DoD Cyber Workforce Framework (DCWF)

Military & Civilian

Workforce Identification & Coding Guide

Version 1.6

August 2025

Prepared by

The Office of the DoD Deputy Chief Information Officer for
Resources & Analysis, Workforce Innovation Directorate

Table of Contents

I. Executive Summary

The DoD cyber workforce operates within a warfighting domain that continues to evolve in terms of technology, threats, and work complexity. Talent and workforce management practices must also continue to evolve to address ever-changing mission requirements. The Department must recruit, develop, and retain a highly skilled workforce that is adaptable in leveraging emerging technologies in dynamic threat environments. Workforce readiness and mission success and rely on a knowledgeable and skilled workforce with the agility to fulfill mission requirements through demonstrable work role capabilities. The DoD Cyber Workforce Framework (hereafter referred to as "DCWF" or the "Framework") provides a standardized approach to describe work for military, civilian, and contractor personnel and affords a methodology to tailor talent management activities based on mission demand signals.

II. Purpose

This document provides supplemental guidance for military and civilian workforce coding efforts to support implementation of the Department of Defense Instruction (DoDI) 8140.02 "Identification, Tracking, and Reporting of Cyberspace Workforce Requirements." For the purpose of this guide, DCWF coding is focused on the identification of positions that require the execution of ANY work role defined within the Framework. Identification includes selection of appropriate work role(s) and a proficiency level associated with each work role.

Components may provide additional, more specific guidance in accordance with DoDI 8140.02. Nothing in this guide replaces, negates, nor infringes on other position/personnel coding requirements as stipulated by Federal, DoD, Component, organizational or functional community policies and programs.

This guide addresses the following topics:

- DoD workforce coding requirements utilizing the DCWF
- Identification and selection of work roles and proficiency levels
- Differentiation between positions and work roles
- Steps for coding civilian positions in the Defense Civilian Personnel Data System (DCPDS)
- Cyber coding's importance for data analytics in *Advana*
- Resources for coding efforts

III. Updates

This guide includes updates based on DoD 8140 policy requirements and lessons learned from workforce coding activities. It expands upon and supersedes previous DoD cyber coding guides. This version replaces the four recognized civilian cyber occupational series with a new expanded list, and all positions in these occ series must be assigned a primary work role code. A new appendix (Appendix C) has been added for military occupational series designated as cyber, selected by the Services, with requirements to code those occupational series. Version 1.6 implements minor corrections and updates for clarity but no new content.

IV. Applicability

This guide is applicable for coding positions with DCWF work roles for all DoD military, including Active Duty and Reserve, as well as the National Guard and U.S. Coast Guard under DoD direction, and DoD civilian positions regardless of funding source or personnel system. DCWF work roles apply to positions in both the competitive and excepted service (e.g., General Schedule (GS), Defense Civilian Intelligence Personnel System (DCIPS), Cyber Excepted Service (CES), and DoD Civilian Acquisition Workforce Personnel Demonstration Project (AcqDemo)). DCWF coding is required in addition to other DoD position requirements that may be required by executive orders; federal regulations; Office of Personnel Management (OPM) standards; and other national, DoD and Component policies, programs, personnel systems, and functional communities.

Figure 1: DCWF Seal

This guide is not applicable to DoD contractors as the Defense Federal Acquisition Regulation Supplement (DFARS) is pending update; more guidance will be promulgated when approved.

V. The Framework

The DCWF is the authoritative reference, as governed by the DoD Cyber Workforce Management Board (CWMB) for the identification, coding, qualification, tracking, and reporting of positions and personnel, serving as the Department's coding structure for authoritative manpower and personnel systems, pursuant to DoDD 8140.01. The DCWF continues to expand in order to support holistic digital workforce management, mission requirements, industry standards, and definition of work for emerging technologies.

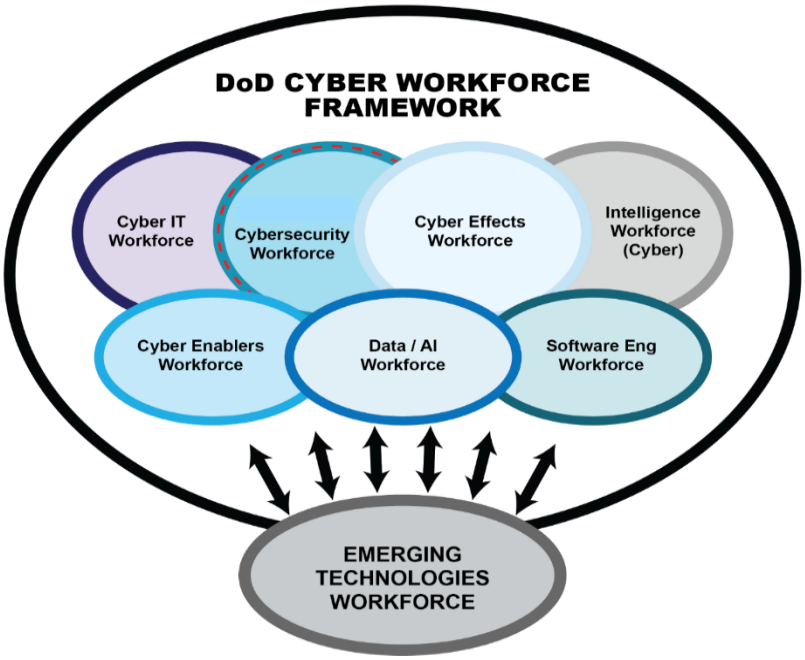


Figure 2: DCWF Workforce Elements

VI. Work Role Identification

DCWF work roles are comprised of the knowledge, skills, abilities, and tasks (KSATs) necessary to perform the work role successfully and identify capabilities. Work roles do not prescribe or limit the use of particular military occupational specialties, civilian occupational series, or career fields; they can be assigned to any occupational series or military specialty. Components may develop "crosswalks" to facilitate coding efforts and promote consistency. Identification of a position's KSAT requirements and selection of corresponding work roles and proficiency levels provide a means to assess readiness and capability. New, vacant, and encumbered military and civilian positions should be validated by leaders and supervisors on a regular basis to assure their alignment with higher-level mission imperatives and organizational direction, as well as the work that is needed to be performed. Work roles are driven by the purpose of the position rather than the preferences of a position's incumbent.

Every military and civilian position (or billet) across DoD that performs DCWF work activities must be assigned at least one work role code, and this coding is executed in Service or agency manpower systems.

DoD authorizes the assignment of up to three work role codes for each position. The first work role, which is known as the "primary" work role, indicates the predominant functions of a position's work. The position's official or organizational title may reflect the primary work role title but is not required. The primary work role is followed by the "Additional 1" and "Additional 2" work roles. The selection of a single DCWF work role code may be sufficient to ensure the right skill set is identified for the position. It is not necessary to identify every KSAT performed in a position, however, the core KSATs should reflect the major duties and responsibilities of a position.

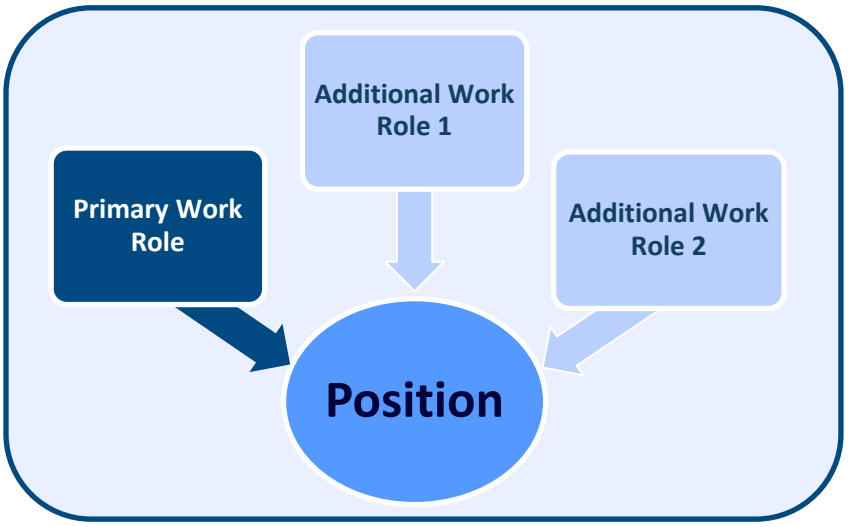


Figure 3: Position & Work Role Relationship

Military and civilian positions, as well as the personnel encumbering positions that **must be coded** with DCWF work roles and proficiency levels, include the following:

- ☑ Positions identified as performing work aligned to DCWF work roles
- ☑ Positions aligned to the civilian occupational series that DoD CIO has designated as cyber
- ☑ Military occupational specialties that Components have designated as cyber

Primary & Additional Work Role Codes

The primary work role code identifies the work role that encompasses the majority of a position's duties and responsibilities. A primary work role applied to a billet or position indicates that the foremost purpose of the position is described by that DCWF work role.

