DoD Cyber Workforce Framework (DCWF)

Military & Civilian

Workforce Identification & Coding Guide

Version 1.2
issued on July 19 2023

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

Table of Contents

I. Executive Summary

The Defense workforce operates within a warfighting domain that continues to evolve in terms of threat and complexity. Talent, and supporting workforce management practices, must then continue to evolve to address the ever-changing landscape posed by our adversaries to meet the strategic mission requirements of tomorrow.

The Department must recruit, develop, and retain a highly skilled workforce adaptable to emerging technologies and changing threat environments. Moreover, mission success and readiness is dependent on having a knowledgeable and skilled workforce with the agility to meet mission requirements. In response, the Department developed the DoD Cyber Workforce Framework (referred to in this document as "the Framework"), to provide a standardized way to describe specific work for military, civilian, and contractor personnel and support talent management activities in support of critical missions.

II. Purpose

This guide 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" and by design, ensure compliance with the Federal Cybersecurity Workforce Assessment Act (FCWAA) of 2015. It also supports use of the Office of Personnel Management memorandum "Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions," January 4, 2017. For the purposes of this guide, workforce coding is focused on the identification of positions that require the execution of ANY specific work defined within the Framework according to proficiency level.

To learn more about the DCWF, visit us on the DoD Cyber Exchange at:

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

This guide outlines workforce coding guidance and provides answers to the following questions:

1) When is coding required? How do I know when to code? *(Section 5: Workforce Coding Requirements)*

2) How do I correctly identify work roles? *(Section 6: Work Role Identification)*

   a. What are the steps for coding in the Defense Civilian Personnel Data System (DCPDS) *(Section 7: Coding in DCPDS)*

   b. What are the steps for coding within authoritative manpower systems? *(Section 4: POC for Coding Military Positions and Personnel)*

3) How can I verify my workforce is properly coded? *(Section 8: Data Validation)*

III. Historical Context

Based on formal signature and publication of the DoD 8140 Instruction, this guide includes recommendations based on 8140 policy series requirements and lessons learned from FCWAA coding activities. It expands upon and supersedes 2017 DoD Cyber Workforce Identification & Coding Guides.

The DCWF

The DCWF, is the authoritative reference for the identification, tracking, and reporting of highly skilled priority positions, serving as the Department's coding structure for authoritative manpower and personnel systems, pursuant to DoDD 8140.01. The DCWF was established in support of workforce coding and to advance DoD strategic goals focused on holistic workforce management.

Demonstrated success of the framework has resulted in directed work for its continued use and expansion beyond cyber to meet emerging mission requirements and maintain parity with industry standards. As of the date of approval for this guidance, the Framework has expanded from the 54 original work roles, increasing to a total of 71 with the inclusion of artificial intelligence (AI), Data, Analytics, Industrial Controls Systems, and Software. The Framework will continue to expand, and may serve as a model for broader science, technology, engineering, and math (STEM) work, as the Department ramps up initiatives to recruit and retain this highly specialized talent.

IV. Support Information

This guide provides instruction to DoD Components on the identification and coding of military and civilian personnel. The roles and responsibilities identified in this section detail POC that may be leveraged for additional information on workforce coding.

Workforce Coding Requirements

For questions on when coding is required and more information on when to code, please refer to Section 5 in this guide or contact the DoD CIO Workforce Innovation Directorate at *osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil.*

Work Role Identification

For questions on identification of work roles and more information on the Framework, please refer to Section 6 in this guide, visit the DCWF Tool at *https://public.cyber.mil/cw/dod-cyber-workforce-framework/*, or contact the DoD CIO Workforce Innovation Directorate at *osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil*.

Helpful Hint

HR and Functional Managers can use work roles to:

- ✓ Develop role-based job announcements and positions descriptions
- ✓ Support recruiting efforts through identification of required knowledge and skills
- ✓ Identify and track work roles of critical need for workforce planning activities

Coding Civilian Personnel in DCPDS

For questions on coding in the Defense Civilian Personnel Data System (DCPDS) and more information, please refer to Section 7 in this guide, access the User Guide for DCPDS basics at *https://media.defense.gov/2018/Sep/04/2001961439/-1/-1/1/DCPDS-PORTAL-USERS-GUIDE.PDF*, or contact the DoD CIO Workforce Innovation Directorate at *osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil*.

Data Validation

For questions on data validation and more information, please refer to Section 8 in this guide, visit *https://public.cyber.mil/cw/*, or contact the DoD CIO Workforce Innovation Directorate at osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil.

V. Workforce Coding Requirements: When is coding required?

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

- ☑ Those identified in accordance with DoDI 8140.02
- ☑ Those aligned to 0332, 0335, 1550, 2210 occupational series in accordance with the Recognized Cyberspace Occupations Memo
- ☑ All military occupational series that have been aligned to the Framework
- ☑ Those aligned to CES organizations meeting the criteria to be considered "cyber" as defined in DoDI 8140.02 (including those personnel who have and have not converted to CES)

VI. Work Role Identification

The DCWF established an authoritative lexicon based on the actual work an individual performs, rather than position title, occupational series. Work roles provide a common foundation for managing the workforce, grouped by the knowledge, skills, and abilities (KSAs) required to perform specific functions or tasks. Work roles provide the most accurate occupational descriptor, providing a higher level of specificity than traditional military occupational specialties and civilian occupational series. Work roles do not align with a specific occupation and may align with more than one occupation.

Up to three work roles may be aligned to a single position depending on the scope of position responsibilities. At a high-level, selection of one or more work roles is determined after analyzing the requirements of the position and reviewing the Framework to select the appropriate work role code(s). Specific guidance to accurately and efficiently complete coding activities is outlined in the following sections.

Selecting Work Roles

Work role codes are additional descriptors applied in conjunction with the civilian occupational series or military occupational specialty classifications. Work roles are not occupation-specific and may align to one of four identified occupational series, but is not restricted and may align to more than one not yet identified.

For example, the Systems Requirement Planner work role could apply to positions in several civilian occupational series such as 2210 IT Management, 0391 Telecommunications, 0301 Miscellaneous Administration and Program, 0343 Management and Program Analysis, 0855 Electronics Engineering, 0854 Computer Engineering, and 2003 Supply Program Management. Actual selection of one or more codes will be determined by analyzing the requirements of the position and then reviewing the Framework located at *https://public.cyber.mil/cw/dcwf/* to select the appropriate work role code(s). Appendix A provides a list of all Framework work role codes as of November 2022.

Each position that meets the criteria to be considered "cyber" as defined in DoDI 8140.02 must be assigned at least one work role code in accordance with that policy. DoD has authorized the use of up to three work role codes for each position. The first role is known as the primary work role; followed by the additional 1 and additional 2 work roles. The selection of a single work role code may provide enough information to ensure the right skill set is identified and maintained. It is not necessary to identify every task and KSA performed.

Primary & Additional Work Role Codes

The primary work role code identifies the work role that encompasses the majority of a position's responsibilities. If a primary work role code from 111-999 is used, this indicates that performance of work defined by the skillsets identified in the Framework is the primary role of the position. The secondary and tertiary codes are utilized to capture other key work required of the position. If both a primary as well as secondary and tertiary work roles) are used, the primary work role captures the most significant requirements of a given position, indicating that 50% or greater of time is spent performing duties aligned to this work role. If a position is required to complete work aligned to a specific work role though that work does not constitute the majority of work duties (<50% time spent), then the use of "000" as the primary work role and the application of a secondary and tertiary (as applicable) work role is allowed.

For each work role coded to a position, a Proficiency level must also be applied per DoD Instruction 8140.02. Valid Proficiency Levels are Basic, Intermediate and Advanced. The definitions of these Proficiency Levels are as follows:

- 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, pursuant to Paragraph 4.1.b of DoDI 8140.02.

Work Role Pairings

Some work roles pair well with other complimentary work roles. These work role pairings commonly represent specialized work roles accompanied by a specific functional or technical work role. Examples include, but are not limited to:

- Instructional Curriculum Developer paired with one or more work roles highlighting the area(s) of expertise required to develop the curriculum
- Cyber Instructor paired with one or more work roles highlighting the area(s) of expertise required to teach the coursework
- Research and Development Specialist paired with one or more areas of technical expertise
- System Testing and Evaluation Specialist paired with one or more areas of technical expertise

Table 2. Work Role Differentiation: Primary, Secondary, Tertiary

Work Role Differentiation
PRIMARY
• A primary work role is identified when the position requires performance of specific tasks as the most significant aspect of its requirements, • The selection of a primary work role code means this skill set has the highest priority for development and maintenance among all work roles assigned to the position. • If the position's primary duties do not qualify for any DCWF work role, identify this position with code "000". A secondary and tertiary (as applicable) work role must be applied in this case. • Identify the position with a primary work role code of "000" if the position's primary work is performed within another functional community (e.g., Acquisition, Financial Management), and identified tasks are performed under secondary or tertiary DCWF work roles. • 000 is not permitted for ANY civilian positions/personnel aligned to one of the four recognized occupations (2210, 1550, 0332, 0335).
Additional 1
• Assign at least one additional work role code if the primary work role designation of "000" is used as the primary work role. • Leave blank if no other work defined in the Framework is performed outside the designated primary work role code or are applicable • This field should never be coded "000."
Additional 2
• Leave blank if a tertiary role code is not applicable. • This field should never be coded "000."
A work role code may only be used once for each position (i.e., Additional 1 and Additional 2 must be unique)

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, DCWF work role coding in DCPDS should be aligned to work role coding for that encumbered position located in the respective manpower system. DoD civilians that must have DCWF work role and proficiency levels coded to their position include the following:

- Personnel identified in accordance with DoDI 8140
- Personnel aligned to 0332, 0335, 1550, 2210 occupational series in accordance with the Recognized Cyberspace Occupations Memo
- Personnel aligned to Cyber Excepted Service (CES) organizations meeting the criteria to be considered “cyber” as defined in DoDI 8140.02
- Personnel performing activities aligned to any DCWF work role

DCPDS data elements you should know:

- 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

NOTE: Cyber Program Identifier start date does not impact qualifications in accordance with DoDM 8140.

