DoW Cyber Workforce Management Module Series Overview

Purpose: The purpose of this document is to introduce Department of War (DoW) cyberspace (cyber) workforce management concepts and activities to DoW cyber workforce 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 (administrative update). If you have a question, please connect with your DoW cyber workforce supervisor or DoW Component Office of Primary Responsibility. Module 2, "An Introduction to DoD 8140 Policy" has absorbed the Module on "DoD 8570 IA Program Transition to DoD 8140 Cyber Workforce Qualification Program."

Resource Title	Original Publication Date
Module 1: An Introduction to the DCWF	April 17, 2025
Module 2: An Introduction to DoD 8140 Policy	April 4, 2024
Module 3: DoD Cyber Workforce Strategy Alignment to DoD 8140	April 23, 2024
Module 4: Personnel Qualification Waiver Supplemental Information	June 3, 2025
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 cyber workforce management teams on an annual basis to support enduring DoD 8140 cyber workforce 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 publication date of this document is December 1, 2025.

Module 1:
An Introduction to the DCWF

Figure 1: DCWF Seal

Module 1 Overview: This module describes how Department of War (DoW) cyber workforce management teams can leverage the DoD Cyber Workforce Framework (DCWF) as defined in Department of Defense Directive (DoDD) 8140.01, "Cyberspace Workforce Management" (October 5, 2020).

DCWF Workforce Element: Each DCWF workforce element is defined in DoDD 8140.01 and pertains to a grouping of associated work roles within the DCWF. As an example, the DCWF Information Technology (IT) workforce element is defined below:

IT Workforce: Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information. (Defined in DoDD 8140.01 (October 5, 2020))

DCWF Work Role: A DCWF work role describes a distinct set of activities and attributes needed for the successful execution of work. A person may perform up to three DCWF work roles within their assigned position, billet, or contracted service requirement. (Defined in DoDD 8140.01)

When building a position description, it is strongly recommended that selection of a DCWF work role aligns with the mission of the DoW Component and requirements of the position, including the DoD 8140 foundational and residential qualification requirements at the appropriate DoD 8140 proficiency level (i.e., Basic, Intermediate, or Advanced). If the tasks and knowledge, skills, and abilities (KSAs) do not seem relevant to the position you are assessing, confer with your local DoW cyber workforce supervisor and your organization's human resource department for additional guidance.

Note: *A DCWF work role is not a position. Up to three DCWF work roles may be assigned to one position, depending on the scope of responsibilities.*

Ask Yourself: *Do the tasks and knowledge, skills, and abilities support the major duties and responsibilities of the position?*

DCWF Tasks and KSAs: DCWF tasks and KSAs can be aligned to one or multiple DCWF work roles, which streamlines the identification of related DCWF work roles to aid in position classification.

DCWF Task: An activity an employee performs on a regular basis to carry out the functions of the job. (Defined in Department of Defense Instruction (DoDI) 8140.02 Identification, Tracking, and Reporting of Cyberspace Workforce Requirements (December 21,2021)).

DCWF KSAs: The attributes required to perform a job, typically demonstrated through DoD 8140 foundational qualifications. (Defined in DoDI 8140.02 Identification, Tracking, and Reporting of Cyberspace Workforce Requirements (December 21,2021).