The selection of a primary work role should periodically be reviewed to ensure that changes resulting from organizational requirements and evolution of applicable technologies are considered for its continued suitability in describing the predominant duties. Identification of work roles for positions should be a deliberate process involving Component officials, organizational leaders, supervisors, and human resources (HR) professionals.

The Additional 1 and Additional 2 work role codes are utilized to capture other key work duties required of the position. If all three (primary, Additional 1 and Additional 2) work roles are used, the primary work role captures the majority of the requirements of a position, indicating that the majority of time is spent performing duties aligned to the primary work role. The additional work roles are not less important; they are just performed less frequently.

All work roles assigned to a position require the incumbent to complete Foundational and Residential qualification for each work role in accordance with DoDM 8140.03, "Cyberspace Workforce Qualification and Management Program."

Positions that have no applicable DCWF codes should be left uncoded. Per DoDI 8140.02, "Personnel in positions performing limited or infrequent cyberspace tasks should be evaluated to determine whether positions require cyberspace coding."

Work Roles

Managers and HR can use work roles to:

- Develop role-based job announcements (JOAs) and position descriptions (PDs)
- Support recruiting efforts through identification of required knowledge and skills
- Identify and track work roles of critical need for workforce planning activities

Table 1: Work Role Coding Differentiation: Primary and Additional Work Roles

Work Role Coding Differentiation
Primary Work Role
• A primary work role must be applied when the majority of a position's duties align with a DCWF work role code. • The selection of a primary work role code means this work role skill set has the highest priority for qualification amongst the work roles assigned to the position. • If the majority of a position's duties do not align with a DCWF work role code, but the position does have some duties that align with a DCWF work role code, then the position should be assigned a "000" code. • At least one additional work role, Additional 1, must be applied when "000" is selected as the primary work role. • Positions in the civilian occupational series designated as cyber by DoD CIO are required to have primary work role code that is not "000" (See Table 2). • A temporary exemption is required for the recognized cyberspace civilian occupation positions if they are assigned a primary work role code of "000" or if these positions are not coded at all. • Leave all coding fields blank if the position does not perform work aligned with the DCWF.

Additional 1 Work Role
• An additional work role should be applied to positions that perform duties that align with a DCWF work role code but are not the primary work role. • An Additional 1 work role code must be assigned if "000" is assigned as the primary work role. • Leave blank if no other work defined in the DCWF is performed outside the designated primary work role code. This field should never be coded "000."
Additional 2 Work Role
• An Additional 2 work role should be applied to positions that perform duties that align with a DCWF work role code but are not the primary work role nor the Additional 1 work role.

Proficiency Levels

A proficiency level must also be applied for each DCWF work role coded to a position. Per DoDI 8140.02, valid DCWF proficiency levels are *Basic, Intermediate, and Advanced* with these definitions:

- *Basic.* The role requires an individual to have familiarity with basic concepts and processes and the ability to apply these with frequent, specific guidance. An individual must be able to perform successfully in routine, structured situations.
- *Intermediate.* The role requires an individual to have extensive knowledge of basic concepts and processes and experience applying these with only periodic high-level guidance. An individual must be able to perform successfully in non-routine and sometimes complicated situations.
- *Advanced.* The role requires an individual to have an in-depth understanding of advanced concepts and processes and experience applying these with little to no guidance. An individual must be able to provide guidance to others; and the work must be performed as a **primary** or **additional** work role.

Coding Process and Requirements

Supervisors, managers, and Human Resources (HR) professionals must review and identify positions and personnel engaged in DCWF work role activities. Periodic reviews, conducted at least annually, should result in determination of appropriate DCWF work role codes and proficiency levels. If there are positions that are not currently coded but perform work aligned with the DCWF, then applicable work role codes and corresponding proficiency levels must be applied.

By Civilian Occupational Series

DoD CIO **requires** civilian personnel with the following occupational series to have a primary work role code:

Table 2: Required Cyber Civilian Occupational Series

Code	Name
0332	Computer Operation
0335	Computer Clerk and Assistant
2210	Information Technology Management
1550	Computer Science
0854	Computer Engineering
0308	Records and Information Management
1515	Operations Research
1529	Mathematical Statistics
1530	Statistics
1560	Data Science

DoD CIO **recommends** personnel with the following civilian occupational series to be reviewed for strong alignment to cyber functions and assigned a work role code as applicable:

Table 3: Recommended Cyber Civilian Occupational Series

Code	Name
0080	Security Administration
0132	Intelligence
0301	Miscellaneous Administration and Program
0306	Government Information
0340	Program Management
0343	Management and Program Analysis
0390	Telecommunications Processing
0391	Telecommunications
0392	General Telecommunications
0850	Electrical Engineering
0855	Electronics Engineering
0856	Electronics Technical
1520	Mathematics
1811	Criminal Investigation
2502	Telecommunications Mechanic
2504	Wire Communications Cable Splicing

Exemptions

If a civilian position within the required cyber civilian occupational series (refer to Table 2 above) is coded with a primary work role code of "000," it must have an approved temporary exemption, even if the position has an Additional 1 work role code assigned or if the position is not coded at all.

- Exemptions are temporary, adjudicated by Components, and coordinated with DoD CIO WID.

VII. Civilian Coding in DCPDS

This section is specific to coding civilian personnel in the Defense Civilian Personnel Data System (DCPDS) with DCWF work role codes and proficiency levels in accordance with DoD Instruction 8140.02. The coding outlined in this guidance should be completed following the successful determination of position requirements and proficiency levels. For each personnel record, DCWF work role coding in DCPDS should be aligned to work role coding for that encumbered position in a Component's authoritative manpower system.

Work roles are assigned to a particular position description (PD) so all positions associated with a PD must have the same work role codes.

DoD civilians that must have a DCWF work role and a proficiency level (Standard 1) coded to their position include the following:

- Personnel performing activities aligned to any DCWF work role
- Personnel aligned to occupational series that require coding (See Table 2)

DoD civilians that have converted to CES must be coded with an Intel/Cyber Indicator of "3" and Current Appointment Authority of "UKM" (Standard 2 and Standard 3) regardless if they have DCWF work roles assigned.

"Program Unique Information" Fields

- These fields store cyber workforce data accordance with DoDI 8140.02.
- Work role data captured here should be aligned to DoD standards**, not OPM standards**, as OPM does not recognize the use of "000" as a valid primary work role.
- *"Cybersecurity Category & Specialty Area"* codes record work roles in accordance with OPM policy in a separate section of DCPDS. DoD does **NOT** track usage these fields. Please consult your cyber workforce lead for further guidance.

DCPDS Data Elements:

- Program Unique Information Fields
  - Cyber Program Identifier and associated Cert Start Date
  - Primary Work Role Code and associated Proficiency Level
  - Additional Work Role Code 1 and associated Proficiency Level
  - Additional Work Role Code 2 and associated Proficiency Level
- Current Appointment Authority
- Intelligence/Cyber Position Indicator

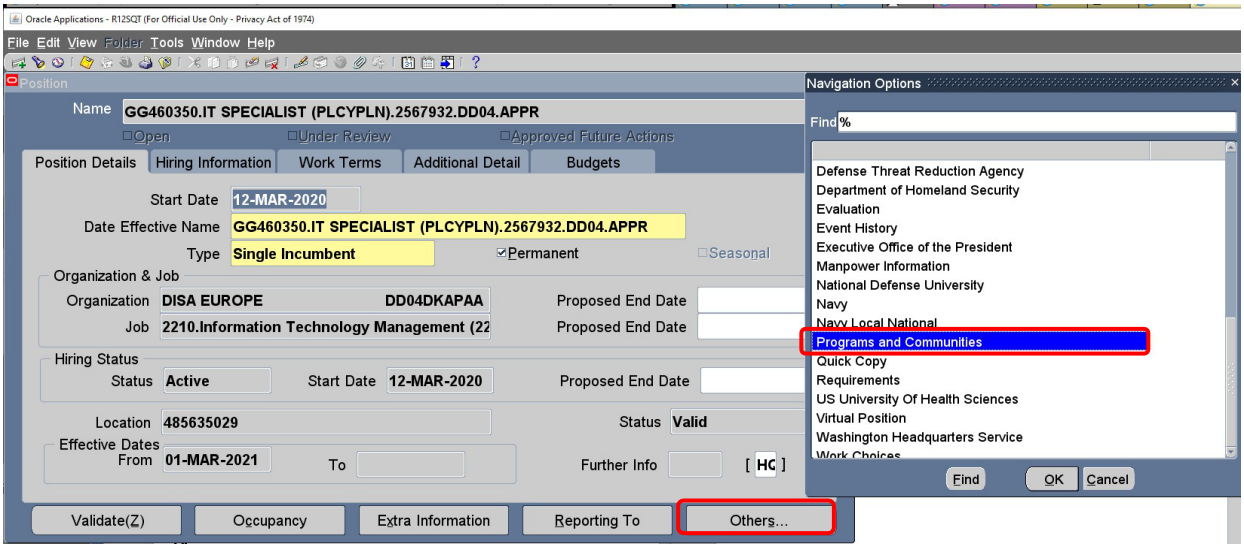
Standard 1

Program Unique Information Fields

The Program Unique Information Fields are designed to capture DCWF work role codes in accordance with DoDI 8140.02. Note that this coding guidance is based on authorized DCWF codes, not OPM coding requirements. The steps necessary to navigate to these fields within DCPDS are as follows:

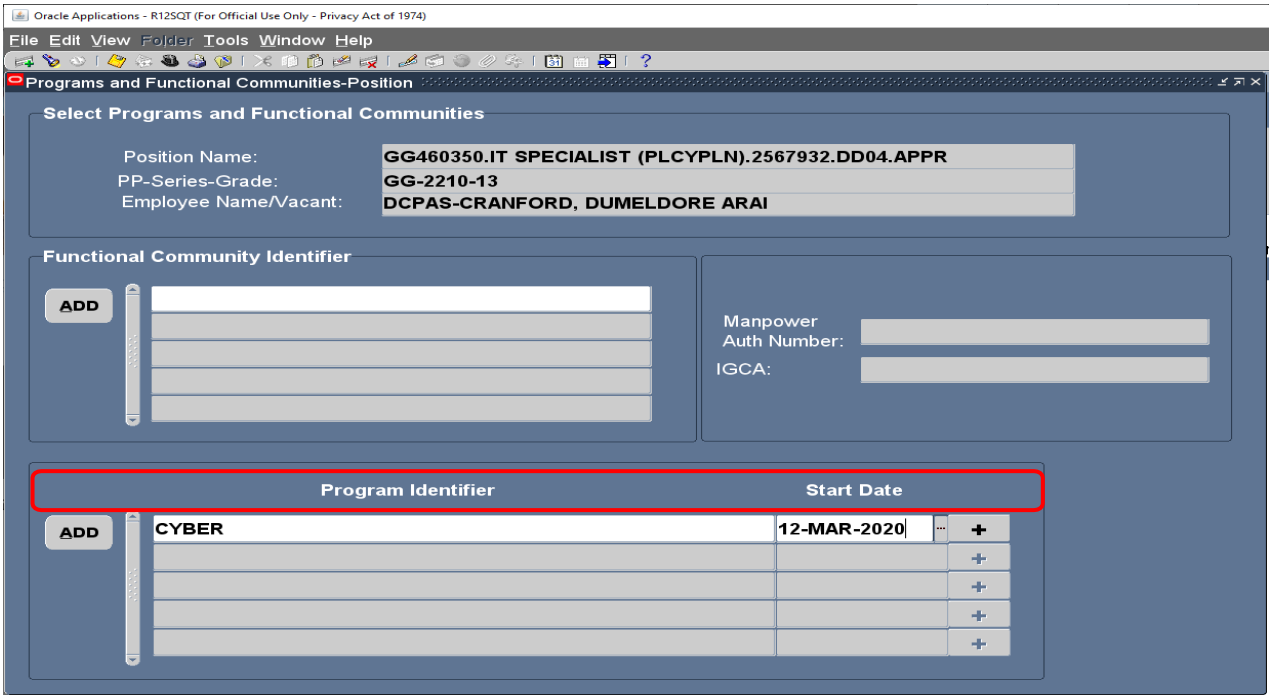
1. **Position/ Other/ Programs and Communities**

Figure 4: Position/Other/Programs and Communities



2. **Select "Cyber" and enter the current date.** as shown in Figure 5. This date solely indicates when the change was made to the personnel record and does not have any impact on qualification timelines specified in DoDM 8140.03. All work roles added to the DCWF, including Data/AI and Software Engineering workforce elements, are available under "Cyber" until DCPDS migrates to DCHRMS.

Figure 5: Program Identifier – Select "Cyber"



3. **Under Program Information**, select "Cyber," then enter the same "Cert Start Date" as entered previously; this date does not have an impact beyond noting the date that these DCWF work role codes were applied/updated to this position record.

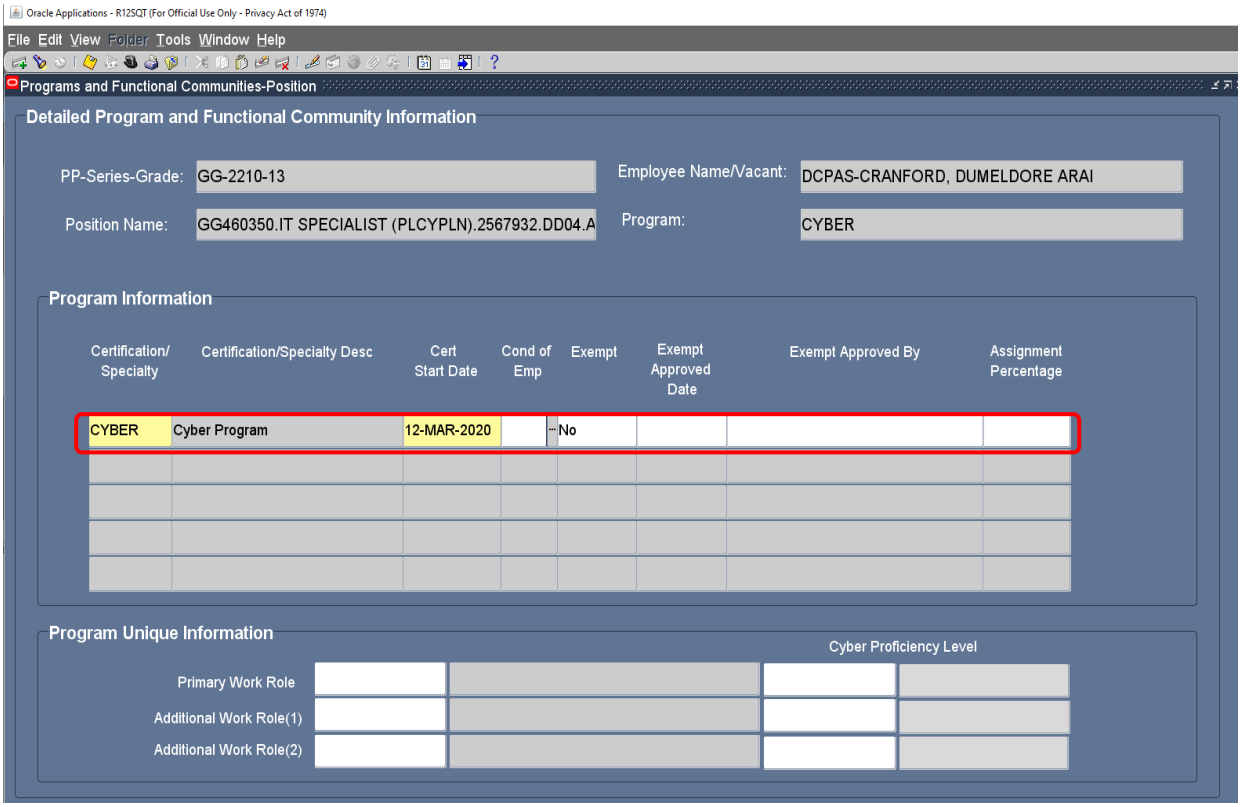


Figure 6: Program Information – Select "Cyber" and Enter "Cert Start Date"

4. **Program Unique Information fields**. Once the Program Information field is complete, you will be able to enter data into the Program Unique Information fields. Business rules for entering codes are:

Primary Work Role

- An associated proficiency level with the primary work role code must be applied per DoDI 8140.02.
- Valid entries for DCWF proficiency levels: B (Basic), I (Intermediate) or A (Advanced).
- Code "000" should be applied if a position is required to complete work aligned to a specific DCWF work role but that work does not constitute the majority of work duties. No proficiency level is applied with the "000" work role code.
    - If "000" is selected, at least one additional work role must be selected.
- If no DCWF work roles apply to the position, **leave all fields blank**.

> ***Note:***
>
> Coding *"Program Unique Information"* fields in the position section will automatically copy those codes over to the corresponding fields in the employee record, but not vice versa. Only code in the position section.

Additional Work Role 1

- This field can have a DCWF work role code assigned or be left blank. If a DCWF work role code is assigned, then a proficiency level must also be assigned.
- If the primary DCWF work role code was assigned as “000” then a non “000” DCWF work role code must be assigned in the Additional 1 work role and a proficiency level must also be assigned.
- Leave blank if no other work defined in the DCWF is performed outside the primary work role.
- Code 000 is not a valid entry for this field.

