



DOD 8140 SUPPLEMENTAL GUIDANCE FOR CYBER WORKFORCE MANAGEMENT V1.0

PUBLISHED JULY 2026



TABLE OF CONTENTS

Document Overview	3
Policy Update: Onboarding and Qualification Management	4
Policy Update: Mandatory Upskilling for DCWF KSAT Additions or Modifications	6
Policy Update: New DCWF Work Role Revision Process	7
Policy Update: Degree Discipline Flexibility	8
Policy Update: Supervisor of the CWF Member Verification Process For Foundational Qualification	9
Policy Update: Transient Status	11
Appendix A: DoD 8140 Personnel Qualification Waiver Supplemental Information	13



Document Overview

Summary: In collaboration with the military services, the Department of War Chief Information Officer Workforce Innovation Directorate (DoW CIO WID) has approved supplemental information pertaining to DoW cyber workforce qualification and has introduced a series of DoD 8140 policy updates to clarify current requirements in support of the cyber warfighter. These updates serve as an extension to the DoD 8140 issuances.

Each new policy update applies to all current and future Department Cyber Workforce Framework (DCWF) work roles under the cybersecurity (CS), information technology (IT), and cyber enabler (EN) workforce elements, at all three DoD 8140 proficiency levels.

Please continue to refer to the DoW CIO guidance pertaining to DoD 8140 waivers, originally published in June of 2025, as an addendum to this guidance. This document can be found here: <https://www.cyberworkforce.mil/DoD-8140/Document-Library/>

For a list of civilian occupational series that the DoW CIO requires to have a primary work role code, please refer to the *“DCWF Military and Civilian Workforce Identification and Coding Guide” V1.6, published August 2025, Table 2, on page 7.*

For a list of military occupational specialties (MOS) designated as cyber, as selected by each Service, please refer to the *“DCWF Military and Civilian Workforce Identification and Coding Guide” V1.6, published August 2025, Appendix C, beginning on page 21.* Each section contains MOS that require identification and coding of at least a primary DCWF work role due to alignment with cyber KSATs, and optionally up to two additional work roles.

As a reminder, the latest *“DCWF Military and Civilian Workforce Identification and Coding Guide”* can always be found on <https://www.cyberworkforce.mil/>.

This document is unclassified and is effective as of July 1, 2026.



Policy Update: Onboarding and Qualification Management

1.1. ONBOARDING REQUIREMENT.

- a. When a CWF member is coded to a DCWF work role and proficiency level (i.e., the effective date the CWF member encumbers the position in the CWF), authoritative manpower and personnel systems will be updated. Upon verification that the authoritative manpower and personnel system, if applicable, accurately reflect the cyber coding, the responsible CWF program manager has 10 business days to update the Component's authoritative readiness databases with the CWF member's information and issue a formal *"DoD 8140 Letter of Designation"* to the CWF member.

2.1. INITIATION OF QUALIFICATION TIMELINES.

- a. Both the 9-month foundational qualification and 12-month residential qualification timelines begin for the CWF member (MIL/CIV) upon official issuance of the DoD 8140 Letter of Designation. At time of document publication, issuing an official DoD 8140 Letter of Designation is at the DoW Components discretion.
- b. DoW contract support personnel must meet foundational qualification requirements upon commencement of cyberspace work in accordance with DoDM 8140.03.

4.1. CONTINUING OPERATIONS REQUIREMENTS.

- a. **Continued Validity:** A CWF member's foundational qualification requirements are permanently tied to the specific version of the foundational qualification matrix in effect on the date their qualification timeline is initiated, as documented by their signed *"DoD 8140 Letter of Designation."* A CWF member remains foundationally qualified for their designated DCWF work role and proficiency level after the initial policy requirement has been met, regardless of future foundational qualification matrix updates.
- b. **Maintenance:** The CWF member's continued foundational qualification is contingent upon:



- 1) The CWF member remaining in the same DCWF work role at the same assigned proficiency level.
- 2) The CWF member completing all annual continuous professional development requirements.

