



# **DoD 8140 Cyber Workforce Qualification Program**

## *Alignment of DoD Cyber Training to the DoD Cyber Workforce Framework Instructions*

Version 1.2  
issued on 19 April 2024

---

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



Unclassified

## Table of Contents

|                                                         |    |
|---------------------------------------------------------|----|
| INTRODUCTION AND PURPOSE.....                           | 3  |
| DOD CYBER TRAINING .....                                | 4  |
| THE DCWF.....                                           | 4  |
| DOD 8140 CYBER WORKFORCE QUALIFICATION PROGRAM.....     | 4  |
| ALIGNMENT OF DOD CYBER TRAINING TO THE DCWF .....       | 5  |
| METHOD OVERVIEW.....                                    | 6  |
| <i>Stage 1: Identification and Reporting</i> .....      | 6  |
| <i>Stage 2: Mapping and Reporting</i> .....             | 6  |
| DETAILED EVALUATION .....                               | 7  |
| <i>Stage 1: Identification and Reporting</i> .....      | 7  |
| <i>Step 1: Identification of Relevant Courses</i> ..... | 7  |
| <i>Step 2: Reporting of Course Information</i> .....    | 7  |
| <i>Stage 2: Mapping and Reporting</i> .....             | 7  |
| <i>Step 1: Course Evaluation and Mapping</i> .....      | 7  |
| <i>Step 2: Reporting Case Alignment</i> .....           | 9  |
| COMBINATION OF COURSES ALIGNED TO DCWF WORK ROLES ..... | 12 |
| SUBMISSION OF ALIGNMENT DOCUMENTATION .....             | 12 |
| GENERAL INFORMATION .....                               | 13 |
| REFERENCES.....                                         | 13 |
| APPENDIX A – MILITARY OCCUPATIONAL SPECIALTIES .....    | 14 |

## Tables and Figures

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| <i>Figure 1: DoD 8140 Qualification Program Model</i> .....                  | 5  |
| <i>Table 1: Example of Case I – Strong Alignment</i> .....                   | 9  |
| <i>Table 2: Example of Alignment to Both Core and Additional KSATs</i> ..... | 11 |



Unclassified

## Introduction and Purpose

Pursuant to the Department of Defense Manual (DoDM) 8140.03, “Cyberspace Workforce Qualification and Management Program,” the DoD CIO maintains a list of available DoD cyber training conducted, supported, or sponsored by the DoD Components. The list of available cyber training can be found on the DoD Cyber Exchange at: <https://public.cyber.mil/cyber-training/> DoD Components are requested to annually review the list of available cyber training on the DoD Cyber Exchange and provide input to the DoD CIO that maintains alignment of existing DoD cyber training to the core content of each DoD Cyber Workforce Framework (DCWF) work role.



To learn more about the DoD 8140 Policy Series, visit us on the DoD Cyber Exchange at:

<https://public.cyber.mil>

The DoDM 8140.03 and the DCWF are designed to be flexible and adaptable, enabling the DoD Components to organize and develop the DoD cyber workforce to meet the challenges of evolving technologies and threats.

Cyber training developed by the DoD alongside other measures of qualification, such as certifications or formal education, will be considered for the DoD 8140 Cyber Workforce Qualification Program to promote quality, equivalency, and recognition of qualifications across the Department. By aligning DoD cyber training to the DCWF work roles for inclusion into the DoD 8140 Cyber Workforce Qualification Program, DoD Components ensure future cost savings associated with identifying, developing, and authorizing training options for the DoD cyber workforce.

In accordance with the DoD Directive (DoDD) 8140.01, “Cyberspace Workforce Management,” the Office of Primary Responsibility (OPR) for each DoD Component should evaluate and recommend requirements for any undefined areas or content. The DoD CIO serves as the impartial facilitator of the DoD 8140 Cyber Workforce Qualification Program by avoiding any direct influence on the evaluation and validation activities.

The DoD CIO Workforce Innovation Directorate (WID) serves as the Cyber Workforce Management Board (CWMB) Secretariate and with the other members of the CWMB, manages and oversees the DoD 8140 Cyber Workforce Qualification Approval Process for the DoD cyber workforce elements including: Information Technology (IT) (Cyber), Cybersecurity, Cyber Enablers, Cyber Effects, Cyber (Intel), Data/Artificial Intelligence (AI), and Software Engineering.