Standard 1

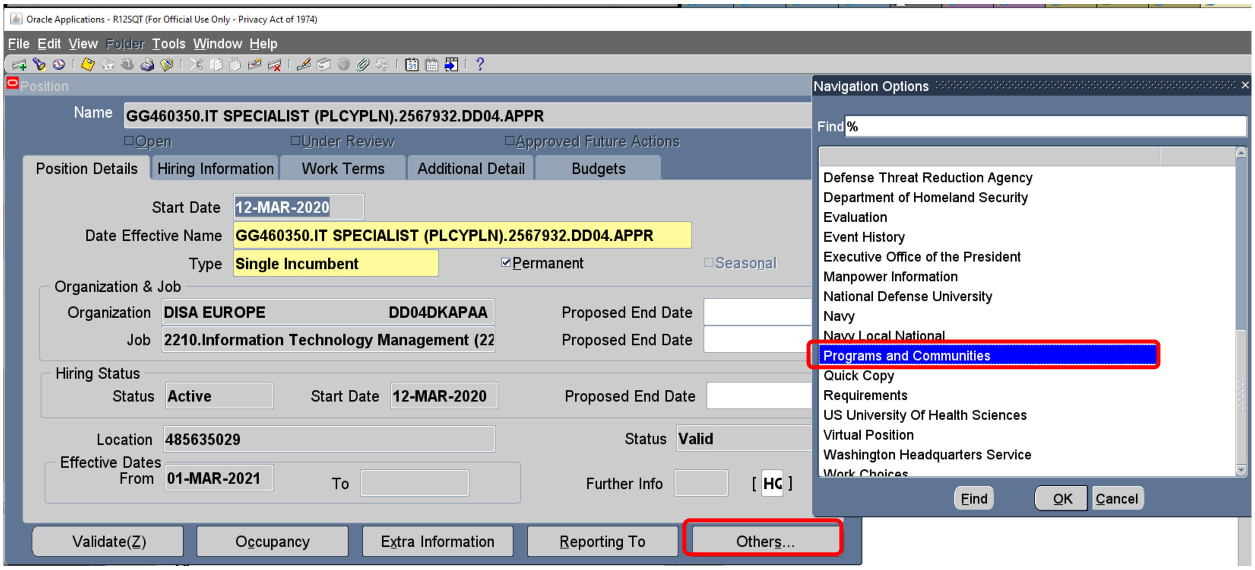
Program Unique Information Fields

DCPDS is the authoritative personnel system for the civilian workforce until the time it is superseded by the Defense Civilian Human Resources Management System (DCHRMS). The Program Unique Information Fields are designed to capture DCWF work role codes in accordance with the DoDI 8140. *These fields are **not** to be used to capture DCWF work role coding in accordance with OPM Coding Guidance as OPM does not recognize the use of “000” as a valid primary work role.*

Note: DCPDS can link to authoritative manpower systems to populate work role codes in the Program Unique Information Fields.

The steps necessary to navigate to these fields within DCPDS are as follows:

1. Position/ Other/ Programs and Communities



Name GG460350.IT SPECIALIST (PLCYPLN).2567932.DD04.APPR

□Open □Under Review □Approved Future Actions

Start Date 12-MAR-2020

Date Effective Name GG460350.IT SPECIALIST (PLCYPLN).2567932.DD04.APPR

Type Single Incumbent ☑Permanent □Seasonal

Organization & Job

Organization DISA EUROPE DD04DKAPAA Proposed End Date

Job 2210.Information Technology Management (22 Proposed End Date

Hiring Status

Status Active Start Date 12-MAR-2020 Proposed End Date

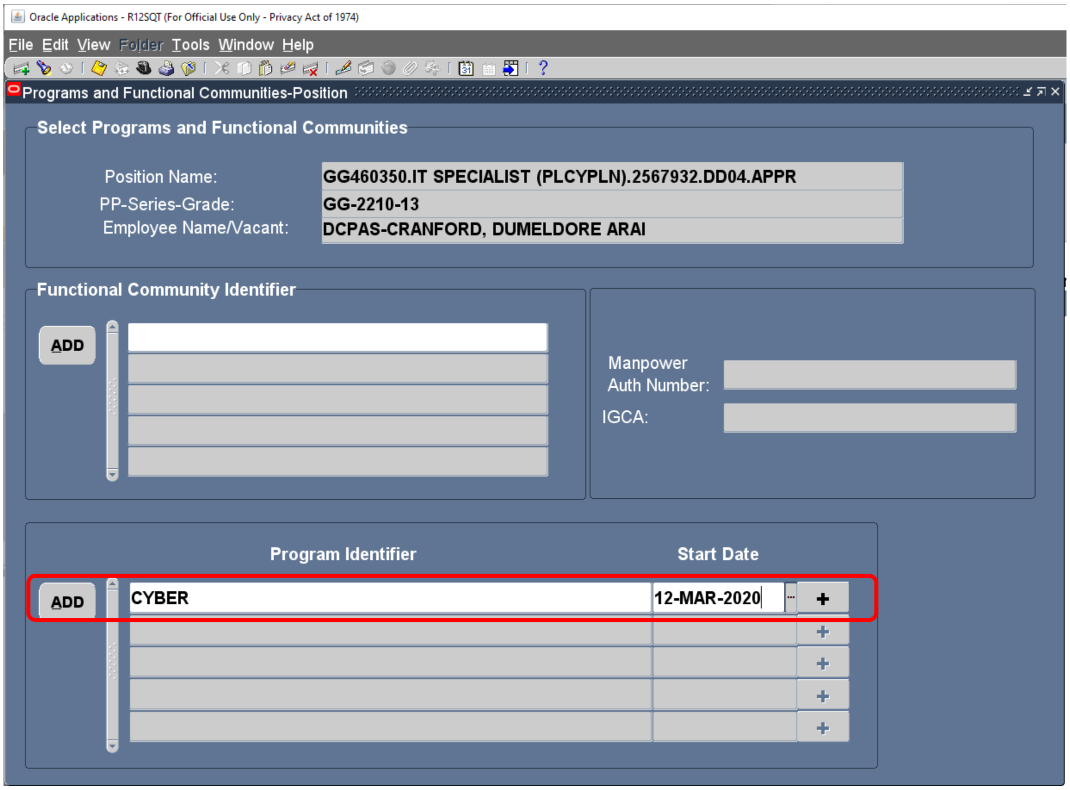
Location 485635029 Status Valid

Effective Dates From 01-MAR-2021 To Further Info [HC]

Find %

Defense Threat Reduction Agency
Department of Homeland Security
Evaluation
Event History
Executive Office of the President
Manpower Information
National Defense University
Navy
Navy Local National
Programs and Communities
Quick Copy
Requirements
US University Of Health Sciences
Virtual Position
Washington Headquarters Service
Work Choices

2. Select “Cyber” and the current date. This date solely indicates when the change was made to the personnel records and does not have any impact beyond this alternation, to include qualifications in accordance with DoDM 8140. All work roles added to the DCWF, to include Data/AI and Software, will also be available under “Cyber” until DCPDS is migrated to DCHRMS.