5.1. APPLICATION TO SPECIFIC SCENARIOS.

- a. **Retirement of a Foundational Qualification Option:** If a foundational qualification option is retired in a future version of the matrix, personnel who are foundationally qualified, or are in a documented process that verifies enrollment of foundationally qualifying under a legacy matrix, may still use the same option identified by the supervisor of the CWF member to achieve and maintain qualification requirements.
- b. To be considered “*in progress*,” the CWF member’s intent to pursue that specific credential must be documented in writing and acknowledged by their supervisor.
- c. **Upskilling Requirements:** Foundationally qualified personnel under a legacy matrix are still subject to mandatory workforce upskilling requirements.

6.1 CWF MEMBER RE-QUALIFICATION REQUIREMENTS.

- a. A CWF member’s foundational qualification status is voided under one of the following conditions:
 - 1) The CWF member is re-coded to a different DCWF work role or DoD 8140 proficiency level.
 - 2) The CWF member does not complete annual continuous professional development requirements.
- b. In either case, the CWF member will be required to foundationally re-qualify against the currently effective matrix.



Policy Update: Mandatory Upskilling for DCWF KSAT Additions or Modifications

1.1 UPSKILLING IMPLEMENTATION REQUIREMENT.

- a. Upon CWMB approval of new or modified DCWF KSATs, all affected personnel must complete the mandatory upskilling requirement within 24 months of the official DoW CIO WID publication of the updated DCWF work role content. CWF personnel remain foundationally qualified during this upskilling period.

2.1 COMPLIANCE METHODS.

- a. Upskilling requirements will be satisfied via one of the following prioritized methods:
 - 1) **Provisioned Training:** The DoW Component sponsoring the DCWF KSAT addition or modification, whether it is a DoW-wide initiative (e.g., Zero Trust) or an update approved at the Cyber Workforce Management Board, is responsible for providing or identifying funded training solutions to meet the new requirement. CWF personnel must complete the training provided by the designated sponsoring DoW Component within the prescribed time period, if one is provided.
 - 2) **DoW Component-Led Training:** For all other DCWF KSAT additions or modifications, including scenarios when a training plan is not provided by the DCWF work role's OPR, DoW Components may address the knowledge gap through residential qualification activities as an interim measure while the requirement is elevated for a funded solution. If residential qualifications are not available, targeted continuous professional development opportunities may be used.
- b. **Documentation:** All such activities must be documented in the CWF member's record and may be subject to inspection, audit, or other readiness assessment.



Policy Update: New DCWF Work Role Revision Process

1.1 NOMINATION REQUIREMENT.

- a. In order for a new work role to be nominated to the CWMB for inclusion into the DCWF, the sponsoring OPR must provide a draft foundational qualification matrix. This matrix may be based on foundational qualification options currently in use by personnel performing the functions of the proposed work role, or, in the case of emergent capability areas, a proposed candidate matrix based on industry standards, academic curricula, or analogous skill sets.

2.1 ADMINISTRATION PERIOD.

- a. Upon approval of a new work role(s) at the CWMB, DoW Components have three months to initiate the formal system change request to update their authoritative manpower and personnel systems.
- b. Upon the publication of the new work role content by the DoW CIO WID, DoW Components have nine months to code all personnel and billets with the new work role(s).

3.1 REPORTING EXEMPTION.

- a. A new DCWF work role is exempt from all foundational qualification readiness reporting until two conditions are met:
 - 1) A criticality analysis for the new DCWF work role has been completed.
 - 2) A foundational qualification matrix for this DCWF work role has been approved and published by the DoW CIO WID. The foundational qualification matrix must include one approved option (i.e., academic program, personnel certification, or training) that can be achieved in nine months or less at each proficiency level.



Note: This policy update rescinds DoW CIO memo and Correspondence and Task Management System (CATMS) tasker CIO000347-25, “DoD 8140 Qualification Reporting Update.”