Unclassified

## DoD Cyber Training

OSD and DoD Component cyber workforce training for military service members, DoD civilians, and contract support personnel should be approved in accordance with relevant OSD and DoD Component training standards and should include an assessment of learning outcomes.

## The DCWF

The DCWF serves as the authoritative lexicon for the uniform identification, tracking, data collection, and reporting of DoD cyber workforce positions and foundation for developing enterprise DoD cyber workforce qualifications. The DCWF provides standardized qualification criteria to improve interoperability and unity of action throughout the DoD and with mission partners across the nation. The DCWF Tool with the DoD cyber workforce elements and 72 work roles and their respective three-digit cyber codes is located on the Common Access Card (CAC)-enabled cyber.mil at the following link: <https://cyber.mil/wid/dcwf/>.

## DoD 8140 Cyber Workforce Qualification Program

The DoD 8140 Cyber Workforce Qualification Program (CWQP) establishes an enterprise approach to DoD cyber workforce qualification to enhance cyber mission readiness across the Department. The Program outlines qualification standards and requirements for each work role according to three levels of proficiency: Basic, Intermediate, and Advanced. Specifically, the Program consists of the following qualification areas:

- Education
- Training
- Personnel credentials
- On-the-job qualification
- Environment-specific requirements
- Continuous professional development



Unclassified

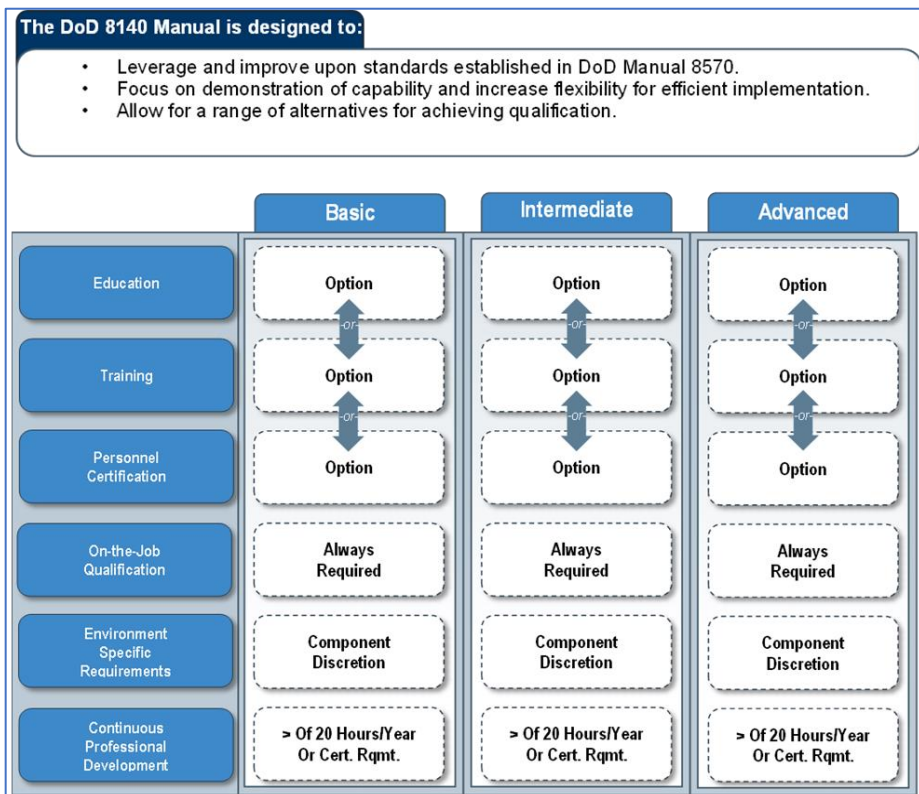


Figure 2: DoD 8140 Qualification Program Model

To achieve qualification, any personnel filling positions coded to the DCWF must meet the foundational and resident qualification requirements outlined for each work role at the assigned proficiency levels. Figure 1 is a notional work role DoD 8140 Cyber Workforce Qualification Program Model illustrating where training will be a qualification factor. In order for a DoD Component to use training as an option for foundational qualification, the training must meet the DoD 8140 criteria. The following sections outline how the DoD Components confirm that training meets the criteria.