Oracle Applications - R12SQT (For Official Use Only - Privacy Act of 1974)
File Edit View Folder Tools Window Help
Programs and Functional Communities-Position
ADD
ADD
+
+
+
+
+

Select Programs and Functional Communities

Position Name: GG460350.IT SPECIALIST (PLCYPLN).2567932.DD04.APPR

PP-Series-Grade: GG-2210-13

Employee Name/Vacant: DCPAS-CRANFORD, DUMELDORE ARAI

Functional Community Identifier

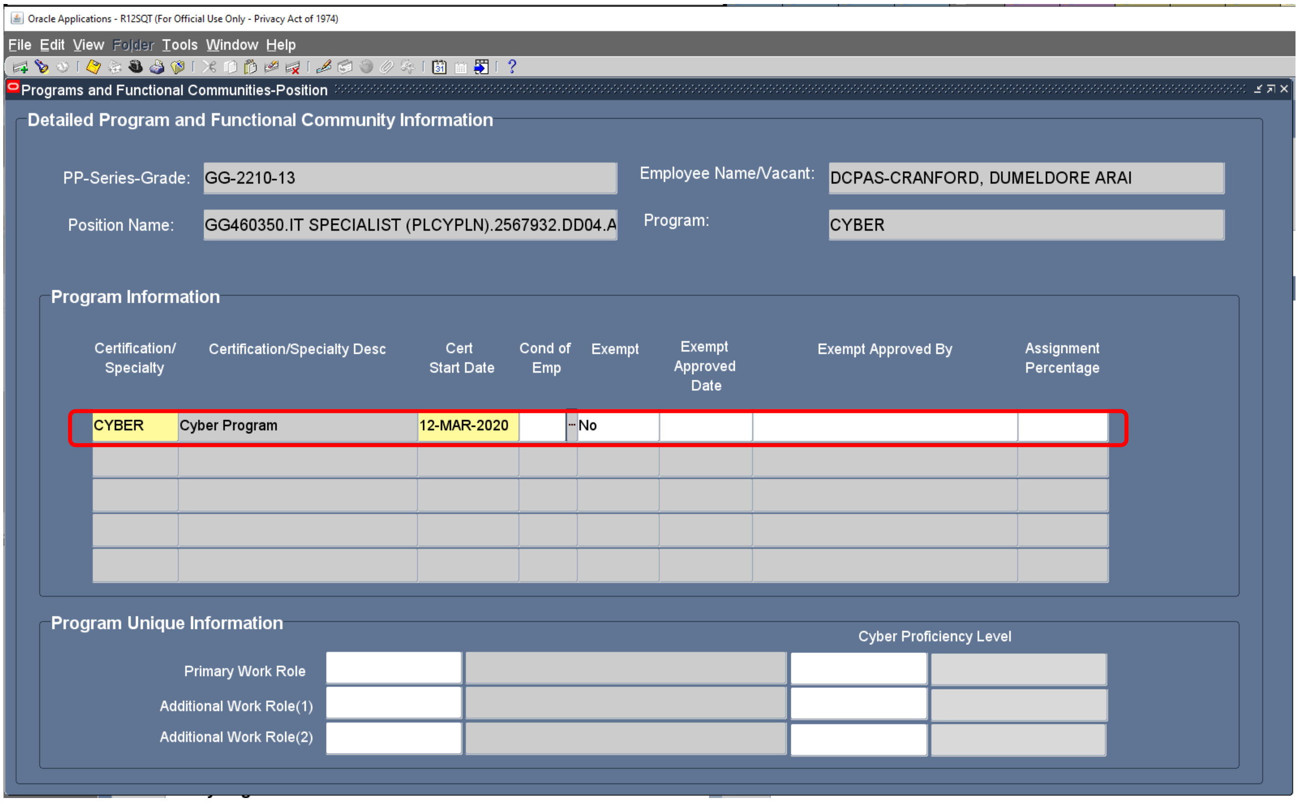
Manpower Auth Number:

IGCA:

Program Identifier	Start Date
CYBER	12-MAR-2020

3. Under Program Information, select “Cyber” then enter the same cert start date as entered previously.

Again, this date does not have an impact beyond noting the date that these DCWF work role codes were applied to this personnel record.


Oracle Applications - R12SQT (For Official Use Only - Privacy Act of 1974)
File Edit View Folder Tools Window Help

Programs and Functional Communities-Position

Detailed Program and Functional Community Information

PP-Series-Grade:	GG-2210-13	Employee Name/Vacant:	DCPAS-CRANFORD, DUMELDORE ARAI
Position Name:	GG460350.IT SPECIALIST (PLCYPLN).2567932.DD04.A	Program:	CYBER

Program Information

Certification/ Specialty	Certification/Specialty Desc	Cert Start Date	Cond of Emp	Exempt	Exempt Approved Date	Exempt Approved By	Assignment Percentage
CYBER	Cyber Program	12-MAR-2020		No			

Program Unique Information

Primary Work Role

Additional Work Role(1)

Additional Work Role(2)

Cyber Proficiency Level

4. Once the Program Information field is complete, you will be able to enter data into the Program Unique Information fields.

**This is where personnel must have DCWF work role codes and proficiency levels codes entered in accordance with DoDI 8140. Business rules to follow when entering codes are:*

Primary Work Role

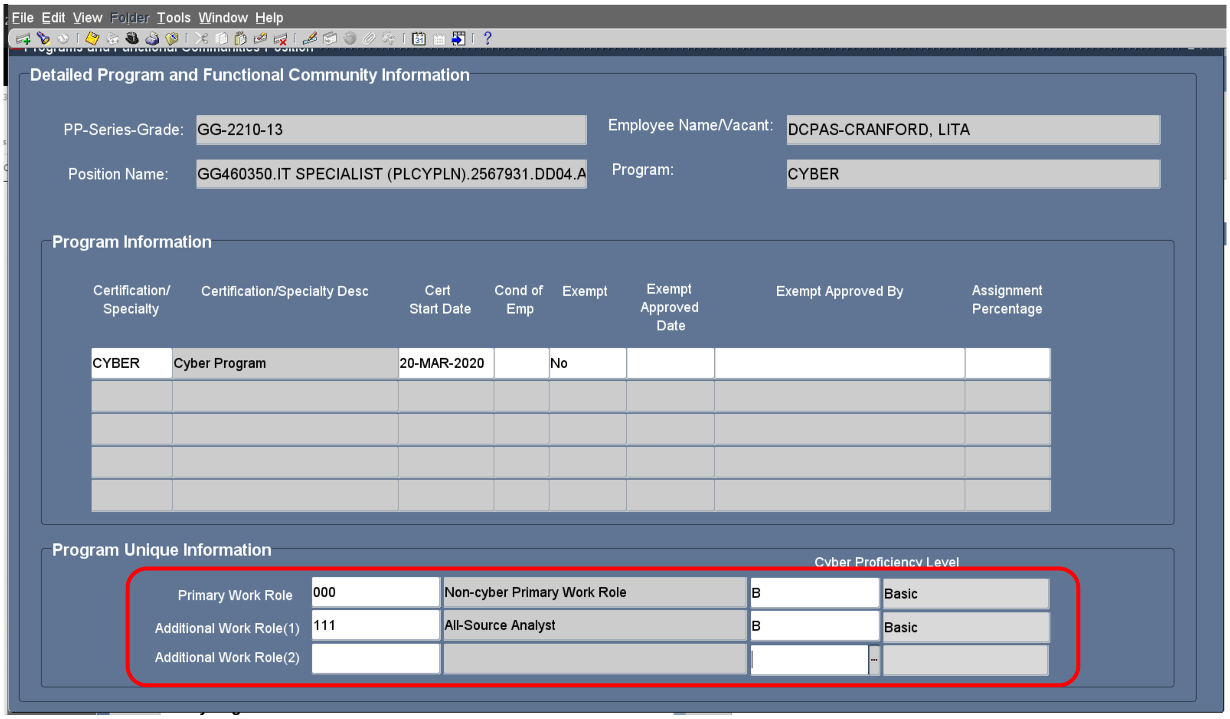
- Can be either “000” or a valid DCWF work role, such as “621”
- An associated Proficiency level must also be applied per DoDI 8140 or set as blank if “000” code is applied. Valid entries for Proficiency Levels are: B (Basic), I (Intermediate) or A (Advanced).

Secondary / Additional Work Role 1

- This field can have a valid DCWF work role code assigned or be left blank
- If the primary DCWF work role code was set as “000” then a valid DCWF work role must be assigned in the Additional 1 work role and a valid proficiency level must be assigned.

Tertiary / 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.