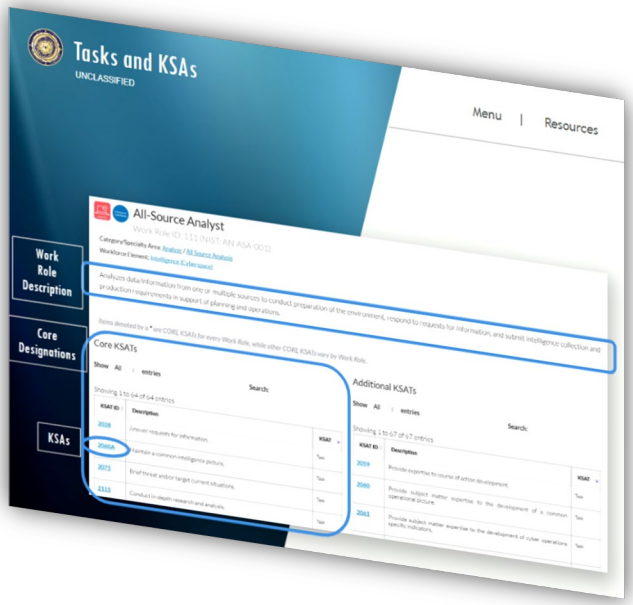

Figure 2: DCWF Tasks and KSAs

DCWF "Core" Tasks and KSAs: DCWF core tasks and KSAs are critical for successful performance within a DCWF work role. Inability to execute the task or not possessing the core task or KSA will inhibit successful performance and likely result in job failure. These are baseline expectations of performance and mandatory elements of the position's responsibilities, and are essential to the DCWF work role, regardless of environment or situation.

*In accordance with Department of Defense Manual (DoDM) 8140.03, "Cyberspace Workforce Qualification and Management Program" (February 15, 2023), DoD 8140 foundational qualification options, whether one course/program or a defined collection of courses/programs, must cover **70% of "core" task and KSA content** of the DCWF work role appropriate for the applicable DoD 8140 proficiency level.*

Figure 3: DoD 8140 Seal and Foundational Qualification Statement

DCWF "Additional" Tasks and KSAs: DCWF additional tasks and KSAs are (a) somewhat important or (b) not important at all for successful performance within a DCWF work role. Inability to execute the task or not possessing the KSA has a minor influence, or no effect at all, on successful job performance. These are optional elements (if applicable) of the position's responsibilities. Ask yourself, are these "additional" tasks and KSAs relevant to the position?

A Note To Remember: DCWF work roles comprise core and additional tasks and KSAs that are continually evolving to combat dynamic cyber threats, whereas DoD 8570 focused on functions to fulfill system responsibilities.

The Eight "Core" Knowledge Statements of the DCWF: There are eight "*core" (C) knowledge statements that are considered "*core" for all DCWF work roles. These knowledge statements are foundational to all cyber positions.

Required	DCWF Task ID	DCWF Core Knowledge Statements	Core (C)
✓ Always Required	*22	*Knowledge of computer networking concepts and protocols, and network security methodologies.	(C)
✓ Always Required	*108	*Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	(C)
✓ Always Required	*1157	*Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	(C)
✓ Always Required	*1158	*Knowledge of cybersecurity principles.	(C)
✓ Always Required	*1159	*Knowledge of cyber threats and vulnerabilities.	(C)
✓ Always Required	*6900	*Knowledge of specific operational impacts of cybersecurity lapses.	(C)
✓ Always Required	*6935	*Knowledge of cloud computing service models Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS).	(C)
✓ Always Required	*6938	*Knowledge of cloud computing deployment models in private, public, and hybrid environment and the difference between on-premises and off-premises environments.	(C)

Functional Community Toolkit Examples: Let's take a look at a Functional Community Toolkit, prepared by the Office of the Under Secretary for War for Personnel and Readiness (OUSW P&R). In figures three and four, you can see how multiple work roles can be composed under one position, with standard tasks and KSA's for each. This provides DoW Components the flexibility to build the best workforce possible.