4.1 END OF EXEMPTION.

- a. This exemption ends, and the standard 9-month foundational qualification timeline begins, for all CWF personnel coded to this new DCWF work role on the date that both conditions of Section 3.1 “*Reporting Exemption*” have been met. This end of exemption will be documented in formal correspondence by the DoW CIO WID.
- b. The supervisor of the CWF member will notify affected personnel of this status change and document the member’s plan to achieve foundational qualification. This action may be completed using an Individual Development Plan (IDP).

Policy Update: Degree Discipline Flexibility

1.1. POLICY.

- a. DoW Components are authorized to accept a degree as meeting a foundational qualification (education) requirement if its discipline is determined to be substantially similar to the one listed in the foundational qualification matrix. An exact word for word match of a degree title to the degree discipline listed in the foundational qualification matrix is not required, provided the DoW Component validates the degree relevance to the DCWF work role.
- b. This policy applies to degree titles that have been updated by academic institutions.

3.1 INTERNAL DOW ROTATIONAL PROGRAMS (E.G., FEDERAL ROTATIONAL CYBER WORKFORCE ROTATION PROGRAM).

- a. This policy establishes a rule for reciprocity, “*Acceptance of DoW Rotational Program Reciprocity.*” Gaining DoW Components will recognize and accept the existing, valid foundational qualification and, if appropriate, residential qualifications of a CWF member rotating from another DoW Component.



4.1 EXTERNAL (INDUSTRY) EXCHANGE PROGRAMS (E.G., CYBER INFORMATION TECHNOLOGY EXCHANGE PROGRAM, PUBLIC/PRIVATE TALENT EXCHANGE PROGRAM).

- a. This policy acknowledges the unique risk of non-DoW personnel performing cyber work on the DoW network, and introduces a formal risk-management solution. A dedicated risk management process is required to govern the access of non-DoW personnel from industry.
- b. DoW Components must establish a formal, documented risk-acceptance process, approved by a designated senior official, before granting any system access, particularly unsupervised privileged access.
- c. **Minimum Vetting:** Favorable adjudication sufficient for Common Access Card issuance.

Policy Update: Supervisor of the CWF Member Verification Process For Foundational Qualification

1.1 ROLES AND RESPONSIBILITIES.

- a. DoW Components should determine processes to document, review, validate, and approve continuous cyber work. The criteria noted in this policy is not intended to be all inclusive; DoW Components should develop supplemental guidance and procedures in alignment with DoD 8140 policy and provide oversight of this process to promote consistent application and guidance across the organization.
- b. Through their DoW Component, supervisors of the CWF member are granted the authority to verify the CWF member's continuous cyber work and will officially document the justification for this verification. This documentation must be verifiable and retained for inspection, audit, or readiness assessment purposes.
- c. Supervisors of the CWF member may require the CWF member to complete additional qualification activities if gaps in the performance of cyber work are identified.



2.1 APPLICABILITY.

- a. This process may be leveraged to support foundational qualification for any DCWF CS, IT, or EN work role (i.e., primary or additional) at any proficiency level (i.e., basic, intermediate, or advanced) that is assigned to the encumbered position.
- b. Continuous cyber work applies to any DCWF work role.

3.1 VERIFICATION PROCESS.

- a. **Governance Principle:** If a CWF member achieved a DoD 8140 approved degree or training more than 5 years prior to their date of encumbering the position in the CWF, the supervisor of the CWF member may verify continuous cyber work to satisfy the 5-year foundational qualification recency requirement. A DoD 8140 approved training or degree may be used to satisfy foundational qualification as far back as continuous cyber work can be verified.
- b. **Policy Standard:** DoDM 8140.03 considers demonstration of continuous cyber work as documentation of employment covering any DCWF work role.
- c. **Verification Process:**
 - 1) **Step 1:** The supervisor of the CWF member will use the CWF member's documented completion of annual continuous professional development (CPD) and a review of the CWF member's employment history as evidence to support the verification of the performance of cyber work.
 - 2) **Step 2:** If the supervisor of the CWF member cannot verify the CWF member's performance of continuous cyber work through either direct employment history or by using CPD records, then the CWF member must foundationally qualify using a different foundational qualification option.