Detailed Program and Functional Community Information

PP-Series-Grade: GG-2210-13

Employee Name/Vacant: DCPAS-CRANFORD, LITA

Position Name: GG460350.IT SPECIALIST (PLCYPLN).2567931.DD04.A

Program: CYBER

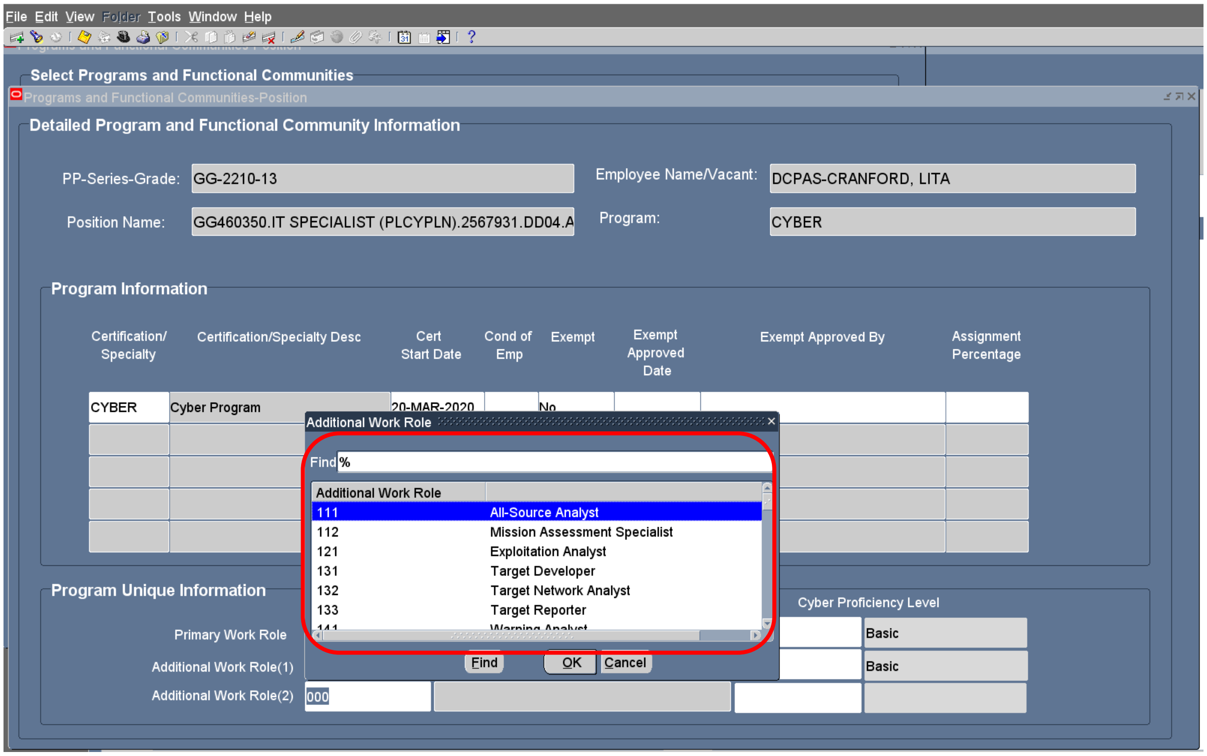
Program Information

Certification/ Specialty	Certification/Specialty Desc	Cert Start Date	Cond of Emp	Exempt	Exempt Approved Date	Exempt Approved By	Assignment Percentage
CYBER	Cyber Program	20-MAR-2020		No			

Program Unique Information

			Cyber Proficiency Level	
Primary Work Role	000	Non-cyber Primary Work Role	B	Basic
Additional Work Role(1)	111	All-Source Analyst	B	Basic
Additional Work Role(2)				

Note that a drop down is available for each work role field.


File Edit View Folder Tools Window Help
Select Programs and Functional Communities
Programs and Functional Communities-Position

Detailed Program and Functional Community Information

PP-Series-Grade: GG-2210-13

Employee Name/Vacant: DCPAS-CRANFORD, LITA

Position Name: GG460350.IT SPECIALIST (PLCYPLN).2567931.DD04.A

Program: CYBER

Program Information

Certification/ Specialty	Certification/Specialty Desc	Cert Start Date	Cond of Emp	Exempt	Exempt Approved Date	Exempt Approved By	Assignment Percentage
CYBER	Cyber Program	20-MAR-2020		No			

Additional Work Role

Find %

Additional Work Role	
111	All-Source Analyst
112	Mission Assessment Specialist
121	Exploitation Analyst
131	Target Developer
132	Target Network Analyst
133	Target Reporter
141	Warning Analyst

Program Unique Information

			Cyber Proficiency Level	
Primary Work Role				Basic
Additional Work Role(1)				Basic
Additional Work Role(2)	000			

Standard 2

Current Appointment Authority

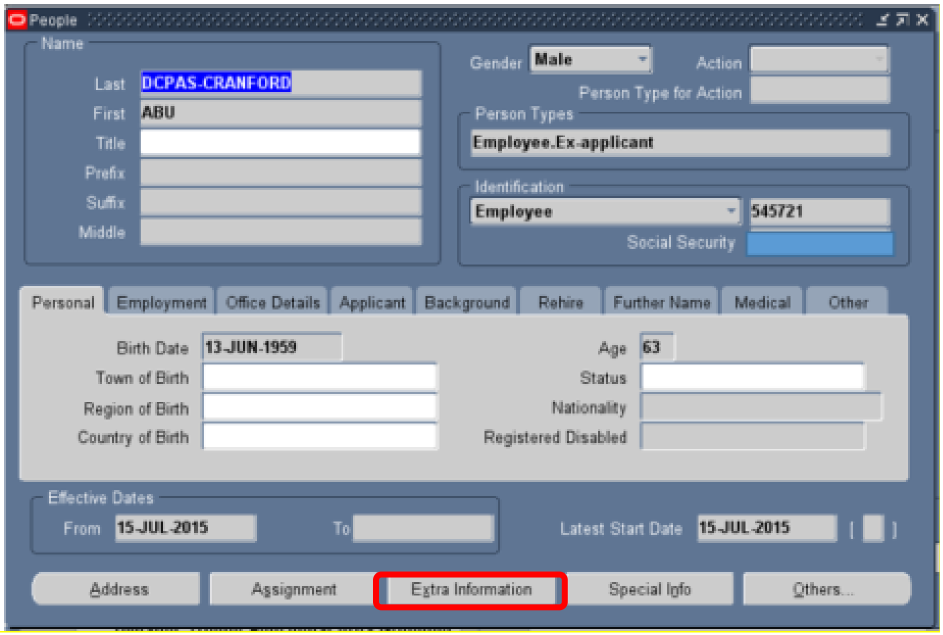
Current Appointment Authority (CAA) – As defined by OPM, CAA is “The law, executive order, rule, regulation, or other basis that, in addition to CURRENT APPOINTMENT AUTHORITY (1), authorizes an employee's most recent conversion or accession action.”

- The relevant CAA values for the purpose of this data remediation is:
  - UKM – This value indicates a personnel conversion into the Cyber Excepted Service personnel system.
  - UAM – This value indicates a personnel conversion into the Defense Civilian Intelligence Personnel System.

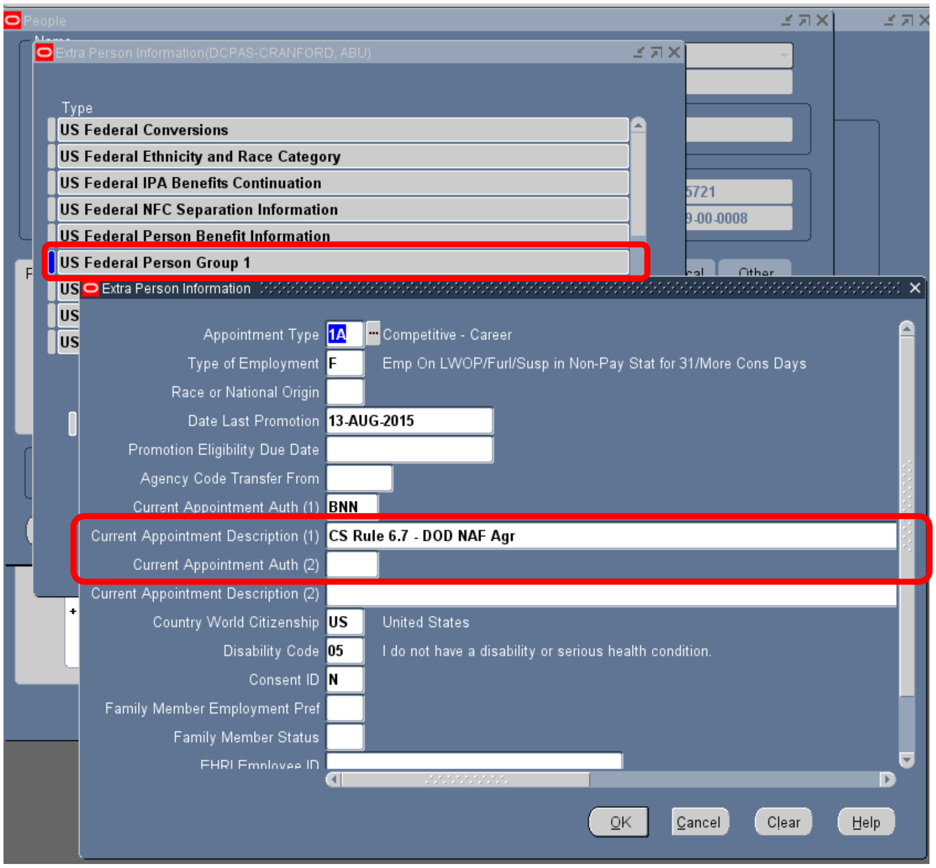
Note: These CAAs are listed as they correspond to Title 10 personnel systems that frequently utilize the DCWF. There are additional CAAs maintained by OPM, further information can be found here: *https://dw.opm.gov/datastandards/referenceData/caa/1428/current?index=C*

Within DCPDS, you can navigate to the CAA page for a given position by following these steps:

- People/Extra Information/US Federal Person Group 1/ Current Appointment Authority