## Alignment of DoD Cyber Training to the DCWF

DoD Components are asked to review and report all cyber courses of instruction aligned to the DCWF elements: **Information Technology (IT) (Cyber), Cybersecurity, Cyber Enablers, Cyber Effects, Cyber (Intel), Data/Artificial Intelligence (AI), and Software Engineering.**

The qualification matrix was designed with Foundational qualifications demonstrating a basic understanding of work roles while giving Components discretion in the Residential requirements. Therefore, some work roles have overlapping features. Trainings may align to more than one work role and/or proficiency level depending on curriculum objectives.

Collection, ingestion, and analysis of cyber-related training developed and/or owned by DoD Components will be completed in stages. This process allows the DoD CIO to first qualify the cyber-workforce, second validate and analyze Component training, and third inform future training development.

This is an open and continuous process with no formal suspense date in place for DoD cyber training to be submitted to DoD CIO.



Unclassified

## Method Overview

Stage 1 requires identification and reporting of cyber courses and Stage 2 requires the detailed analysis. The information requested by each stage may be submitted together or separately to the DoD CIO.

For stage 1, DoD Components should utilize the *DoD Cyber Training Alignment Report Form*. For stage 2, DoD Components should utilize the *DCWF Work Role Tool* to evaluate courses.

Alignment includes evaluation of the core knowledge, skills, abilities, and tasks (KSATs) of the DCWF work roles. It is the Components' responsibility to provide full course evaluation materials to the DoD CIO.

This alignment process consists of a detailed evaluation establishing first: the number of cyber trainings available, second: the degree to which a training meets the DoD 8140 Cyber Workforce Qualification Program criteria and application of the appropriate proficiency level, and third: the outlook for future training development.

### Stage 1: Identification and Reporting

Components should identify only relevant trainings developed and owned by the DoD. Commercially offered vendor courses/training, certifications, and certificates should not be included in this submission. However, information on those trainings can be forwarded to the DoD CIO at [osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil](mailto:osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil).

Components must include the following: course name, identification number, description, length, corresponding MOS, the weblink/location (CANTRAC, ATRRS, etc.) and proficiency level for inclusion in the DoD 8140 Cyber Workforce Qualification Program (*DoD Cyber Training Alignment Report Form*).

Curriculum developers and other appropriate subject matter experts should identify the course as meeting a Basic, Intermediate, or Advanced level of proficiency.

### Stage 2: Mapping and Reporting

Alignment of training to core KSATs should be *at least* 70%. However, by providing appropriate justification, Components may submit courses that align to core KSATs within 60-69%.

Components should document their mapping methodology of Terminal Learning Objectives (TLOs) to the core and additional KSATs of the applicable DCWF work role(s). Referencing Bloom's Taxonomy of Learning, TLOs refer to broad learning outcomes learners should be able to demonstrate upon completion of training. Course curricula should provide information on



Unclassified

TLOs as the official course numbering/designation with a brief written description. See the *DoD Cyber Training Standards-Guidebook* for more information.

## Detailed Evaluation

### Stage 1: Identification and Reporting

#### Step 1: Identification of Relevant Courses

Identification of POCs for schoolhouses or internal DoD-owned training.

Identification of cyber-related Military Occupational Specialty (MOS).

- DoD 8140.01 identifies four occupational series for consideration of cyber positions to be coded:
  - 0032- Computer Operation Series
  - 0335- Computer Clerk and Assistant Series
  - 1550- Computer Science Series
  - 2210- Information Technology Management Series
- Additionally, *Appendix A* offers an example list of cyber-related MOSs. It is at Component discretion if these MOSs and aligned training(s) should be aligned to the DCWF.

#### Step 2: Reporting of Course Information

Utilizing the: *DoD Cyber Training Alignment Report Form*, Components should list all cyber courses including the following: course name, identification number, description, length, corresponding MOS, the weblink/location (NIPR, SIPR, CANTRAC, ATRRS etc.) and proficiency level for inclusion in the DoD 8140 Cyber Workforce Qualification Program.