Additional Work Role 2

- This field can have a valid DCWF work role code assigned or left blank. If a DCWF work role code is assigned, then a proficiency level must also be assigned.
- The Additional Work Role 2 field can only be updated if a DCWF work role is entered into the Additional Work Role 1 field.
- Leave blank if no other work defined in the DCWF is performed outside the primary and Additional 1 work role.
- Code 000 is not a valid entry for this field.

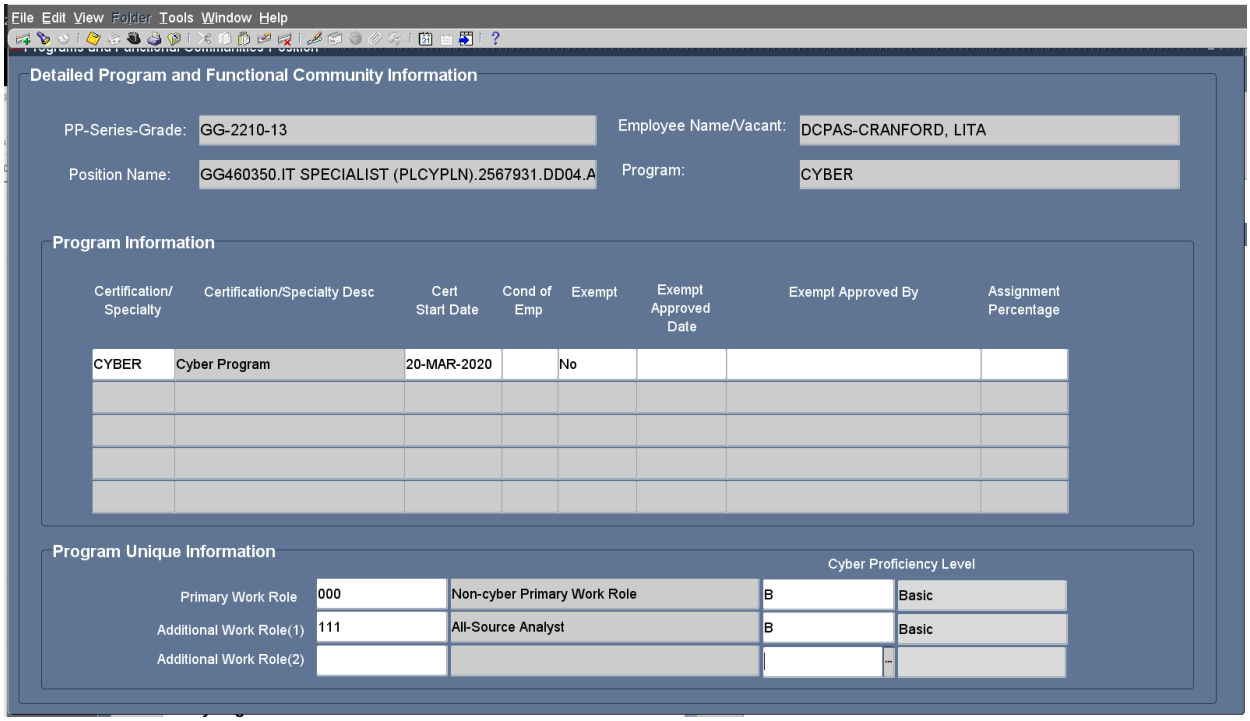


Figure 7: Detailed Program and Functional Community Information

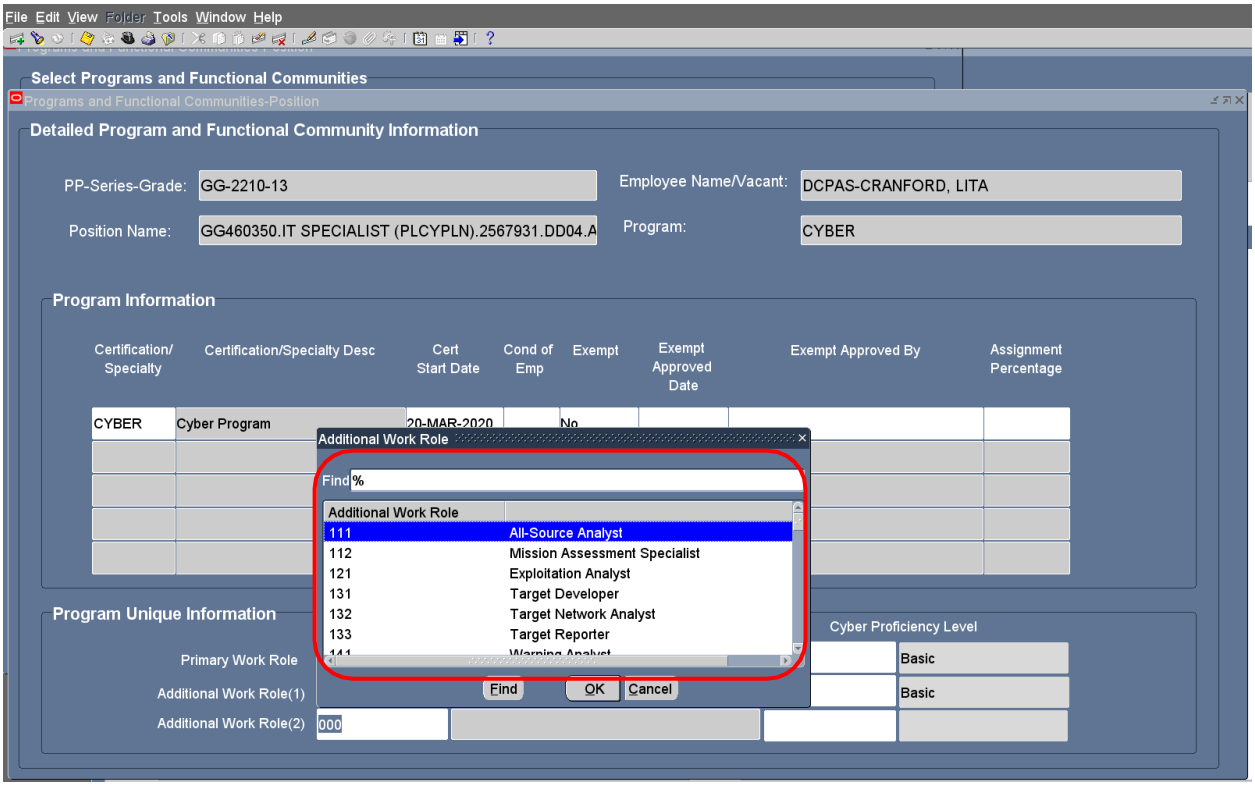


Figure 8: Detailed Program and Functional Community Information – Additional Work Role

Standard 2

Current Appointment Authority

Current Appointment Authority (CAA) as defined by OPM:

CAA is "The law, executive order, rule, regulation, or other basis that, in addition to Current Appointment Authority (1), authorizes an employee's most recent conversion or accession action."

Relevant CAA values for cyber are:

- UKM – This value indicates a personnel conversion into the Cyber Excepted Service (CES) personnel system.
- UAM – This value indicates a personnel conversion into the Defense Civilian Intelligence Personnel System (DCIPS).

NOTE: Other CAA values may apply based on the employee's accession authority into the position. These CAA options are listed above as they correspond to United States Code (USC) Title 10 civilian personnel systems that frequently utilize the DCWF.

There are additional CAAs maintained by OPM, further information can be found here: https://dw.opm.gov/datastandards/referenceData/caa/1428/current?index=C

Within DCPDS, you can navigate to the CAA page for a given position by selecting the following menus: *"People/Extra Information/US Federal Person Group 1/Current Appointment Authority"* as shown in Figure 9 and Figure 10.