Last: DCPAS-CRANFORD
First: ABU
Gender: Male
Person Types: Employee.Ex-applicant
Identification: Employee 545721
Birth Date: 13-JUN-1959
Age: 63
Effective Dates From: 15-JUL-2015
Latest Start Date: 15-JUL-2015



Type

- US Federal Conversions
- US Federal Ethnicity and Race Category
- US Federal IPA Benefits Continuation
- US Federal NFC Separation Information
- US Federal Person Benefit Information
- US Federal Person Group 1

Extra Person Information

Appointment Type	1A	Competitive - Career
Type of Employment	F	Emp On LWOP/Furl/Susp in Non-Pay Stat for 31/More Cons Days
Race or National Origin		
Date Last Promotion	13-AUG-2015	
Promotion Eligibility Due Date		
Agency Code Transfer From		
Current Appointment Auth (1)	BNN	
Current Appointment Description (1)	CS Rule 6.7 - DOD NAF Agr	
Current Appointment Auth (2)		
Current Appointment Description (2)		
Country World Citizenship	US	United States
Disability Code	05	I do not have a disability or serious health condition.
Consent ID	N	
Family Member Employment Pref		
Family Member Status		
EHRI Employee ID		

Standard 3

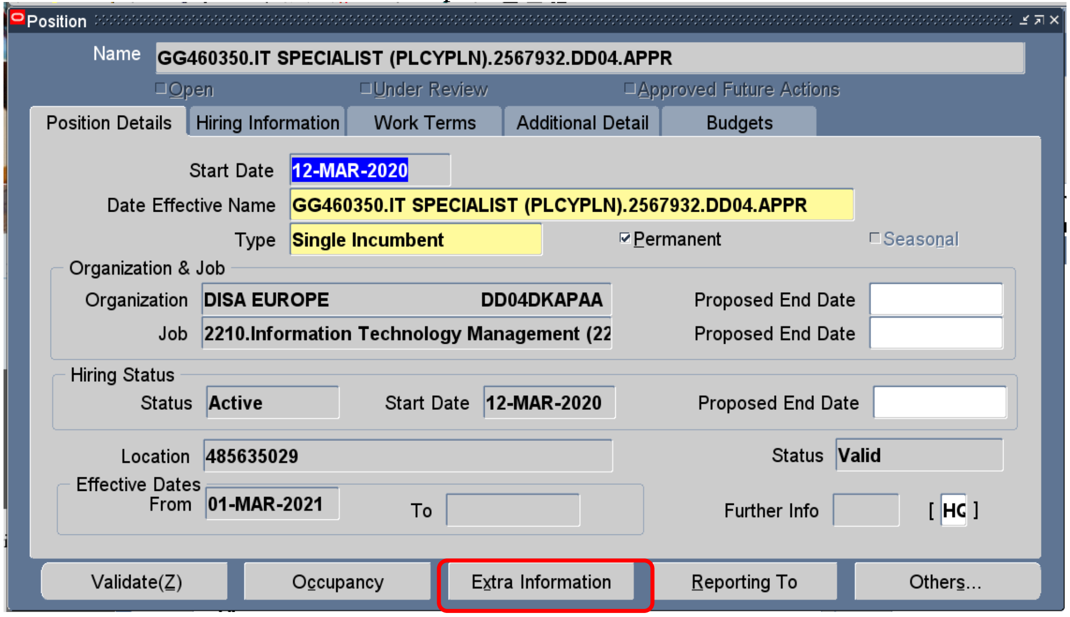
Intelligence/Cyber Position Indicator

The Intelligence/Cyber Position Indicator field is used to identify those personnel who are a part of the larger civilian workforce defined within 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
- 2 - Defense Civilian Intelligence Personnel System (DCIPS)
- 3 - Cyber Excepted Service (CES)
- 4 - DoD Cyber (Non- CES and Non- DCIPS)

The steps necessary to navigate to these fields within DCPDS are as follows:
Position/Extra Information/US Federal Position Group 2



Position

Name GG460350.IT SPECIALIST (PLCYPLN).2567932.DD04.APPR

□Open □Under Review □Approved Future Actions

Start Date 12-MAR-2020

Date Effective Name GG460350.IT SPECIALIST (PLCYPLN).2567932.DD04.APPR

Type Single Incumbent ☑Permanent □Seasonal

Organization & Job

Organization DISA EUROPE DD04DKAPAA Proposed End Date

Job 2210.Information Technology Management (22 Proposed End Date

Hiring Status

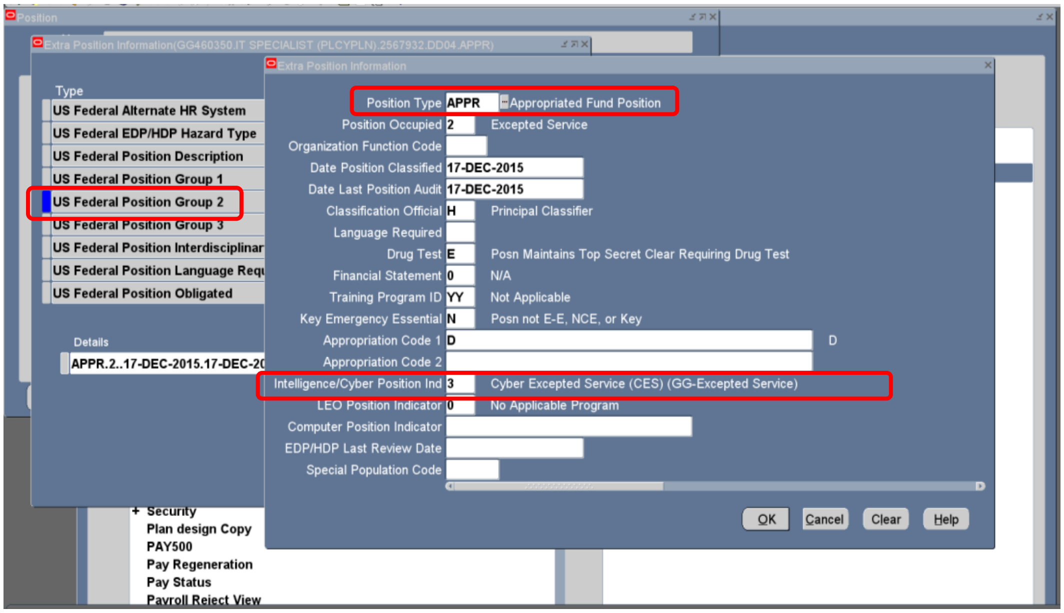
Status Active Start Date 12-MAR-2020 Proposed End Date

Location 485635029 Status Valid

Effective Dates

From 01-MAR-2021 To

Further Info [HC]



Position

Extra Position Information(GG460350.IT SPECIALIST (PLCYPLN).2567932.DD04.APPR)

Type
US Federal Alternate HR System
US Federal EDP/HDP Hazard Type
US Federal Position Description
US Federal Position Group 1
US Federal Position Group 2
US Federal Position Group 3
US Federal Position Interdisciplinar
US Federal Position Language Requ
US Federal Position Obligated

Details
APPR.2..17-DEC-2015.17-DEC-20

Extra Position Information

Position Type APPR Appropriated Fund Position
Position Occupied 2 Excepted Service
Organization Function Code
Date Position Classified 17-DEC-2015
Date Last Position Audit 17-DEC-2015
Classification Official H Principal Classifier
Language Required
Drug Test E Posn Maintains Top Secret Clear Requiring Drug Test
Financial Statement 0 N/A
Training Program ID YY Not Applicable
Key Emergency Essential N Posn not E-E, NCE, or Key
Appropriation Code 1 D D
Appropriation Code 2
Intelligence/Cyber Position Ind 3 Cyber Excepted Service (CES) (GG-Excepted Service)
LEO Position Indicator 0 No Applicable Program
Computer Position Indicator
EDP/HDP Last Review Date
Special Population Code

VIII. Data Validation

Data validation of military and civilian workforce coding is necessary to ensure the accuracy and completeness of coding across the Department, to assist the Services with the tracking of their workforce to inform resourcing needs, and to ensure DoD is postured to complete reporting and analytics efforts. Coding compliance supports higher quality analytic efforts at the Department, Service, and Component level and helps to ensure Advana is positioned to accurately report on the workforce. Validation efforts apply to Service and Component owned manpower and personnel systems as well as DCPDS. To ensure accurate coding down to the work role level, the following steps must be completed.