3.2 TABLE 2: QUALIFICATION REPORTING SCENARIO.

Foundational Qualification Method	Date of Achievement	(NEW) Verification Method
Training	✓ January 1, 2026	N/A
Education	January 1, 1980	✓ CPD OR Supervisor of the CWF Member Verification

*Table 2 illustrates how the foundational qualification 5-year recency requirement **OR** the two types of verification methods, CPD **OR** Supervisor of the CWF Member Verification, satisfies the requirement.*

Policy Update: Transient Status

1.1 REQUIREMENT.

- When a military CWF member is assigned to a non-cyber billet for a period exceeding six months for career-broadening, leadership, operational, or other temporary duties, their status will be changed to “*Transient Status*,” removing the military CWF member from standard foundational and residential qualification reporting for the duration of their assignment.
- Civilian CWF member personnel actions will continue to be governed by civilian personnel regulations (e.g., Title 5, Office of Personnel Management).



2.1 GOVERNANCE.

- a. While in “*Transient Status*,” their qualification baseline is considered “*frozen*” against the DCWF work role and DoD 8140 proficiency level of their last assigned cyber billet, and their only DoD 8140 requirement is to complete their annual 20 hours of continuous professional development relevant to that baseline to maintain currency.
- b. The “*Transient Status*” expires upon the member’s return to a coded DCWF billet.

3.1 LIST OF DESIGNATED MILITARY DUTIES.

- a. Consider the below list of possible duties when considering if military personnel should be classified under this policy: The “*Transient Status*” is limited to military personnel assigned to the following designated duties:
 - 1) Limited, rotational, joint, or special duty assignments outside of primary cyber units.
 - 2) Natural disaster and/or homeland defense response operational support.
 - 3) Professional military education (PME) or structured professional development tied directly to promotion eligibility or maintenance of a military occupational specialty, enlisted classification or specialty code.
 - 4) Any duty that takes the service member outside of their military occupational specialty, enlisted classification or specialty code.
 - 5) Specialized staff roles or command positions (e.g., OIC Billet, Command Executive Officer, Company or Squadron Commander).
 - 6) Specialized duties supporting institutional requirements (e.g., Drill Instructor, Recruiter, Recruit Training Command Staff).



Appendix A: DoD 8140 Personnel Qualification Waiver Supplemental Information

Purpose

To issue supplemental guidance regarding DoD 8140 personnel qualification waiver eligibility in accordance with Department of Defense Manual (DoDM) 8140.03, “Cyberspace Workforce Qualification and Management Program” (Pub. 15 February 2023) for military and civilian personnel in positions that are assigned DoD Cyber Workforce Framework (DCWF) work role codes.

Components may further promulgate guidance to support DoD 8140 waiver implementation and guidelines provided by DoD Chief Information Officer (CIO).

This appendix is current as of June 3, 2025.

DoDM 8140.03 Policy

DoD military and civilian personnel must complete DoD 8140 foundational qualification requirements within nine (9) months of assignment to a DCWF cyberspace work role, and Component/organizational residential qualification requirements within twelve (12) months of assignment to a DCWF cyberspace work role.

For DoD cyber workforce personnel (i.e., military and civilian personnel in positions with DCWF primary and/or additional work role code(s) assigned) who may require a DoD 8140 qualification waiver, the governing policy is DoDM 8140.03, Section 4, paragraphs 4.2c. and 4.2d. on page 20 which 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.

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" (Pub. 21 December 2021) and this issuance.