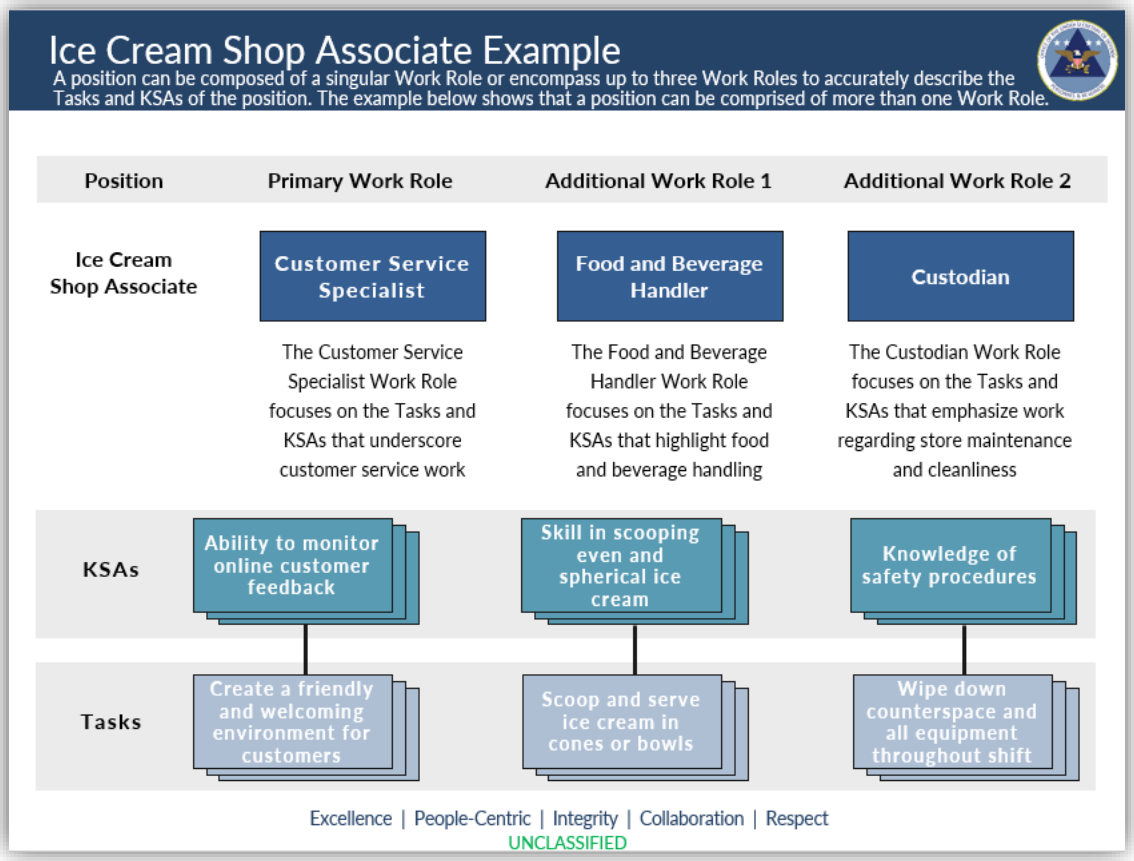

Figure 4: Functional Community Toolkit Example

Figure 5: Functional Community Toolkit Example

Key Benefits of Using DCWF Work Roles

- **Human Resources and Functional Managers can use work roles to:**
  - ✓ Develop role-based job announcements and positions descriptions that provide greater fidelity than existing occupational structures for targeted recruitment activities
  - ✓ Support recruiting efforts through identification of knowledge and skills
  - ✓ Identify and track work roles of critical need for workforce planning
  - ✓ Create career maps

- **Training Teams can use work roles to:**
  - ✓ Evaluate existing training for applicability
  - ✓ Update existing training with the relevant tasks and KSAs
  - ✓ Create new training
  - ✓ Share training knowing that the tasks and KSAs have been vetted by SMEs across DoD and approved

- **Individuals can use work roles to:**
  - ✓ Explore career pathing and skill requirements
  - ✓ Identify and gain skills in work roles of interest

Module 2:

An Introduction to DoD 8140 Policy

Figure 1: DoD 8140 Seal

Historical Background Knowledge: No longer in effect, the Department of Defense (DoD) 8570 Information Assurance (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:

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 redescribed 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.