Process

- On a regular basis, HR Personnel and functional managers will identify and review positions and personnel engaged in DCWF work role activities in accordance with DoDI 8140. Review will determine appropriate DCWF work role codes and 8140 Proficiency Levels that will then be applied to individual position records in applicable manpower system of record.
    - All civilian positions aligned to the following occupational series must be coded in accordance with 2022 Recognized Cyberspace Occupations Memo: 0332 Computer Operations, 0335 Computer Clerk, 1550 Computer Science and 2210 Information Technology Management. There will be positions and personnel outside of these 4 occupational series that must be considered for this validation effort. If there are positions that are not currently coded but meet the criteria established in DoDI 8140, then DCWF work role codes and proficiency levels must be applied.
    - All military and civilian positions and personnel aligned to Cyber Excepted Service (CES) organizations meeting the criteria to be considered “cyber” as defined in DoDI 8140.02 must be coded with appropriate DCWF work roles and proficiency levels.
- HR Personnel and functional managers should review an exhaustive extract of all encumbered and vacant coded positions from manpower system on an interim basis. Minimum recommended data elements in extract should include:
    - Component
    - UIC
    - PAS (Air Force only)
    - Agency Group Description
    - Billet unique identifier (data element must enable linkage from manpower system to DCPDS or Service owned personnel system)
    - Occupational Series
    - Grade
    - Encumbered/Vacant Status
    - Primary, Additional 1, and Additional 2 work roles as applicable
    - Basic, Intermediate, and Advanced Proficiency Levels as applicable
    - Has position converted to Cyber Excepted Service (CES)? (Yes/No)
  - Data element(s) and associated business logic used to link individual billets from manpower system to DCPDS should be noted and retained for future validation efforts.
- Extracts can be coordinated with DoD CIO WID Actions Officers to assist with validating data for completeness and compliance with guidance.
- Once manpower coding data has been validated, DCWF work role codes and proficiency levels applied to manpower system records must be applied to corresponding personnel records within DCPDS or Service specific personnel system.

- Personnel that have converted to Cyber Excepted Service (CES) are identified in DCPDS using the Intelligence/Cyber Position Indicator and Current Appointment Authority Fields in accordance with DoD CIO Data Standards.
- A Service or Component POC should review the extracts from manpower systems and DCPDS to ensure that DCWF work roles codes and proficiency levels are consistent for individual records between each system, and that coding is completed in accordance with DoD Guidance. DoD CIO WID Action Officers will be able to assist with this validation.

Data Validation Goals

- All civilian positions and personnel engaged in cyberspace activities are reviewed and accurately coded with DCWF work role codes and 8140 proficiency level codes.
- DCWF work role codes and 8140 proficiency levels are synchronized between Service owned manpower systems and DCPDS.
- All personnel aligned to CES organizations are identified using the Current Appointment Authority and Intelligence/Cyber Position Indicator Fields in DCPDS.
- Services and Components will provide CIO AO with course of action to carry on the sustainment of DCWF coding validation and synchronization between manpower systems and DCPDS.

APPENDIX A – DCWF Work Roles

This appendix outlines the current list of DCWF work role codes as of November 2022

Table 3: DCWF Work Role Codes

DCWF Work Role Code	DCWF Work Role Name
000	NON CYBER PRIMARY WORK ROLE
111	ALL-SOURCE ANALYST
112	MISSION ASSESSMENT SPECIALIST
121	EXPLOITATION ANALYST
131	TARGET DEVELOPER
132	TARGET NETWORK ANALYST
133	TARGET REPORTER
141	WARNING ANALYST
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	INTERACTIVE OPERATOR
331	CYBER INTELLIGENCE PLANNER
332	CYBER OPERATIONS PLANNER
333	PARTNER INTEGRATION PLANNER
411	TECHNICAL SUPPORT SPECIALIST
421	DATABASE ADMINISTRATOR
422	DATA ANALYST
423	DATA SCIENTIST
424	DATA STEWARD
431	KNOWLEDGE MANAGER
441	NETWORK OPERATIONS SPECIALIST
451	SYSTEM ADMINISTRATOR
461	SYSTEMS SECURITY ANALYST
462	CONTROL SYSTEMS SECURITY SPECIALIST
511	CYBER DEFENSE ANALYST
521	CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST
531	CYBER DEFENSE INCIDENT RESPONDER
541	VULNERABILITY ASSESSMENT ANALYST
611	AUTHORIZING OFFICIAL/DESIGNATING REPRESENTATIVE
612	SECURITY CONTROL ASSESSOR
621	SOFTWARE DEVELOPER

622	SECURE SOFTWARE ASSESSOR
623	AT/ML SPECIALIST
624	DATA OPERATIONS SPECIALIST
625	Product Designer User Interface (UI)
626	Service Designer User Experience (UX)
627	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 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
723	COMSEC MANAGER
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

APPENDIX B – Civilian Occupational Series

The Cyber Workforce Advisory Group (CWAG) general membership and the Cyber Workforce Management Board (CWMB) general membership have agreed upon 2210 Information Technology (IT) Management, 1550 Computer Science, 0332 Computer Operations, and 0335 Computer Clerk and Assistant occupational series to be the recognized cyberspace occupations that must be coded under the 8140 Policy Series. On July 26, 2022, the DoD CIO, on behalf of the CWMB Tri-Chairs, formally approved these four occupational series as the recognized occupations that must be coded under the 8140 Policy Series and aligned to the Framework.

Per the Formal approval of the Recognized Cyberspace Occupations Memo, all positions aligned to the 2210, 1550, 0332 and 0335 occupational series must be coded with DCWF work roles.

NOTE: This business logic is not currently built into DCPDS and must be manually certified by personnel applying DCWF work roles and associated proficiency levels.

Table 4. Civilian Occupations Identified

Occupation Series	
2210	Information Technology (IT) Management
1550	Computer Science
0332	Computer Operations
0335	Computer Clerk and Assistant

APPENDIX C – Military Occupational Specialties

This appendix includes military occupations related to positions and personnel aligned to the Framework sourced from DoD COOL, which can be found at *https://www.cool.osd.mil/research-military-occupations.htm.* For the purposes of this coding guidance, DCWF coding should not be limited to the below military occupations. Table 5 is provided only as an example of the military occupations resulting from a query of "cyber".

To identify occupational specialties the complete military occupation crosswalk is available for download here: *https://www.onetcenter.org/dl_files/2019/military_crosswalk.zip*

Table 5: Military Occupation Specialties

Occupation Code	Occupation Title	Personnel Category
	Air Force	
1D711	Cyber Defense Operations Helper	Enlisted
1D731	Cyber Defense Operations Apprentice	Enlisted
1D731A	Cyber Defense Operations Apprentice, Networks Operations	Enlisted
1D731B	Cyber Defense Operations Apprentice, Systems Operations	Enlisted
1D751	Cyber Defense Operations Journeyman	Enlisted
1D751A	Cyber Defense Operations Journeyman, Networks Operations	Enlisted
1D751B	Cyber Defense Operations Journeyman, Systems Operations	Enlisted
1D771	Cyber Defense Operations Craftsman	Enlisted
1D771A	Cyber Defense Operations Craftsman, Networks Operations	Enlisted
1D771B	Cyber Defense Operations Craftsman, Systems Operations	Enlisted
17D1Y	Warfighter Communications Operations, Special Operations CSO (if Prefix N)	Officer
17D1Y	Warfighter Communications Operations, General	Officer
17D2S	Warfighter Communications Operations, Tanker (if Prefix N)	Officer
17D3S	Warfighter Communications Operations, Tanker (if Prefix N)	Officer
17D4S	Warfighter Communications Operations, Tanker (if Prefix N)	Officer
17S1Y	Cyberspace Effects Operations, Special Operations (if Prefix Nor P)	Officer
17S1Z	Cyberspace Effects Operations , C2ISREW	Officer
17S1S	Cyberspace Effects Operations, Software Development	Officer
17S2S	Cyberspace Effects Operations, Software Development	Officer
17S3S	Cyberspace Effects Operations, Software Development	Officer
17S4S	Cyberspace Effects Operations, Software Development	Officer
17S2Y	Cyberspace Effects Operations, Special Operations (if Prefix N or P)	Officer
17S3Y	Cyberspace Effects Operations, Special Operations (if Prefix N or P)	Officer
17S4Y	Cyberspace Effects Operations, Special Operations (if Prefix N or P)	Officer
17S2Z	Cyberspace Effects Operations , C2ISREW (if Prefix N or P)	Officer
17S3Z	Cyberspace Effects Operations , C2ISREW (if Prefix N or P)	Officer
17S4Z	Cyberspace Effects Operations , C2ISREW (if Prefix N or P)	Officer
1D700	Cyber Defense Operations Manager	Enlisted
1D791	Cyber Defense Operations Superintendent	Enlisted
1D731R	Cyber Defense Operations Apprentice, RF Operations	Enlisted