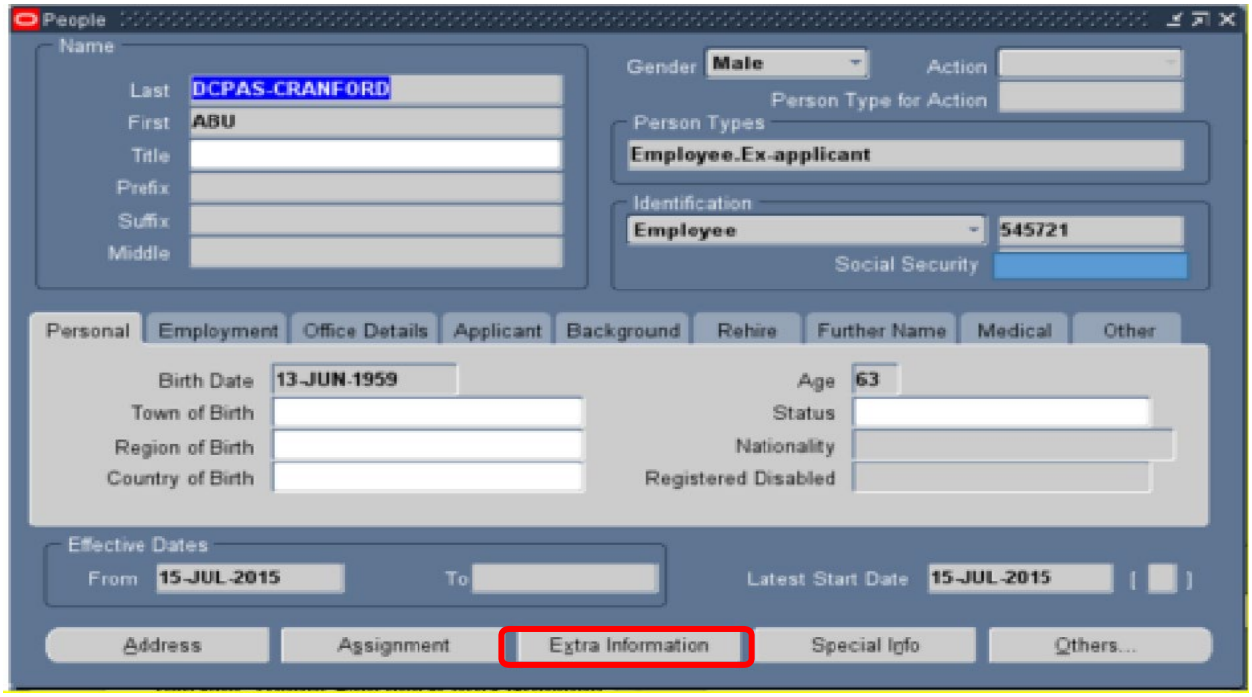


Figure 9: Current Appointment Authority (CAA) – People

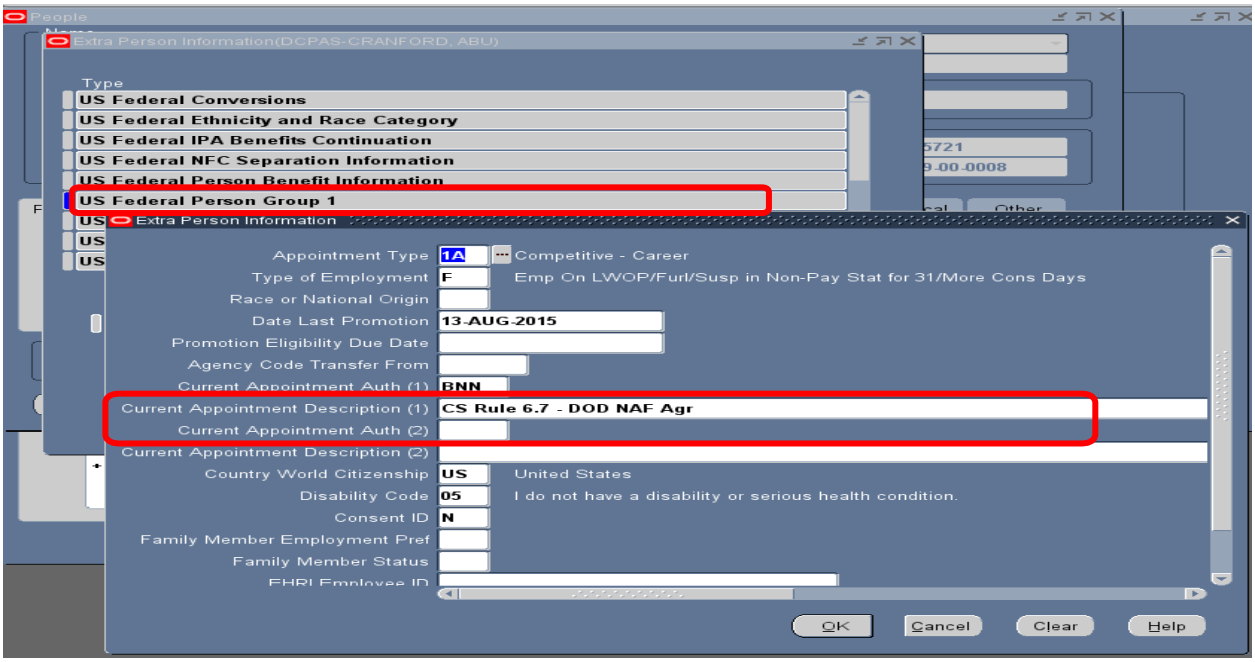


Figure 10: Current Appointment Authority (CAA) – Extra Person Information

Standard 3

Intelligence/Cyber Position Indicator

The Intelligence/Cyber Position Indicator field is used to identify personnel who are a part of the digital

civilian workforce as defined by the Framework, Cyber Excepted Service (CES) and the Defense Civilian Intelligence Personnel System (DCIPS).

Valid entries for this data element are as follows:

1 – Non-DCIPS, Non-CES, Non-Cyber Position (no DCWF work role)

2 – DCIPS (with or without DCWF work roles)

3 – CES (with or without DCWF work roles)

4 – DoD Cyber Position (Non-CES and Non-DCIPS) (with DCWF work role)

The steps necessary to navigate to these fields within DCPDS are as follows: "Position/Extra Information/US Federal Position Group 2" and are shown in Figure 11 and Figure 12.

Figure 11: Position – Extra Information

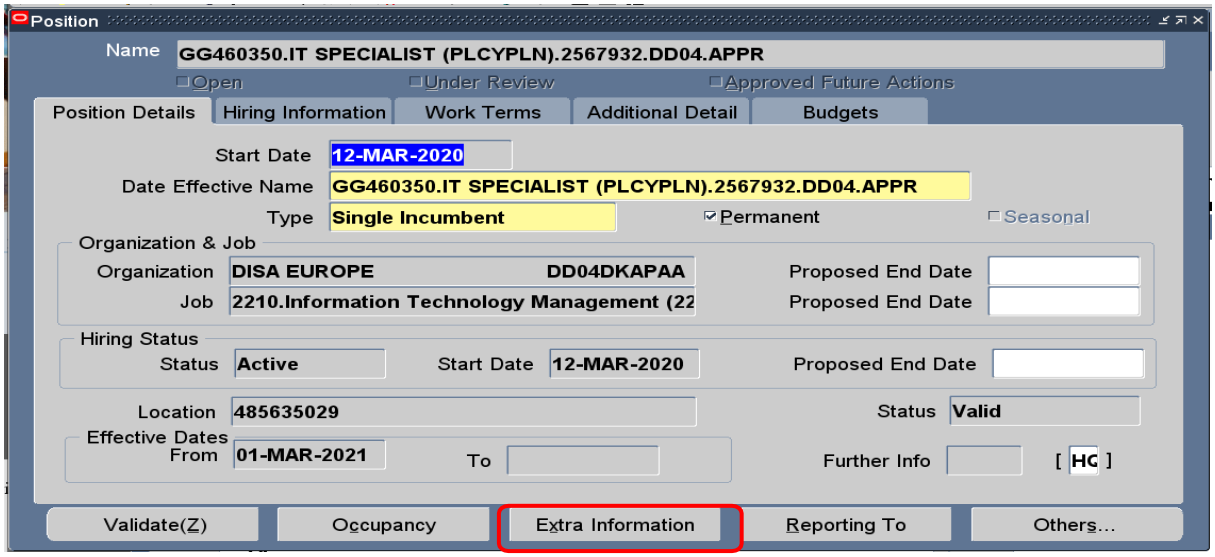
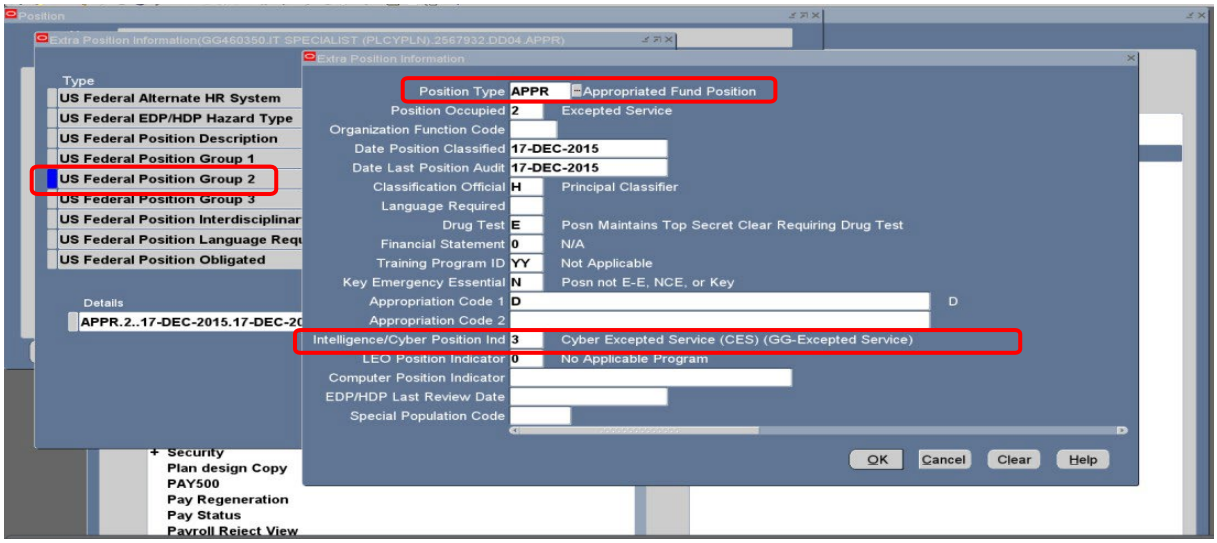


Figure 12: Intelligence/Cyber Position Indicator



VIII. Data Quality and Validation

Why it Matters

Data validation of military and civilian workforce coding is necessary to ensure the accuracy and completeness of workforce coding across the Department, to assist DoD Components with the tracking of their workforce to inform resourcing needs, and to ensure DoD is postured to submit analytics and reporting requirements. Coding compliance supports quality analytic efforts at the DoD and Component level as well as meeting Federal responsibilities.