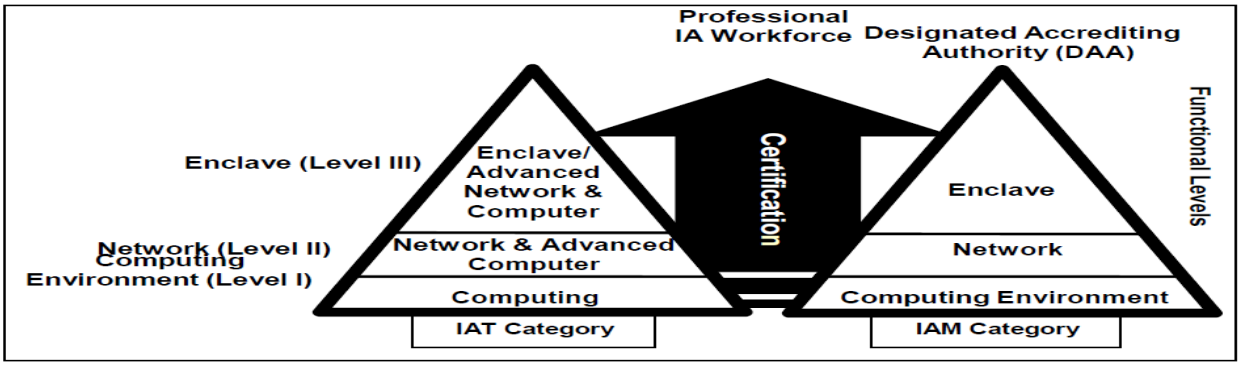

Figure 2: DoD 8570 IA Program

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 focus from information assurance to a broader view of the cyber workforce comprising personnel who build, secure, operate, defend, and protect DoD (now DoW) and U.S. cyberspace resources, conduct related intelligence activities, enable future operations, and project power in or through cyberspace.

Transition Period: The 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: This remaining information found in this modules provides a high-level overview of DoD 8140 policy tenants and benefits when applied properly.

- ✓ The DoD 8140 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 Cyber Workforce Qualification Program (CWQP) unifies the overall DoW cyber workforce 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 cyber workforce.
  - ➢ **Responsive**: The ability to identify and track DCWF work roles and measure DoW cyber workforce qualification at three different proficiency levels allows senior leaders to assess DoW cyber workforce readiness in a timely manner.

- ✓ The DoD 8140 CWQP addresses the scope of expertise needed for all cyber disciplines, using a comprehensive approach for cyber workforce 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: The DoW Cyber Workforce Management Board (CWMB), in accordance with DoD Directive 8140.01, is chartered as the Senior Executive Service (SES)/General/Flag Officer (GO/FO) level decision body that provides decisions on behalf of DoW Components. The CWMB Tri-Chairs are 1) The Office of the Under Secretary of War for Personnel and Readiness (OUSW P&R), 2) The Office of the Principal Cyber Advisor (OPCA), and 3) The DoW Chief Information Officer (CIO).

DCWF Work Roles: See *Module 1* of this document for additional information.

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 Level*s (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 cyber workforce personnel that 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.

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 cyber workforce personnel to demonstrate capability in a mission environment against the assigned DCWF work role and DoD 8140 proficiency level. DoW cyber workforce personnel must complete their DoW Component's DoD 8140 residential qualification requirements within twelve months of a DCWF work role assignment.

Continuous Professional Development: Upon attainment of both DoD 8140 foundational and residential qualification, DoW cyber workforce personnel are required to complete 20 hours of continuous professional development per fiscal year.

Privileged Access: DoD 8140 does not specify privileged access requirements (i.e., those with access to elevated control functions of systems & networks). DoW cyber workforce 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.

Letters of Designation or Appointment: DoD 8140 does not require appointing letters or official designations, as DCWF work role coding activities suffice.