1D731Z	Cyber Defense Operations Apprentice, Software Development Operations	Enlisted
1D751R	Cyber Defense Operations Journeyman, RF Operations	Enlisted
1D751Z	Cyber Defense Operations Journeyman, Software Development Operations	Enlisted
1D771R	Cyber Defense Operations Craftsman, RF Operations	Enlisted
1D771Z	Cyber Defense Operations Craftsman, Software Development Operations	Enlisted
3D032	Cyber Systems Operations Apprentice	Enlisted
3D052	Cyber Systems Operations Journeyman	Enlisted
3D072	Cyber Systems Operations Craftsman	Enlisted
3D033	Cyber Surety Apprentice	Enlisted
3D053	Cyber Surety Journeyman	Enlisted
3D073	Cyber Surety Craftsman	Enlisted
17C0	Cyberspace Warfare Operations Commander	Officer
17D1A	Warfighter Communications Operations, Network Operations	Officer
17D3A	Warfighter Communications Operations, Network Operations	Officer
17D4A	Warfighter Communications Operations, Network Operations	Officer
17D1B	Warfighter Communications Operations, Expeditionary Communications Operations	Officer
17D3B	Warfighter Communications Operations, Expeditionary Communications Operations	Officer
17D4B	Warfighter Communications Operations, Expeditionary Communications Operations	Officer
17D1M	Warfighter Communications Operations, RPA	Officer
17D1N	Warfighter Communications Operations, ABM	Officer
17D1P	Warfighter Communications Operations, Fighter	Officer
17D1Q	Warfighter Communications Operations, Trainer	Officer
17D1R	Warfighter Communications Operations, Bomber	Officer
17D1T	Warfighter Communications Operations, Airlift	Officer
17D1V	Warfighter Communications Operations, Helicopter or EWO	Officer
17D1W	Warfighter Communications Operations, General CSO	Officer
17D3M	Warfighter Communications Operations, RPA	Officer
17D3N	Warfighter Communications Operations, ABM	Officer
17D3P	Warfighter Communications Operations, Fighter	Officer
17D3Q	Warfighter Communications Operations, Trainer	Officer
17D3R	Warfighter Communications Operations, Bomber	Officer
17D3S	Warfighter Communications Operations, Software Development	Officer
17D3T	Warfighter Communications Operations, Airlift	Officer
17D3V	Warfighter Communications Operations, Helicopter or EWO	Officer
17D3W	Warfighter Communications Operations, General CSO	Officer
17D3Y	Warfighter Communications Operations, Special Operations CSO (if Prefix N)	Officer
17D4M	Warfighter Communications Operations, RPA	Officer
17D4N	Warfighter Communications Operations, ABM	Officer
17D4P	Warfighter Communications Operations, Fighter	Officer
17D4Q	Warfighter Communications Operations, Trainer	Officer
17D4R	Warfighter Communications Operations, Bomber	Officer
17D4S	Warfighter Communications Operations, Software Development	Officer

17D4T	Warfighter Communications Operations, Airlift	Officer
17D4V	Warfighter Communications Operations, Helicopter or EWO	Officer
17D4W	Warfighter Communications Operations, General CSO	Officer
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
17D2A	Warfighter Communications Operations, Network Operations	Officer
17D2B	Warfighter Communications Operations, Expeditionary Communications Operations	Officer
17D2M	Warfighter Communications Operations, RPA	Officer
17D2N	Warfighter Communications Operations, ABM	Officer
17D2P	Warfighter Communications Operations, Fighter	Officer
17D2Q	Warfighter Communications Operations, Trainer	Officer
17D2R	Warfighter Communications Operations, Bomber	Officer
17D2S	Warfighter Communications Operations, Software Development	Officer
17D2T	Warfighter Communications Operations, Airlift	Officer
17D2V	Warfighter Communications Operations, Helicopter or EWO	Officer
17D2W	Warfighter Communications Operations, General CSO	Officer
17D3Z	Warfighter Communications Operations, C2ISREW CSO	Officer
17S4B	Cyberspace Effects Operations, Defensive Cyberspace Operator	Officer
17S4M	Cyberspace Effects Operations, RPA	Officer
17S4N	Cyberspace Effects Operations, ABM	Officer
17S4P	Cyberspace Effects Operations, Fighter	Officer
17S4Q	Cyberspace Effects Operations, Trainer	Officer
17S4R	Cyberspace Effects Operations, Bomber	Officer
17S4S	Cyberspace Effects Operations, Tanker (if Prefix N or P)	Officer
17S4T	Cyberspace Effects Operations, Airlift	Officer
17S4V	Cyberspace Effects Operations, Helicopter or EWO	Officer
17S4W	Cyberspace Effects Operations, General (if Prefix N or P)	Officer
17S4C	Cyberspace Effects Operations, Capabilities Development	Officer
17S2A	Cyberspace Effects Operations, Offensive Cyberspace Operator	Officer
17S2B	Cyberspace Effects Operations, Defensive Cyberspace Operator	Officer
17S2M	Cyberspace Effects Operations, RPA	Officer
17S2N	Cyberspace Effects Operations, ABM	Officer
17S2P	Cyberspace Effects Operations, Fighter	Officer
17S2Q	Cyberspace Effects Operations, Trainer	Officer
17S2R	Cyberspace Effects Operations, Bomber	Officer
17S2S	Cyberspace Effects Operations, Tanker (if Prefix N or P)	Officer
17S2T	Cyberspace Effects Operations, Airlift	Officer
17S2V	Cyberspace Effects Operations, Helicopter or EWO	Officer
17S2W	Cyberspace Effects Operations, General (if Prefix N or P)	Officer

17S2Y	Cyberspace Effects Operations, General	Officer
17S1Y	Cyberspace Effects Operations, General	Officer
17S3Y	Cyberspace Effects Operations, General	Officer
17S4Y	Cyberspace Effects Operations, General	Officer
17S1A	Cyberspace Effects Operations, Offensive Cyberspace Operator	Officer
17S1B	Cyberspace Effects Operations, Defensive Cyberspace Operator	Officer
17S1M	Cyberspace Effects Operations, RPA	Officer
17S1N	Cyberspace Effects Operations, ABM	Officer
17S1P	Cyberspace Effects Operations, Fighter	Officer
17S1Q	Cyberspace Effects Operations, Trainer	Officer
17S1R	Cyberspace Effects Operations, Bomber	Officer
17S1S	Cyberspace Effects Operations, Tanker (if Prefix N or P)	Officer
17S1T	Cyberspace Effects Operations, Airlift	Officer
17S1V	Cyberspace Effects Operations, Helicopter or EWO	Officer
17S1W	Cyberspace Effects Operations, General (if Prefix N or P)	Officer
17S3A	Cyberspace Effects Operations, Offensive Cyberspace Operator	Officer
17S3B	Cyberspace Effects Operations, Defensive Cyberspace Operator	Officer
17S3M	Cyberspace Effects Operations, RPA	Officer
17S3N	Cyberspace Effects Operations, ABM	Officer
17S3P	Cyberspace Effects Operations, Fighter	Officer
17S3Q	Cyberspace Effects Operations, Trainer	Officer
17S3R	Cyberspace Effects Operations, Bomber	Officer
17S3S	Cyberspace Effects Operations, Tanker (if Prefix N or P)	Officer
17S3T	Cyberspace Effects Operations, Airlift	Officer
17S3V	Cyberspace Effects Operations, Helicopter or EWO	Officer
17S3W	Cyberspace Effects Operations, General (if Prefix N or P)	Officer
17S4A	Cyberspace Effects Operations, Offensive Cyberspace Operator	Officer
17S3C	Cyberspace Effects Operations, Capabilities Development	Officer
17S2C	Cyberspace Effects Operations, Capabilities Development	Officer
17S1C	Cyberspace Effects Operations, Capabilities Development	Officer
17D4C	Warfighter Communications Operations, Capabilities Development	Officer
17D3C	Warfighter Communications Operations, Capabilities Development	Officer
17D2C	Warfighter Communications Operations, Capabilities Development	Officer
17D1C	Warfighter Communications Operations, Capabilities Development	Officer
17D2Y	Warfighter Communications Operations, Special Operations CSO (if Prefix N)	Officer
17D2Y	Warfighter Communications Operations, General	Officer
17D2Z	Warfighter Communications Operations, C2ISREW CSO	Officer
17D3Y	Warfighter Communications Operations, General	Officer
17D4Y	Warfighter Communications Operations, General	Officer
17D4Z	Warfighter Communications Operations, C2ISREW CSO	Officer
17D1Z	Warfighter Communications Operations, C2ISREW CSO	Officer
17D4Y	Warfighter Communications Operations, Special Operations CSO (if Prefix N)	Officer