Advana

Advana is DoD's analytics platform and data visualization tool utilized for assessing the readiness of the digital workforce, and it is leveraged to facilitate accurate workforce reporting. Advana draws from all relevant authoritative data systems, therefore validation efforts apply to Service-owned manpower and personnel systems, as well as DCPDS. With the data aggregated in Advana, DoD CIO generates comprehensive metrics to power data-driven decisions, with tailored visualizations for senior Department leadership and command-level action officers alike.

Key Principles and Activities

- To ensure accurate coding for positions, DCWF work role codes must be applied to individual position records in an applicable, authoritative manpower system of record. If a position description (PD) has more than one position assigned to it, then the work roles and proficiency levels assigned to the PD apply to all the associated positions.
    - Component managers and HR personnel should review extracts of all encumbered and vacant coded positions from manpower systems on an annual basis.
- Data element(s) and associated business logic used to link individual billets between manpower systems and personnel systems should be noted and retained for future validation efforts, including recurring data logic meetings with the DoD CIO WID Analytics team.
    - DoD CIO recommends the use of unique billet ID numbers to link records across systems, often called connecting "faces to spaces."
- As the DCWF grows and adapts, positions with work roles that have been superseded or replaced must be recoded to a valid work role.
- Once manpower coding data has been validated, DCWF work role codes and proficiency levels applied to manpower system records must also be applied to corresponding personnel records within DCPDS and DoD Component-specific personnel systems.

Getting Advice and Assistance

DoD Component cyber workforce program managers and the DoD CIO WID Analytics Branch can assist in the validation of data extracts, advise on sustaining data quality over quarterly or yearly cycles, and support efforts to synchronize data between Component manpower systems and DCPDS.

IX. Resources

DoD Component personnel should refer to *their Component's cyber functional community leads* for more specific guidance and coding information; DoD CIO provides support as indicated below:

- DoD CIO Workforce Innovation Directorate (WID) can be contacted via email at ***osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil***
- Access the User Guide for DCPDS basics at *https://media.defense.gov/2018/Sep/04/2001961439/-1/-1/1/DCPDS-PORTAL- USERS-GUIDE.PDF*
- Information on DoD 8140 policies, DCWF, Cyber Excepted Service, and more cyber workforce topics at https://www.cyber.mil/dod-workforce-innovation-directorate

X. APPENDIX A – Sample Coding Scenario

An exemption is required for recognized cyberspace occupation positions that are either uncoded or coded with a "000" primary work role. Coding exemptions are limited to a defined timeframe, typically no longer than 12 months to afford time for a position's update. If multiple positions use one position description, code each position, differentiated by individual position sequence numbers, with the same work role codes.

Scenario – Information Technology (IT) Specialist (Information Security) Position

You are a supervisor overseeing a small team and have been tasked to code all civilian positions, requiring the performance of work defined within the DCWF. Review the position's key requirements and activities to determine which work role code(s) best apply. Then review the recommended coding solution and justification following the position information.

This position requires providing recommendations and oversight for Agency Information Security programs, including certification and accreditation of the Agency's unclassified information technology (IT) systems and the implementation of programs critical to compliance with national level policies for security. Approximately 40% of the position requires the following duties:

- *Provide authoritative advice and guidance related to the Agency Information Security Program.*
- *Direct the implementation of Agency security programs designed to anticipate, assess, and minimize system vulnerabilities.*
- *Oversee the implementation of security programs across platforms and the establishment of vulnerability reporting criteria.*

Helpful Hint

Remember to review work role descriptions, knowledge, skills, abilities, and tasks (KSATs) for applicability.

Consider the "Core" versus "Additional" KSATs in the DCWF.

If position requirements and activities consistently align with "Core" KSATs of a work role, that is an indicator that the position under review should be coded with that work role.

Approximately 30% of the position requires the following duties:

- *Analyze existing, new, and emerging functional requirements of the IT Security Program and measures of effectiveness.*
- *Provide feedback on IT security plans, architecture, and initiatives supporting IT security policy. This includes, but is not limited to, budget advocacy, strategic direction, planning and deployment, and procedures and guidelines.*
- *Approve the establishment of guidelines for IT security in initial designs and lifecycle of IT systems.*

Another 30% of the position requires the following duties:

- *Develop Agency information security policies and ensure compliance with Federal laws.*
- *Resolve problems related to phases of security policy development and implementation of a variety of programs in information security.*
- *Represent Agency work groups established to develop Agency-wide IT security policy initiatives and solutions*.

Work Role Code Solution

Code this position with a primary work role code of 722 - Information Systems Security Manager (ISSM) and an Additional 1 work role code of 752 - Cyber Policy and Strategy Planner.

- This position should have a primary ISSM work role code of 722 because of the alignment between work role functions and position requirements and activities. The work role comprises the majority of the time when compiling the work indicated by the duty statements.
- This position should have an Additional 1 Cyber Policy and Strategy Planner work role code of 752 because an important focus of the position is performing IT and information security policy development, but it comprises less than a majority of the time.

Coding to the DCWF does not change or replace a position's occupational series (i.e., for this position 2210 – Information Technology Management) or other position classification factors; DCWF work roles are added to this position's information, allowing DoD to more efficiently and effectively identify and track execution of cyber work.

Duty percentages in PDs will typically not be exact in nature for constitution of work roles, therefore, the supervisor of the position is typically suited to determine the primary and additional work roles that are most representative of the work requirements for the position. The determination may involve inferences that require updates to the PD, including further analysis with managers and HR professionals.

XI. APPENDIX B – DCWF Work Roles

This appendix outlines the approved list of DCWF work role codes as of July 2025

Table B-1: DCWF Work Role Codes by Number

Work Role Code	Work Role Name
111	ALL-SOURCE ANALYST (ASA)
121	EXPLOITATION ANALYST (EA)
122	DIGITAL NETWORK EXPLOITATION ANALYST (DNEA)
131	JOINT TARGETING ANALYST (JTA)
132	TARGET DIGITAL NETWORK ANALYST (TDNA)
133	TARGET ANALYST REPORTER (TAR)
151	MULTI-DISCIPLINED LANGUAGE ANALYST
211	FORENSICS ANALYST
212	CYBER DEFENSE FORENSICS ANALYST
221	CYBER CRIME INVESTIGATOR
311	ALL-SOURCE COLLECTION MANAGER
312	ALL-SOURCE COLLECTION REQUIREMENTS MANAGER
321	ACCESS NETWORK OPERATOR
322	CYBERSPACE OPERATOR
331	CYBER INTELLIGENCE PLANNER
332	CYBER OPERATIONS PLANNER
341	CYBERSPACE CAPABILITY DEVELOPER
411	TECHNICAL SUPPORT SPECIALIST
421	DATABASE ADMINISTRATOR
422	DATA ANALYST
423	DATA SCIENTIST
424	DATA STEWARD
431	KNOWLEDGE MANAGER (KM)
441	NETWORK OPERATIONS SPECIALIST (NETOPS)
442	NETWORK TECHNICIAN
443	NETWORK ANALYST
451	SYSTEM ADMINISTRATOR (SYSADMIN)
461	SYSTEMS SECURITY ANALYST
462	CONTROL SYSTEMS SECURITY SPECIALIST
463	HOST ANALYST
511	CYBER DEFENSE ANALYST
521	CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST
531	CYBER DEFENSE INCIDENT RESPONDER
541	VULNERABILITY ASSESSMENT ANALYST
551	RED TEAM SPECIALIST
611	AUTHORIZING OFFICIAL (AO)/DESIGNATING REPRESENTATIVE
612	SECURITY CONTROL ASSESSOR (SCA)
621	SOFTWARE DEVELOPER
622	SECURE SOFTWARE ASSESSOR
623	ARTIFICIAL INTELLIGENCE/MACHINE LEARNING SPECIALIST (AI/ML)