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 DoD CIO

Military service and federal civilian employment are governed by differing laws and regulations; civilians are also governed by human resources policies codified by the U.S. Office of Personnel Management (OPM). The following guidance considers typical absences by military and civilian personnel that would warrant DoD 8140 waiver eligibility to ensure that DoD 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; Components should develop supplemental guidance and procedures in alignment with this policy and provide oversight of the waiver process to promote consistent application of policy and guidance across the workforce. 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**

- 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 prevented the employee from performing work due at the approved location due to unexpected/severe weather conditions or an emergency condition. Components are delegated the authority to exercise discretion for determining impacts to qualification timelines.
- A special detail directed by the DoD Component’s commanding officer or official less than 120 days
 - Examples: A short-term, temporary assignment of an employee to a different position or DCWF work role within or outside the DoD Component, to support a specific, assignment, project or task.
 - A special detail’s purpose would 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 agencies structure.
- Deployment to a combat environment
- Long-term temporary duty (TDY) (over 30 days)

If these constraints affect groups of personnel, then all personnel in the group may be eligible for a waiver eligibility.



➤ Personnel Constraints

Extended special leave and absences generally exceeding one month, excluding routine or regularly scheduled leave or time off, may warrant a waiver. Examples include:

- sick/convalescent leave
- authorized leave (pay & non-pay status) for legal matters
- parental/adoption leave
- jury duty
- any leave covered under Family and Medical Leave Act (FMLA)
- Human Resource (HR) approved reasonable accommodation
- Administrative matters beyond an employee's control (e.g., funding or scheduling issues). For service members specifically awaiting military schoolhouse training availability, Components may grant additional time.
- *Does **not** include regular leave or time off.*

DoD 8140 Waiver Tracking & Reporting

Components will compile, adjudicate, track, and retain all supporting waiver documentation. The DoD CIO Workforce Innovation Directorate (WID) may request waiver documentation to support program 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 DoD-wide reporting, DoD CIO WID Analytics will collect waiver data for compliance purposes via an Excel file submitted from each Component cyber workforce program manager starting FY26 via “DoD SAFE” or other secure mechanism. If you are not sure who to route your waiver data to, please coordinate with your cyber workforce program manager or email DoD 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 DoD.*

- Component
- Org/Unit Identification Code
- DoD ID Number (EDIPI)
 - *The DoD 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).*



- Work Role(s) & associated Proficiency Level(s) being waived (Primary & Additional)
- Revised/extended Qualification date (numeric MM-DD-YEAR)

Additional Notes To Remember

- DoD 8140 waivers may be granted for any DCWF work role (i.e., primary or additional) that is assigned to the encumbered position.
- DoD 8140 waivers may be used and managed by the DoD Component for any duration, up to six (6) months.
- All DoD 8140 waivers must include an expiration date, not to extend six months.
 - This limitation does not apply to service members who are unable to satisfy the requirement due to training availability or scheduling; consecutive waivers may be granted in these cases.
- DoD 8140 qualification timeline 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 DoD’s *Advana* advanced analytics and data visualization platform for reporting to DoD senior leadership, the Cyber Workforce Management Board, and Congress, when required.
- Per DoDM 8140.03, “Waivers must be a management review item in accordance with DoDI 8500.01, “Cybersecurity” (Pub. 14 March 2014). DoDI 8500.01 addresses Cybersecurity inspections, assessments, and reviews for all DoD organizations.

Sample Scenarios

Parental Leave/FMLA: A civilian employee is working towards a DoD 8140 foundational qualification option through a commercial certification process and is four months into the nine-month timeline. Prior to completing 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 five months upon return for qualification (for the nine-month timeline). Due to the timing of the leave and its effect on training and examination availability, a waiver/extension may be granted per Component approval that extends the nine-month timeline for an additional period, not to exceed six months, for obtainment of certification.



Military Training Availability: A service member has received orders to attend a military schoolhouse training, which begins (12) months after the service member is coded to the DCWF work role. In this case, a DoD 8140 waiver may be granted beyond six (6) months due to this training scheduling constraint, which is beyond the control of the Component. While waiting to attend the training, the twelve (12) months would not negatively count against the service member's qualification timeline.

DoD 8140 Helpdesk

If you have additional questions, please connect with your supervisor, and then connect with one of the mailboxes below.

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

4th Estate:

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