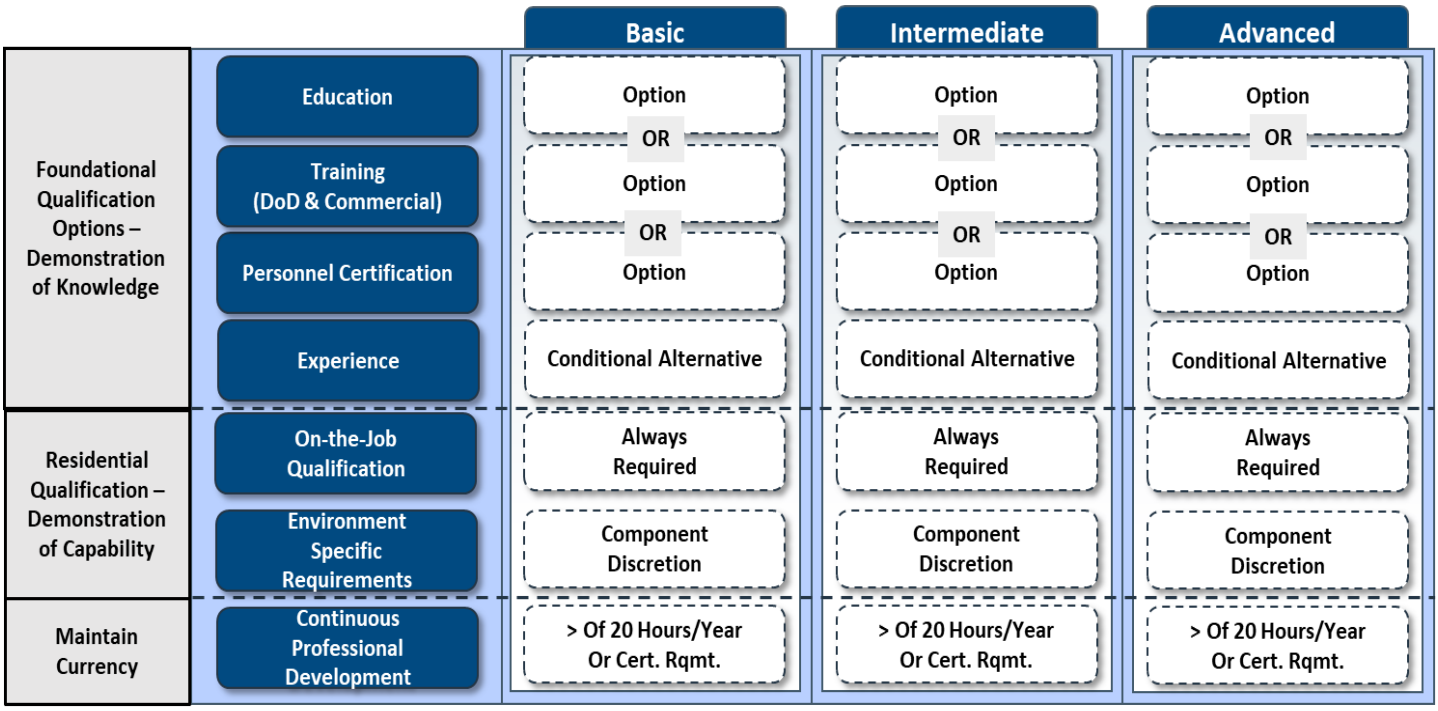

Figure 3: Sample DCWF Work Role Qualification Matrix

Module 3:

DoD Cyber Workforce Strategy Alignment to DoD 8140

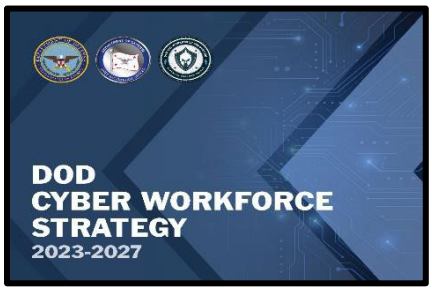

Figure 1: DOD CWF Strategy

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 workforce. The DCWS initiated DoD cyber workforce 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 DoD 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 cyber workforce management efforts developed over the past 20 years, while moving forward with specific actionable and measurable outcomes.

Module 3 Overview: This Strategy sets the foundation for how the DoW will foster a cyber workforce capable of executing the Department's complex and varied cyber missions and provides a unifying direction for DoW cyber workforce 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.

The 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.