Work Role Code	Work Role Name
624	DATA OPERATIONS SPECIALIST
625	PRODUCT DESIGNER USER INTERFACE (UI)
626	SERVICE DESIGNER USER EXPERIENCE (UX)
627	DEVELOPMENT, SECURITY, OPERATIONS (DEVSECOPS) SPECIALIST
628	SOFTWARE/CLOUD ARCHITECT
631	INFORMATION SYSTEMS SECURITY DEVELOPER
632	SYSTEMS DEVELOPER
641	SYSTEMS REQUIREMENTS PLANNER
651	ENTERPRISE ARCHITECT
652	SECURITY ARCHITECT
653	DATA ARCHITECT
661	RESEARCH & DEVELOPMENT (R&D) SPECIALIST
671	SYSTEM TESTING & EVALUATION SPECIALIST
672	AI TEST & EVALUATION SPECIALIST
673	SOFTWARE TEST & EVALUATION SPECIALIST
711	CYBER INSTRUCTIONAL & CURRICULUM DEVELOPER
712	CYBER INSTRUCTOR
722	INFORMATION SYSTEMS SECURITY MANAGER (ISSM)
723	COMMUNICATIONS SECURITY MANAGER (COMSEC)
731	CYBER LEGAL ADVISOR
732	PRIVACY COMPLIANCE MANAGER
733	AI RISK & ETHICS SPECIALIST
751	CYBER WORKFORCE DEVELOPER AND MANAGER
752	CYBER POLICY AND STRATEGY PLANNER
753	AI ADOPTION SPECIALIST
801	PROGRAM MANAGER
802	IT PROJECT MANAGER
803	PRODUCT SUPPORT MANAGER
804	IT INVESTMENT/PORTFOLIO MANAGER
805	IT PROGRAM AUDITOR
806	PRODUCT MANAGER
901	EXECUTIVE CYBER LEADERSHIP
902	AI INNOVATION LEADER
903	DATA OFFICER

Table B-2: DCWF Work Role Codes by Workforce Element

IT	Cybersecurity	Cyber Effects	Intel (Cyber)	Data/AI	Software Engr.
(411) Technical Support Specialist (421) Database Administrator (431) Knowledge Manager (KM) (441) Network Operations (NETOPS) Specialist (451) Systems Administrator (SYSADMIN) (632) Systems Developer (641) Systems Requirements Planner (651) Enterprise Architect (ENTARCH) (661) Research and Development (R&D) Specialist (671) System Testing & Evaluation (T&E) Specialist	(212) Cyber Defense Forensics Analyst (462) Control Systems Security Specialist (511) Cyber Defense Analyst (521) Cyber Defense Infrastructure Support Spec. (531) Cyber Defense Incident Responder (541) Vulnerability Assessment Analyst (611) Authorizing Official (AO) (612) Security Control Assessor (622) Secure Software Assessor (631) Info Systems Security Developer (652) Security Architect (722) ISSM (723) Comms Security (COMSEC) Mgr.	(121) Exploitation Analyst (EA) (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 (442) Network Technician (443) Network Analyst (463) Host Analyst (551) Red Team Specialist	(111) All-Source Analyst (151) Multi-Disciplined Language Analyst (311) All-Source Collection Manager (312) All-Source Collection Requirements Manager (331) Cyber Intelligence Planner	(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	(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	Leadership: (732) Privacy Compliance Mgr.; (751) Cyber Workforce Dev. & Mgr.; (752) Cyber Policy & Strategy Planner; (901) Executive Cyber Leader Legal: (211) Forensics Analyst; (221) Cyber Crime Investigator; (731) Cyber Legal Advisor Training & Ed: (711) Cyber Instructional & Curriculum Developer; (712) Cyber Instructor Acquisition: (801) Program Mgr.; (802) IT Project Mgr.; (803) Product Support Mgr.; (804) IT Investment/Portfolio Mgr.; (805) IT Program Auditor				

XII. APPENDIX C – Cyber Military Occupational Specialties

This appendix includes military occupational specialties (MOS) designated as cyber, as selected by each Service. 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.

Navy and Marine Corps have also identified recommended cyber MOS that should be reviewed for applicability of work role coding but are not mandatory. For further questions on the content of these lists, please contact your Service cyber workforce program manager.

Air Force Cyber MOS - Required

Code	Title	Personnel Category
1D711	Information Technology Systems Helper, Technical Support Specialist	Enlisted
1D731	Information Technology Systems Apprentice, Technical Support Specialist	Enlisted
1D751	Information Technology Systems Journeyman, Technical Support Specialist	Enlisted
1D771	Information Technology Systems Craftsman, Technical Support Specialist	Enlisted
1D711A	Information Technology Systems Helper, Network Operations Specialist	Enlisted
1D731A	Information Technology Systems Apprentice, Network Operations Specialist	Enlisted
1D751A	Information Technology Systems Journeyman, Network Operations Specialist	Enlisted
1D771A	Information Technology Systems Craftsman, Network Operations Specialist	Enlisted
1D711B	Information Technology Systems Helper, Systems Administration Specialist	Enlisted
1D731B	Information Technology Systems Apprentice, Systems Administration Specialist	Enlisted
1D751B	Information Technology Systems Journeyman, Systems Administration Specialist	Enlisted
1D771B	Information Technology Systems Craftsman, Systems Administration Specialist	Enlisted
1D712F	Radio Frequency and Electromagnetic Activities Helper, Spectrum Management	Enlisted
1D732F	Radio Frequency and Electromagnetic Activities Apprentice, Spectrum Management	Enlisted
1D752F	Radio Frequency and Electromagnetic Activities Journeyman, Spectrum Management	Enlisted
1D772F	Radio Frequency and Electromagnetic Activities Craftsman, Spectrum Management	Enlisted
1D712R	Radio Frequency and Electromagnetic Activities Helper, RF Transmissions	Enlisted
1D732R	Radio Frequency and Electromagnetic Activities Apprentice, RF Transmissions	Enlisted
1D752R	Radio Frequency and Electromagnetic Activities Journeyman, RF Transmissions	Enlisted
1D772R	Radio Frequency and Electromagnetic Activities Craftsman, RF Transmissions	Enlisted
1D713	Cable and Antenna Helper	Enlisted
1D733	Cable and Antenna Apprentice	Enlisted
1D753	Cable and Antenna Journeyman	Enlisted
1D773	Cable and Antenna Craftsman	Enlisted
1D714D	Data Engineering, Data Operations Specialist, Helper	Enlisted
1D734D	Data Engineering, Data Operations Specialist, Apprentice	Enlisted
1D754D	Data Engineering, Data Operations Specialist, Journeyman	Enlisted
1D774D	Data Engineering, Data Operations Specialist, Craftsman	Enlisted
1D714P	Data Engineering, Software Engineer, Helper	Enlisted
1D734P	Data Engineering, Software Engineer, Apprentice	Enlisted
1D754P	Data Engineering, Software Engineer, Journeyman	Enlisted

1D774P	Data Engineering, Software Engineer, Craftsman	Enlisted
1D715	Cybersecurity Helper	Enlisted
1D735	Cybersecurity Apprentice	Enlisted
1D755	Cybersecurity Journeyman	Enlisted
1D775	Cybersecurity Craftsman	Enlisted
1D791	Warfighter Communications, Superintendent	Enlisted
1D700	Warfighter Communications, Chief Enlisted Manager	Enlisted
1B000	Cyber Warfare Operations Manager	Enlisted
1B491	Cyber Warfare Operations Superintendent	Enlisted
1B431	Cyber Warfare Operations Apprentice	Enlisted
1B451	Cyber Warfare Operations Journeyman	Enlisted
1B471	Cyber Warfare Operations Craftsman	Enlisted
17C0	Cyberspace Warfare Operations Commander	Officer
17D1W	Warfighter Communications Operations	Officer
17D3W	Warfighter Communications Operations	Officer
17D4W	Warfighter Communications Operations	Officer
17D1WT	Warfighter Communications Operations, Technical Track	Officer
17D3WT	Warfighter Communications Operations, Technical Track	Officer
17D4WT	Warfighter Communications Operations, Technical Track	Officer
17S1A	Cyber Effects Operations, Offensive Cyberspace Operator	Officer
17S3A	Cyber Effects Operations, Offensive Cyberspace Operator	Officer
17S4A	Cyber Effects Operations, Offensive Cyberspace Operator	Officer
17S1B	Cyber Effects Operations, Defensive Cyberspace Operator	Officer
17S3B	Cyber Effects Operations, Defensive Cyberspace Operator	Officer
17S4B	Cyber Effects Operations, Defensive Cyberspace Operator	Officer
17S1AT	Cyber Effects Operations, Offensive Cyberspace Operator (Technical Track)	Officer
17S3AT	Cyber Effects Operations, Offensive Cyberspace Operator (Technical Track)	Officer
17S4AT	Cyber Effects Operations, Offensive Cyberspace Operator (Technical Track)	Officer
17S1BT	Cyber Effects Operations, Defensive Cyberspace Operator (Technical Track)	Officer
17S3BT	Cyber Effects Operations, Defensive Cyberspace Operator (Technical Track)	Officer
17S4BT	Cyber Effects Operations, Defensive Cyberspace Operator (Technical Track)	Officer
17W1C	Warfighter Communications and IT Systems Operations, Cybersecurity	Warrant Officer
17W3C	Warfighter Communications and IT Systems Operations, Cybersecurity	Warrant Officer
17W4C	Warfighter Communications and IT Systems Operations, Cybersecurity	Warrant Officer
17W1D	Warfighter Communications and IT Systems Operations, Data Operations	Warrant Officer
17W3D	Warfighter Communications and IT Systems Operations, Data Operations	Warrant Officer
17W4D	Warfighter Communications and IT Systems Operations, Data Operations	Warrant Officer
17W1I	Warfighter Communications and IT Systems Operations, Information Technology	Warrant Officer
17W3I	Warfighter Communications and IT Systems Operations, Information Technology	Warrant Officer
17W4I	Warfighter Communications and IT Systems Operations, Information Technology	Warrant Officer
17W1R	Warfighter Communications and IT Systems Operations, Radio Frequency and Electromagnetic Activities	Warrant Officer
17W3R	Warfighter Communications and IT Systems Operations, Radio Frequency and Electromagnetic Activities	Warrant Officer
17W4R	Warfighter Communications and IT Systems Operations, Radio Frequency and Electromagnetic Activities	Warrant Officer
17Y1A	Cyber Effects and Warfare Operations, Cyber Warfare Analyst	Warrant Officer
17Y3A	Cyber Effects and Warfare Operations, Cyber Warfare Analyst	Warrant Officer
17Y4A	Cyber Effects and Warfare Operations, Cyber Warfare Analyst	Warrant Officer
17Y1C	Cyber Effects and Warfare Operations, Cyber Capability Developer	Warrant Officer
17Y3C	Cyber Effects and Warfare Operations, Cyber Capability Developer	Warrant Officer

