications; for example, Cisco Certified Network Associate (CCNA) Security Certification waiver is valid through 15 February 2025 to satisfy 8140 qualifications for cyber positions aligned to the DCWF Cybersecurity Workforce Element, provided it is maintained/renewed according to Cisco's procedures.
- “Good for Life” (GFL) certifications are not valid under DoD 8140 and were also phased out under DoD 8570 policy. All certifications must be renewed/maintained according to their provider’s specified periodicities as there is no “blanket” renewal under DoD 8140.
- Civilian positions that reference DoD 8570 requirements should be updated; however, new hires and incumbents will need to attain DoD 8140 qualifications applicable to the work role(s) of their positions regardless of reference to DoD 8570.

Figure 3: Example Work Role Code Qual Matrix

(612) Security Control Assessor					
		Basic	Intermediate	Advanced	NOTES
Foundational Qualification Options* (Training, Certifications, Education aligned to higher proficiency levels qualify lower proficiency levels.)	Education	A BS degree in Information Technology, Cybersecurity, Data Science, Information Systems, or Computer Science, from an ABET accredited or CAE designated institution fulfills the educational requirement for this WRC	A BS degree in Information Technology, Cybersecurity, Data Science, Information Systems, or Computer Science, from an ABET accredited or CAE designated institution fulfills the educational requirement for this WRC	TBD	For additional information pertaining to ABET: www.abet.org or CAE: www.caecommunity.org
		OR	OR	OR	
	DoD/Military Training	Officers: J-3B-0440 Enlisted: A-150-1980 Enlisted: A-150-1202 Enlisted: A-150-1203 Enlisted: A-150-1250 or CYB 5640/CYB 5640V/WSS 010 or DCMA DIBCAC Cybersecurity Assessor	A-150-1980 or A-150-1202 or A-150-1203 or A-150-1250 or WSS 011 or WSS 012	A-531-0009 or A-531-0022 or A-531-0045 or DCMA DIBCAC Cybersecurity Assessor	See TAB C (DCWF Training Repository) for additional course information.
	Commercial Training	TBD	TBD	TBD	
		OR	OR	OR	
	Personnel Certification		CGRC/CAP or CASP+ or Cloud+ or PenTest+ or Security+ or GSEC	CISM or CISSO or CPTE or CySA+ or FITSP-A or GCISA or CISA or CISSP or CISSP-ISSEP or GSLC or GSNA	See TAB B (Certification Index) at the beginning of this document for certification vendor information.
Foundational Qualification Alternative	Experience	Conditional Alternative	Conditional Alternative	Conditional Alternative	Refer to Section 3 of the DoD 8140 Manual for more information.
Residential Qualification	On-the-Job Qualification	Always Required	Always Required	Always Required	Individuals must demonstrate capability to perform their duties in their resident environment.
	Environment-Specific Requirements	Component Discretion	Component Discretion	Component Discretion	
Annual Maintenance	Continuous Professional Development	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	

More information can be found regarding DoD 8140 CWQP on the DoD Cyber Exchange:

[8140 FAQ – DoD Cyber Exchange](#) or <https://public.cyber.mil/wid/cwmp/>