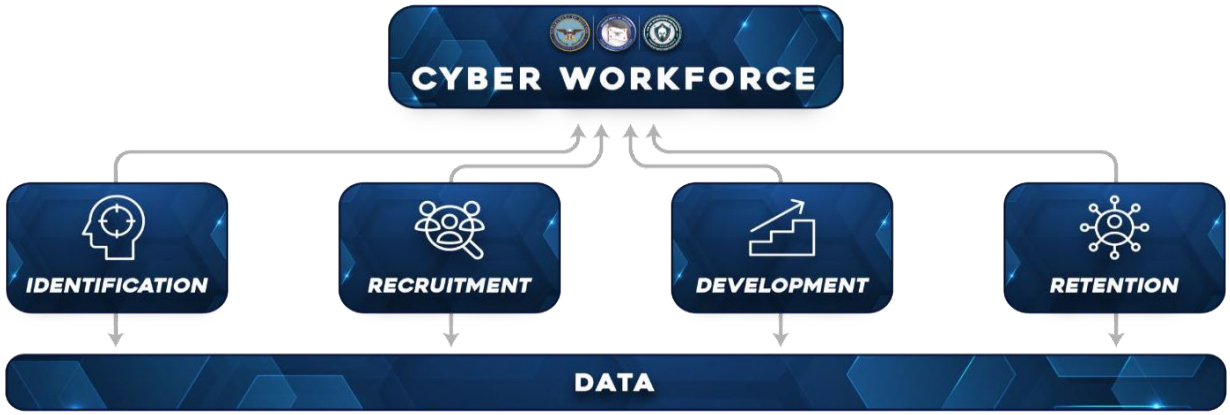

Figure 2: DoD Cyber Workforce Strategy Overview

The Strategy highlights actions for human capital strategic planning informed by DoW cyber workforce analytics garnered from DoD 8140 requirements. Successful execution of the Strategy and achieving these goals will enable the DoW to close cyber workforce development gaps, apply resources for cyber workforce initiatives, stay at the forefront of technological advances, securely and rapidly deliver resilient systems, and assess workforce 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 cyber workforce analytics. This roadmap supports data-driven talent management of critical skillsets and cyber workforce 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 4:

DoD 8140 Personnel Qualification Waiver Supplemental Information

Figure 1: DoD 8140 Seal

Module 4 Overview: This module describes supplemental guidance regarding Department of Defense (DoD) 8140 personnel qualification waiver eligibility in accordance with DoD Manual (DoDM) 8140.03, "Cyberspace Workforce Qualification and Management Program" (February 15, 2023) for military and civilian personnel in positions that are assigned DoD Cyber Workforce Framework (DCWF) work role codes. DoW Components may further promulgate guidance to support DoD 8140 waiver implementation and guidelines provided by the Department of War (DoW) Chief Information Officer (CIO).

DoDM 8140.03 Policy Waiver Language: DoDM 8140.03 Section 4, paragraphs 4.2c. and 4.2d. on page 20, specifies:

4.2c. *OSD and DoD Component heads, or a delegated authority, may waive the qualification requirements for DoD civilian employees and Service members only under severe operational or personnel constraints.*

(1) OSD and DoD Component heads:

(a) May delegate waiver authority, as appropriate, while retaining oversight of subordinate use of waiver authority.

(b) Will document, in a memorandum for the record, the justification for any granted waiver and the final plan to rectify the constraint.

(2) Waivers must include an expiration date, not to extend beyond 6 months, except in an emergency situation during a deployment to a combat environment. In this event, DoD civilian employees and Service members will make every attempt to achieve qualification without sacrifice to the mission requiring deployment. The 6-month waiver timeline will commence upon return from deployment, and the dates must be updated in all waiver documentation.

(3) Consecutive waivers for DoD civilian employees and Service members are not authorized. Waivers must be a management review item in accordance with DoDI 8500.01, "Cybersecurity" (Incorporating Change 1, October 7, 2019).

4.2d. *OSD and DoD Components must track cyberspace workforce qualifications against positions with cyberspace work role requirements in accordance with DoDI 8140.02, "Identification, Tracking, and Reporting of Cyberspace Workforce Requirements" (December 21, 2021) and this issuance.*

> *(1) OSD and DoD civilian employees and Service members assigned to positions identified as requiring the performance of more than one cyberspace work role must achieve qualification requirements for each cyberspace work role, unless an OSD or DoD Component head or a designated authority issues a waiver."*

Additional Guidance from DoW CIO: DoW military and civilian employment are governed by differing laws and regulations, including human resources policies codified by the U.S. Office of Personnel Management for DoW civilians. The following guidance considers typical absences by military and civilian personnel that would warrant DoD 8140 waiver eligibility to ensure that DoW cyber workforce members are not unduly impacted by situations practicably or legally considered to be outside of their control.

The criteria below are not intended to be all inclusive; DoW Components should develop supplemental guidance and procedures in alignment with DoD 8140 policy and provide oversight of the waiver process to promote consistent application and guidance across the organization.