As further information may be required, and to reduce through channels, DoD CIO asks for the inclusion of schoolhouse and training POCs.

### Stage 2: Mapping and Reporting

#### Step 1: Course Evaluation and Mapping

Per Stage 1, trainings have already been nominated and submitted for consideration in the Qualification Matrix. Now, the Component should analyze and compare the training curriculum to the DCWF KSATs, ensuring the curriculum assesses proficiency in at least 70% of the core KSATs. For each DCWF work role aligned to the training, it must achieve a score of 70% or better to be approved for use in accordance with DoDM 8140.03.

If the training does not achieve proficiency in at least 70% of the core KSATs for the DCWF work role, the offering is not ready and will require modification prior to approval for use. If the alignment falls between the 60-69% of core KSATs, mapping to additional KSATs should be provided as well as a justification for why the course should be accept.



Unclassified

A training may be used in tandem with another training to achieve proficiency in at least 70% of the core KSATs for the given DCWF work role. In this case, it must be clarified the trainings are “linked” and, only after completion of the final course, qualifies to a work role. For example, Defense Acquisition University has credentialing programs in which several courses are combined to create a learning pathway which align to a work role. However, completion of a single course within the pathway does not meet the criteria for alignment to a work role.

A nominated training program must directly train towards the DCWF work role(s) (not 2% training towards DCWF work role and 98% training towards unrelated topics).

**To perform the assessment of course alignment to the KSATs, the following steps are recommended:**

1. Identify the DCWF work role(s) that best aligns to the training(s). The training(s) must demonstrate alignment with at least one DCWF work role. Compare the training curriculum information against the relevant DCWF elements, work roles and their core KSATs to determine if the training sufficiently aligns to achieve a 70% alignment score.
2. For the chosen DCWF work role(s) that align to the training, determine whether each of the DCWF work role’s core KSATs are compatible with the training. This suitability analysis step should be completed for each KSAT within the DCWF work roles aligned to the training.
  - a. For example, it may not be realistic for a certification exam or course objective to address a core KSAT requiring the ability to “lead a team.” A specific core KSAT should be excluded from the set of KSATs for the aligned training offering if the KSAT is outside the scope of training.
    - i. The KSAT outside the scope of the training offering (i.e., “lead a team”), would need to be met through a separate qualification method (e.g., certification, training, or experience).
  - b. Consequently, the KSAT not met by the training offering will contribute to the 30% not aligned for needed approval.
3. For each of the core KSATs, determine the degree to which the core KSAT is fully or partially covered by one or more of the curriculum objectives.
  - a. Course curricula should provide information on TLOs as the official course numbering/designation with a brief written description.
  - b. A single core KSAT can be covered by one or more objectives, and an objective can be used to address multiple core KSATs.



Unclassified

4. Assess, and if necessary, extrapolate details using the available course content to determine whether the description of a specific objective could reasonably be expected to satisfy a given core KSAT.
5. Consider the course objectives that correlate to a skill or task in the DCWF work role description:
  - a. Whether the experience and knowledge required of a person is sufficient to satisfy the exam objectives correctly and adequately; and
  - b. Whether the exam objectives provide and/or enhance the person's understanding and comprehension such that they would be better able to identify, apply, analyze, demonstrate, and evaluate situations related to conducting the core KSATs required for the DCWF work role.
6. Consider "prerequisite" knowledge required and determine whether prerequisites are needed prior to enrolling in a training. For advanced level cyber trainings in particular, course objectives often do not explicitly address fundamental skills either assumed or not directly applicable to specialized skill sets. For instance, forensics analysts or penetration testing certification offerings may not explicitly address core KSATs pertaining to cyber defense in-depth concepts or basic computer protocols, but it may be reasonable to expect an individual holding such a certification to have that knowledge or proficiency.
7. Document and tabulate the KSATs covered by the course material.
8. The overall evaluation score is calculated as a ratio of the number of core KSATs covered by the curriculum to the total number of core KSATs. In accordance with DoD 8140.03, to achieve approval, the overall evaluation must meet or exceed 70% alignment of the core KSATs for a DCWF work role.
9. A curriculum subject matter expert should determine the proficiency level of the course.