1D731D	Cyber Defense Operations Apprentice, Security Operations	Enlisted
1D731E	Cyber Defense Operations Apprentice, Client Systems Operations	Enlisted
1D731K	Cyber Defense Operations Apprentice, Knowledge Operations	Enlisted
1D751D	Cyber Defense Operations Journeyman, Security Operations	Enlisted
1D751E	Cyber Defense Operations Journeyman, Client Systems Operations	Enlisted
1D751K	Cyber Defense Operations Journeyman, Knowledge Operations	Enlisted
1D771D	Cyber Defense Operations Craftsman, Security Operations	Enlisted
1D771E	Cyber Defense Operations Craftsman, Client Systems Operations	Enlisted
1D771K	Cyber Defense Operations Craftsman, Knowledge Operations	Enlisted
1D732	Spectrum Defense Operations Apprentice	Enlisted
1D752	Spectrum Defense Operations Journeyman	Enlisted
1D772	Spectrum Defense Operations Craftsman	Enlisted
1D732F	Spectrum Defense Operations Apprentice, Spectrum Operations	Enlisted
1D752F	Spectrum Defense Operations Journeyman, Spectrum Operations	Enlisted
1D772F	Spectrum Defense Operations Craftsman, Spectrum Operations	Enlisted
1D733	Cable and Antenna Defense Operations Apprentice	Enlisted
1D753	Cable and Antenna Defense Operations Journeyman	Enlisted
1D773	Cable and Antenna Defense Operations Craftsman	Enlisted
1D733C	Cable and Antenna Defense Operations Apprentice, Cable and Antenna Operations	Enlisted
1D753C	Cable and Antennae Defense Operations Journeyman, Cable and Antenna Operations	Enlisted
1D773C	Cable and Antenna Defense Operations Craftsman, Cable and Antenna Operations	Enlisted
Marine Corps		
0659	Cyber Network Systems Chief	Enlisted
2611	Cryptologic Cyberspace Analyst	Enlisted
0605	Cyber Network Operations Officer	Officer
1702	Cyberspace Warfare Officer	Officer
1705	Cyberspace Warfare Development Officer	Officer
1710	Offensive Cyberspace Warfare Officer	Warrant
1720	Defensive Cyberspace Warfare Officer	Warrant
1711	Offensive Cyberspace Warfare Operator	Enlisted
1721	Defensive Cyberspace Warfare Operator	Enlisted
1799	Cyberspace Warfare Chief	Enlisted
Navy		
H32A	Cyber Threat Emulation Operator (CTEO)	Enlisted
H30A	Cyber Defense Analyst	Enlisted
H42A	Cyber Research and Development Specialist	Enlisted
735A	Consolidated Afloat Networks and Enterprise Services (CANES) Administrator	Enlisted
746A	Information Systems Administrator	Enlisted
737A	Naval Tactical Command Support System (NTCSS) II Manager	Enlisted
738A	Global Command and Control System Maritime (GCCS-M) (Force Level 4.1) Increment 2 System Administrator	Enlisted
H05A	Joint Force Air Component Commander (JFACC) System Administrator	Enlisted

H06A	MQ-4C Unmanned Aircraft System (UAS) Forward Operating Base (FOB) Mission Control System (MD-38) Administrator	Enlisted
H08A	Advanced Network Analyst	Enlisted
742A	Network Security Vulnerability Technician	Enlisted
H33A	Cyber Network Defense Infrastructure Specialist (CNDIS)	Enlisted
741A	Information System Security Manager	Enlisted
H04A	Transmission System Technician	Enlisted
H33A	Cyber Network Defense Infrastructure Specialist (CNDIS)	Enlisted
H08A	Advanced Network Analyst	Enlisted
H07A	Applied Cyber Operations Master	Enlisted
H31A	Cyber Defense Analyst – Host (CDA-Host)	Enlisted
H33A	Cyber Network Defense Infrastructure Specialist (CNDIS)	Enlisted
H29A	Cyberspace Operations Planner	Enlisted
785B	Special Operations Forces (SOF) Offensive Cyberspace Operator	Enlisted
9690	Intelligence Support to CNO/CYBER	Officer
9690	Intelligence Support to CNO/CYBER	Warrant
C26A	AN/SSQ-137 Ship’s Signal Exploitation Equipment-SSEE Maintenance Technician	Enlisted
C28A	Ship’s Signal Exploitation Equipment Increment Foxtrot (SSEE INC F) Maintenance Technician	Enlisted
728A	Limited Communications Security (COMSEC) Maintenance Technician	Enlisted
C26A	AN/SSQ-137 Ship’s Signal Exploitation Equipment-SSEE Maintenance Technician	Enlisted
C27A	Submarine Carry-On Equipment Technician	Enlisted
C28A	Ship’s Signal Exploitation Equipment Increment Foxtrot (SSEE INC F) Maintenance Technician	Enlisted
C37A	Cryptologic Infrastructure Maintenance Technician	Enlisted
C38A	Surface Cryptologic Carry-On Program (CCOP) Technician	Enlisted
C27A	Submarine Carry-On Equipment Technician	Enlisted
C38A	Surface Cryptologic Carry-On Program (CCOP) Technician	Enlisted
H29A	Cyberspace Operations Planner	Enlisted
848A	CI/HUMINT Cyber Specialist	Enlisted
802R	Classification Interviewer	Enlisted
H07A	Applied Cyber Operations Master	Enlisted
H30A	Cyber Defense Analyst	Enlisted
H31A	Cyber Defense Analyst- Host (CDA-Host)	Enlisted
H12A	Exploitation Analyst	Enlisted
003107	Access Network Operator	Enlisted
H13A	Navy Interactive On-Net Operator	Enlisted
H14A	Navy Interactive On-Net (ION) Operator (Windows)	Enlisted
H15A	Navy Interactive On-Net (ION) Operator (Unix)	Enlisted
H11A	Digital Network Analyst	Enlisted
H32A	Cyber Threat Emulation Operator (CTEO)	Enlisted
H34A	Cyber Defense Analyst (CDA) - Network	Enlisted
H41A	Basic Offensive Cyber Operator	Enlisted

H42A	Cyber Research and Development Specialist	Enlisted
Army		
17B	Cyber and Electronic Warfare Officer	Officer
25D	Cyber Network Defender	Enlisted
17A	Cyber Warfare Officer	Officer
17C	Cyber Operations Specialist	Enlisted
170A	Cyber Warfare Technician	Warrant
17D	Cyber Capabilities Development Officer	Officer
170D	Cyber Capabilities Developer Technician	Warrant
Coast Guard		
CYB10	Cyber	Officer
CYB12	Cybersecurity	Officer
CYB13	Cyber Effects	Officer

APPENDIX D – Scenarios

Civilian-Specific Coding Considerations

This appendix provides specific civilian workforce coding guidance.   The following guidelines apply, whether the position is vacant or encumbered:

- Civilian positions in any of the four recognized occupational series are prohibited from using primary code 000.
- Civilian positions in occupational series within Tiers 1 and 2, or the Common Occupations may be identified with a primary code 000 if not aligned to the DCWF.
- If multiple positions use one position description, code each position (differentiated by individual position sequence numbers) with the relevant work role codes.

Sample Coding Scenarios

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. Two positions are provided as an introduction to the coding process. Review each of the position's key requirements and activities to determine which work role code(s) best apply. Then review the recommended coding solution and justification.

Scenario 1 - Information Technology Specialist (Information Security) position

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 executing the following activities:

- 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.

Approximately 30% of the position requires executing the following activities:

- 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.

Helpful Hint

Remember to review work role descriptions, tasks and KSAs for applicability. Also consider the "Core" versus "Additional" tasks and KSAs in the DCWF. If position requirements and activities consistently align with "Core" tasks and KSAs, that is an indicator that the position under review should be coded to the respective work role.

Another 30% of the position requires executing the following activities:

- 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 Information Systems Security Manager (ISSM) work role code of 722 and an additional Cyber Policy and Strategy Planner work role code of 752.

- This position should have a primary ISSM work role code of 722 because of the close alignment between work role functions and position requirements and activities. For example, in your review, you should have noticed that the ISSM work role definition directly aligns to the position summary provided.
- This position should have an additional Cyber Policy and Strategy Planner work role code of 752 because a smaller, but important focus of the position is related to IT and information security policy development.

Please note that coding to the DCWF does not change or replace a position's OPM occupational series (i.e., GS 2210 – Information Technology Management series). Rather, DWF work roles are added to this information, allowing the Department to better identify and track execution of specific work functions.

Scenario 2 – Data Scientist Position

This position provides expertise to management through the application of advanced data science techniques including data extraction, transformation, cleaning, modeling, machine learning, and artificial intelligence (AI) to process and extract insights from structured and unstructured data and provide guidance for solutions to a variety of complex challenges.

Approximately 40% of the position requires executing the following activities:

- Write and document reproducible code.
- Plan, coordinate, and execute complex studies using advanced data modeling techniques and procedures, data trend analysis, and data algorithms.
- Plan and conduct complex analytical, mathematical, and statistical research that informs operational requirements.
- Build predictive, prescriptive, or descriptive models in collaboration with stakeholders.
- Utilize open-source languages, as appropriate, and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line).

Approximately 30% of the position requires executing the following activities:

- Analyze data sources to provide actionable recommendations.
- Train and evaluate machine learning models.
- Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.
- Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method.

Another 30% of the position requires executing the following activities:

- Evaluate energy implications (graphical processing unit, tensor processing unit, etc.) when designing AI solutions.
- Collaborate with appropriate personnel to address Personal Health Information (PHI), Personally Identifiable Information (PII), and other data privacy and data reusability concerns for AI solutions.
- Program custom algorithms.

Work Role Code Solution
Code this position with a primary Data Science work role code of 423.

- This position should have a primary work role code of 423 because of the close alignment between work role functions and position requirements and activities. For example, when you review the Framework, you will notice that the Data Scientist work role definition directly aligns to the position summary provided.