DoW Components have the authority to approve waivers and the responsibility to document the justification for any waiver granted for DCWF work role qualification timelines, including plans to rectify constraints. DoD 8140 waiver eligibility related to DoD 8140 foundational & residential qualification timelines, in the cases of "severe operational or personnel constraints," may include the following:

Severe Operational Constraints:

- ✓ Administrative matters beyond an employee's control (e.g., technical, funding or scheduling issues)
- ✓ Unscheduled telework, leave, or weather/safety emergencies
    - Examples: If an agency announces unscheduled telework or an unforeseen operating status that would prevent the employee from working in-person; if an employee cannot report to work due to unforeseen circumstances; or if the work environment is unsafe and prevents the employee from performing work at the approved location due to unexpected or severe weather conditions or an emergency condition.

- ✓ A special detail directed by the DoW Component's commanding officer or official less than 120 days
    - Examples: A short-term, temporary assignment or detail of an employee to a different position or DCWF work role within or outside the DoW Component, to support a specific, assignment, project or task. A short-term, temporary assignment or detail's purpose may include: Handling crises or unexpected events, coping with unexpected increases in workload, covering vacancies or filling specific skill gaps, participation in short-term projects or studies, gaining experience in a different area or skill, or adapting to temporary changes in the DoW Component's structure.
- ✓ Deployment to a combat environment
- ✓ Long-term temporary duty (TDY) over 30 days

Personnel Constraints:

- ✓ Extended special leave and absences generally exceeding one month
    - Examples: Sick/convalescent leave; authorized leave (pay & non-pay status) for legal matters; parental/adoption leave; jury duty; any leave covered under the Family and Medical Leave Act (FMLA); human resource approved reasonable accommodation.
- ✓ For military personnel awaiting military schoolhouse training availability, DoW Components may grant additional time.

DoD 8140 Waiver Tracking & Reporting: DoW Components will compile, adjudicate, track, and retain all supporting waiver documentation. The DoW CIO may request waiver documentation to support DoD 8140 implementation and auditing efforts. DoD 8140 policy requires tracking and reporting of DCWF coded positions and the qualification status of the military and civilian incumbents of the positions.

To facilitate DoW-wide reporting, DoW CIO WID Analytics will collect waiver data for compliance purposes via an Excel file submitted from each DoW Component cyber workforce program manager starting fiscal year 2026 (FY26) via "DoD SAFE" or other secure mechanism. If you are not sure who to route your waiver data to, please coordinate with your DoW cyber workforce program manager or email DoW CIO WID Analytics at the following address: osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil

DoD 8140 Waiver Required Data Fields: The following data fields must be included in all DoD 8140 waiver reporting activities. No other detailed waiver information, such as Personally Identifiable Information (PII) or Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), will be collected by the DoW.

- ✓ Component
- ✓ Org/Unit Identification Code
- ✓ DoW ID Number (EDIPI); the DoW identification number, formerly referred to as the Electronic Data Interchange Personal Identifier (EDIPI), is a unique 10-digit number that is associated with each person and their Common Access Card (CAC).
- ✓ DCWF work role(s) & associated proficiency level(s) being waived (i.e., primary & additional)
- ✓ Revised/extended qualification date (numeric MM-DD-YEAR)

Additional Notes To Remember:

- ➢ If the constraints listed above affect groups of personnel, then all personnel in the group may be eligible for a DoD 8140 waiver.
- ➢ Regularly scheduled or routine leave or time off is **not** included as DoD 8140 waiver eligibility criteria.
- ➢ DoD 8140 waivers may be granted for any DCWF work role (i.e., primary or additional) at any proficiency level (i.e., basic, intermediate, or advanced) that is assigned to the encumbered position.
- ➢ DoD 8140 waivers may be used and managed by the DoW Component for any duration, up to six months.
- ➢ All DoD 8140 waivers must include an expiration date, not to extend six months. This limitation does not apply to military personnel who are unable to satisfy the requirement due to training availability or scheduling; consecutive waivers may be granted in these cases.
- ➢ DoD 8140 qualification timelines will commence or re-commence upon return from deployment or at the end of the "special absence" period. DoD 8140 qualification timelines before and after the special absence may be considered.
- ➢ DoD 8140 waiver documentation must include new qualification compliance dates in the employee's record.
- ➢ DoD 8140 waivers should be carefully managed for personnel in a probationary status.
- ➢ "DoD 8140 Waiver Required Data Fields" will be visible and tracked in DoW's Advana advanced analytics and data visualization platform for reporting to DoW senior leadership, the DoW Cyber Workforce Management Board (CWMB), and Congress, when required.