### Step 2: Reporting Case Alignment

The cases below describe the three alignment options: *Case I- Strong Alignment*, *Case II- Possible Alignment*, and *Case III- Poor Alignment*.

#### *Case I- Strong Alignment*

For *Case I-Strong Alignment*, include curriculum objectives aligned to only **core** KSATs. Aligning the core KSATs demonstrates due diligence on behalf of the curriculum owner and establishes a



Unclassified

record of alignment for traceability and accountability. If a course's TLOs cover 70% or more of the total number of core KSATs, the course meets the "Strong Alignment" criteria for inclusion. *Table 1* illustrates the *Case I* documentation required for each course.

*Table 1: Example of Case I-Strong Alignment*

| Element  |        | OPR/OCR  |                                                                                                                                         | Work Role (DCWF Code)        |
|----------|--------|----------|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Cyber IT |        |          |                                                                                                                                         | Database Administrator (421) |
| NIST SP# | DCWF # | Task/KSA | Tasks                                                                                                                                   | Core (C) Or Additional(A)    |
|          | 5890   | Task     | <b>Identify data consolidation opportunities across database systems, including data sharing and access between business lines.</b>     | <b>C</b>                     |
|          |        |          | Official Course TLO numbering/designation-Brief Description                                                                             |                              |
|          |        |          | Official Course TLO numbering/designation-Brief Description                                                                             |                              |
| T0162    | 740    | Task     | <b>Perform backup and recovery of databases to ensure data integrity.</b>                                                               | <b>C</b>                     |
|          |        |          | Official Course TLO numbering/designation-Brief Description                                                                             |                              |
| T0491    | 665A   | Task     | <b>Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.</b> | <b>C</b>                     |
|          |        |          | Official Course TLO numbering/designation-Brief Description                                                                             |                              |
| T0162    | 740    | Task     | <b>Perform backup and recovery of databases to ensure data integrity.</b>                                                               | <b>C</b>                     |
|          |        |          | Official Course TLO numbering/designation-Brief Description                                                                             |                              |
| NIST SP# | DCWF # | Task/KSA | Knowledge, Skills, and Abilities                                                                                                        | Core (C) Or Additional(A)    |
|          | 7029   | KSA      | <b>Knowledge of how to collect, store, and monitor data.</b>                                                                            | <b>C</b>                     |



Unclassified

|  |             |            |                                                                 |          |
|--|-------------|------------|-----------------------------------------------------------------|----------|
|  |             |            | Official Course TLO numbering/designation-<br>Brief Description |          |
|  | <b>179B</b> | <b>KSA</b> | <b>Skill in establishing data security controls.</b>            | <b>C</b> |
|  |             |            | Official Course TLO numbering/designation-<br>Brief Description |          |
|  |             |            | Official Course TLO numbering/designation-<br>Brief Description |          |

### Case II- Possible Alignment

For *Case II- Possible Alignment*, indicate the applicable TLOs that satisfy both core *and* additional KSATs. *Table 2* **Error! Reference source not found.** illustrates the *Case II* process and exemplifies the documentation required for each course.

Table 1: Example of Alignment to Both Core and Additional KSATs

| Element      |             | OPR/OCR     |                                                                                                                                         | Work Role (DCWF Code)        |
|--------------|-------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Cyber IT     |             |             |                                                                                                                                         | Database Administrator (421) |
| NIST SP#     | DCWF #      | Task/KS A   | Tasks                                                                                                                                   | Core (C) Or Additional(A)    |
|              | <b>5890</b> | <b>Task</b> | <b>Identify data consolidation opportunities across database systems, including data sharing and access between business lines.</b>     | <b>C</b>                     |
|              |             |             | Official Course TLO numbering/designation-<br>Brief Description                                                                         |                              |
|              |             |             | Official Course TLO numbering/designation-<br>Brief Description                                                                         |                              |
| <b>T0162</b> | <b>740</b>  | <b>Task</b> | <b>Perform backup and recovery of databases to ensure data integrity.</b>                                                               | <b>C</b>                     |
|              |             |             | Official Course TLO numbering/designation-<br>Brief Description                                                                         |                              |
|              |             |             | Official Course TLO numbering/designation-<br>Brief Description                                                                         |                              |
| <b>T0491</b> | <b>665A</b> | <b>Task</b> | <b>Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.</b> | <b>A</b>                     |
|              |             |             | Official Course TLO numbering/designation-<br>Brief Description                                                                         |                              |