17Y4C	Cyber Effects and Warfare Operations, Cyber Capability Developer	Warrant Officer
17Y1D	Cyber Effects and Warfare Operations, Cyber Threat Defense Analyst	Warrant Officer
17Y3D	Cyber Effects and Warfare Operations, Cyber Threat Defense Analyst	Warrant Officer
17Y4D	Cyber Effects and Warfare Operations, Cyber Threat Defense Analyst	Warrant Officer
17Y1O	Cyber Effects and Warfare Operations, Cyber Attack Operator	Warrant Officer
17Y3O	Cyber Effects and Warfare Operations, Cyber Attack Operator	Warrant Officer
17Y4O	Cyber Effects and Warfare Operations, Cyber Attack Operator	Warrant Officer
17Y1I	Cyber Effects and Warfare Operations, Cyber Threat Defense Integrator	Warrant Officer
17Y3I	Cyber Effects and Warfare Operations, Cyber Threat Defense Integrator	Warrant Officer
17Y4I	Cyber Effects and Warfare Operations, Cyber Threat Defense Integrator	Warrant Officer

Army Cyber MOS - Required

Code	Title	Personnel Category
17C	Cyber Operations Specialist	Enlisted
17Z	Cyberspace and Electromagnetic Activities (CEMA) Senior Sergeant	Enlisted
25B	Information Technology Specialist	Enlisted
25D	Cyber Network Defender	Enlisted
25X	Chief Signal (NCO)	Enlisted
17A	Cyber Warfare Officer	Officer
17B	Cyber and Electronic Warfare Officer	Officer
17D	Cyber Capabilities Development Officer	Officer
25A	Signal Operations	Officer
26A	Network Systems Engineering	Officer
26B	Data Systems Engineering	Officer
26Z	Data Network Engineering	Officer
170A	Cyber Warfare Technician	Warrant Officer
170B	Electronic Warfare Technician	Warrant Officer
170D	Cyber Capabilities Developer Technician	Warrant Officer
255A	Data Operations Warrant Officer	Warrant Officer
255N	Network Operations Warrant Officer	Warrant Officer
255S	Cyberspace Defense Warrant Officer	Warrant Officer
255Z	Senior Signal Warrant Officer	Warrant Officer

Marine Corps Cyber MOS - Required Coding

These Marine Corps MOS are determined to be core cyber and require every position within the occupation to have a primary DCWF work role code and proficiency level.

Code	Military Occupation Title	Personnel Category
0631	Network Administrator	Enlisted
0639	Network Chief	Enlisted
0671	Data Systems Administrator	Enlisted
0673	Application Developer	Enlisted
0679	Data Systems Chief	Enlisted
0681	Information Security Technician	Enlisted
0691	Communications Training Instructor	Enlisted
0699	Communications Chief	Enlisted
1721	Cyber Warfare Operator (includes the following NMOSs: 1712, 1713, 1722, 1723)	Enlisted
1799	Cyber Warfare Chief	Enlisted
26XX	Signals Intelligence/Electronic Warfare/Cyberspace Operations (includes NMOSs)	Enlisted
5974	Tactical Data Systems Technician	Enlisted
6046	Maintenance Administrative Specialist	Enlisted
6694	Aviation Logistics Information Management Systems (ALIMS) Specialist	Enlisted
0602	Communications Officer	Officer
0605	Cyber Network Operations Officer	Officer
1702	Cyber Warfare Officer	Officer
1705	Cyber Warfare Development Officer	Officer
8834	Technical Information Operations Officer	Officer
8846	Data Systems Specialist	Officer
8848	Management, Data Systems Officer	Officer
8858	C4I Officer	Officer
0630	Network Engineering Officer	Warrant Officer
0640	Strategic Electromagnetic Spectrum Planning Officer	Warrant Officer
0670	Data Systems Engineering Officer	Warrant Officer
1710	Offensive Cyber Warfare Officer	Warrant Officer
1720	Defensive Cyber Warfare Officer	Warrant Officer

Marine Corps Cyber MOS - Recommend Review for Coding

These MOS should be reviewed for potential strong alignment to cyber functions and when identified as cyber require a primary DCWF work role code and proficiency level.

Code	Military Occupation Title	Personnel Category
02XX	Intelligence	Enlisted
0621	Transmissions Systems Operator	Enlisted
0627	Satellite Transmissions Systems Operator	Enlisted
0629	Transmissions Chief	Enlisted
2831	Digital Wideband Repairer	Enlisted
2841	Ground Radio Repairer	Enlisted
2847	Telephone Systems/Personal Computer Repairers	Enlisted
2862	Electronics Maintenance Technician	Enlisted
2871	Calibration Technician	Enlisted
2874	Metrology Technician	Enlisted
2887	Artillery Electronics Technician	Enlisted
2891	Electronics Maintenance Chief	Enlisted
02XX	Intelligence	Officer
1704	Electromagnetic Spectrum Operations Planner	Officer
2802	Electronics Maintenance Officer (Ground)	Officer
2805	Data/Communications Maintenance Officer	Officer
0620	Space and Waveform Integration Officer	Warrant Officer

Navy Cyber Ratings and Designators - Required

These Navy ratings and designators are determined to be core cyber and require every position within the occupation to have a primary DCWF work role code and proficiency level.

Code	Military Occupation Title	Personnel Category
CTM	Cryptologic Technician Maintenance	Enlisted
CWT	Cyber Warfare Technician	Enlisted
IT	Information Systems Technician	Enlisted
ITE	Information Systems Technician (Electronic Warfare)	Enlisted
ITN	Information Systems Technician (Network)	Enlisted
ITR	Information Systems Technician (Communications)	Enlisted
1820	Information Professional	Officer
1840	Cyber Warfare Engineer	Officer
1880	Maritime Cyber Warfare Officer	Officer
6290	Communication – Submarine (Limited Duty Officer)	Officer
6820	Information Systems (Limited Duty Officer)	Officer
7820	Information Systems Technician	Warrant Officer
7840	Cyber Warrant Officer	Warrant Officer

Navy Cyber Ratings and Designators – Recommend Review for Coding

These ratings and designators should be reviewed for potential strong alignment to cyber functions and when identified as cyber require a DCWF work role code and proficiency level.

Code	Military Occupation Title	Personnel Category
CTI	Cryptologic Technician – Interpreter (Multiple Languages)	Enlisted
CTR	Cryptologic Technician – Collection	Enlisted
EMN	Electrician's Mate, Nuclear Power	Enlisted
ETN	Electronics Technician, Nuclear Power	Enlisted
IS	Intelligence Specialist	Enlisted
MMN	Machinist's Mate, Nuclear Power	Enlisted
1810	Cryptologic Warfare	Officer
1830	Intelligence	Officer
1860	Information Warfare	Officer
6810	Cryptologic Warfare (Limited Duty Officer)	Officer
7810	Cryptologic Warfare Technician	Warrant Officer