Sample Scenarios:

Parental Leave/FMLA: A civilian employee is working towards a DoD 8140 foundational qualification option through a commercial certification process and is eight months into the nine-month timeline. Prior to completing the certification requirements (e.g., training, examination) the employee is approved for parental leave. In this case, the qualification timeline is "paused" during the parental leave, and the employee still has one month upon return to complete DoD 8140 foundational qualification requirements. Towards the end of the initial nine-month qualification timeline after the employee has returned, the employee experiences an unforeseen certification assessment scheduling issue, and the employee is unable to reserve the certification assessment until twelve months into initial DCWF work role assignment. In this case, a DoD 8140 waiver may be introduced by the DoW Component to provide the employee up to an additional six months to schedule and complete the certification assessment.

Military Training Availability: A service member has received orders to attend a military schoolhouse training, which begins twelve months after the service member is coded to a DCWF work role. In this case, a DoD 8140 waiver may be granted beyond six months due to this training scheduling constraint, which is beyond the control of the DoW Component. While waiting to attend the training, the twelve months would not negatively count against the service member's qualification timeline.

Appendix A: DoW Cyber Workforce Management Resources & References

Governance

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*
DoD CWF Strategy	*https://dl.dod.cyber.mil/wp-content/uploads/cyber-workforce/pdf/unclass-cyber_workforce_strategy.pdf*
DoD CWF Strategy Implementation Plan	*https://dl.dod.cyber.mil/wp-content/uploads/cyber-workforce/pdf/unclass-cyber_workforce_strategy_implementation_plan.pdf*

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, 4th Estate, Federal Government, Commercial Partners	*osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil*

If you have additional questions, please connect with your DoW cyber workforce supervisor, and then connect with one of the mailboxes listed above. The mailboxes listed above can be found on the DoD Cyber Exchange (Public) at the following link: https://www.cyber.mil/dod-workforce-innovation-directorate/dod8140/help

Online Supplemental Guidance

Figure 1: DoD Cyber Exchange

Summary: The DoD Cyber Exchange provides one-stop access to cyber information, policy, guidance and training for cyber professionals throughout the DoW. These resources are provided to enable the user to comply with rules, regulations, best practices and federal laws. The Defense Information Systems Agency (DISA) is mandated to support and sustain the DoD Cyber Exchange as directed by DoD Instruction (DoDI) 8500.01 "Cybersecurity" (March 14, 2014) and DoD Directive (DoDD) 8140.01 (October 5, 2020).

Additional resources, such as the DCWF Revision Process Guide, the DCWF Workforce Identification and Coding Guide, and the DoD 8140 foundational qualification matrices are available online at the below listed web pages.

Topic Area	Name of Webpage	New DoD Cyber Exchange Webpage Links
DCWF	DCWF Homepage	***Public:*** *https://www.cyber.mil/dod-workforce-innovation-directorate/dod-cyber-workforce-framework*
DCWF	DCWF Student Self-Paced Training	***NIPR (CAC-Enabled):*** *https://www.cyber.mil/training*
DoD 8140	DoD 8140 Homepage	***Public:*** *https://www.cyber.mil/dod-workforce-innovation-directorate/dod8140*
DoD 8140	DoD 8140 Documents Library	***Public:*** *https://www.cyber.mil/dod-workforce-innovation-directorate/dod8140/documents-library*
DoD 8140	DoD 8140 Foundational Qualification Matrix Homepage	***Public:*** *https://www.cyber.mil/dod-workforce-innovation-directorate/dod8140/qualification-matrices*
DoD 8140	DoD 8140 Frequently Asked Questions	***Public:*** *https://www.cyber.mil/dod-workforce-innovation-directorate/dod8140/faq*
Cyber 101	DCWF Training	***NIPR (CAC-Enabled):*** *https://www.cyber.mil/dod-workforce-innovation-directorate/dod-cyber-workforce-framework/training*