Unclassified

|                     |                   |                      |                                                                           |                                      |
|---------------------|-------------------|----------------------|---------------------------------------------------------------------------|--------------------------------------|
|                     |                   |                      | Official Course TLO numbering/designation-<br>Brief Description           |                                      |
| <b>T0162</b>        | <b>740</b>        | <b>Task</b>          | <b>Perform backup and recovery of databases to ensure data integrity.</b> | <b>A</b>                             |
|                     |                   |                      | Official Course TLO numbering/designation-<br>Brief Description           |                                      |
| <b>NIST<br/>SP#</b> | <b>DCWF<br/>#</b> | <b>Task/KS<br/>A</b> | <b>Knowledge, Skills, and Abilities</b>                                   | <b>Core (C) Or<br/>Additional(A)</b> |
|                     | <b>7029</b>       | <b>KSA</b>           | <b>Knowledge of how to collect, store, and monitor data.</b>              | <b>C</b>                             |
|                     |                   |                      | Official Course TLO numbering/designation-<br>Brief Description           |                                      |
|                     | <b>179B</b>       | <b>KSA</b>           | <b>Skill in establishing data security controls.</b>                      | <b>A</b>                             |
|                     |                   |                      | Official Course TLO numbering/designation-<br>Brief Description           |                                      |
|                     |                   |                      | Official Course TLO numbering/designation-<br>Brief Description           |                                      |

If the percentage of core KSATs covered by the TLOs is between 60% and 69%, the course may meet the criteria for inclusion. In this case, the Component should submit the course information along with a brief explanation of how the course maps to the DCWF content. In this case, the course information will be reviewed by a third-party validator to assist in making a final determination.

#### Case III- Poor Alignment

If alignment percentage is not within acceptable limits, no further evaluation is necessary. The course does not qualify for inclusion into the DoD 8140 Cyber Workforce Qualification Program.

### Combination of Courses Aligned to DCWF Work Roles

If a designed combination of DoD Component courses fulfills the requirements for a single work role, then complete the Cyber Training Alignment Report Form with information for each of the respective courses and complete a DCWF Work Role Tool evaluation for each course.

### Submission of Alignment Documentation

DoD Components should submit the Cyber Training Alignment Report Form (*Attachment 1*) and the DCWF Work Role Tool evaluation results for all *Case I* and *Case II* cyber courses. Following a review of each submission, the DoD CIO WID will develop a comprehensive list of cyber training courses eligible for inclusion in the DoD 8140 Cyber Workforce Qualification Program. This information will be stored on the Defense Information Systems Agency (DISA) Cyber Exchange



Unclassified

(CE). DoD Components are to ensure documentation was reviewed by a subject matter expert and by the appropriate Command or organization personnel who can authorize the submission.

DoD Components should submit all Cyber Training Alignment Report Forms, completed evaluation results, and any additional supporting documentation to the DoD CIO WID at [osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil](mailto:osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil).

## General Information

The DoD CIO WID will update the appropriate public and CAC-enabled DoD 8140 Cyber Workforce Qualification Program online portals and databases regarding final decisions. Meeting minutes documenting any official decisions will count as official correspondence.

For questions regarding this document or for more information, visit <https://public.cyber.mil/> or contact the DoD CIO WID at [osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil](mailto:osd.mc-alex.dod-cio.mbx.cyberspace-workforce-tag@mail.mil).

## References

- a. DoD Directive 8140.01, Cyberspace Workforce Management, October 2020
- b. DoD Instruction 8140.02, Identification, Tracking, and Reporting of Cyberspace Workforce Requirements, December 2021
- c. DoD Manual 8140.03, Cyberspace Workforce Qualification and Management Program, February 2023
- d. Anderson, L.W., Krathwohl, D.R., Airasian, P.W., Cruikshank, K.A., Mayer, R.E., Pintrich, P.R., Raths, J., Wittrock, M.C. (2001). [\*A Taxonomy for Learning, Teaching, and Assessing: A revision of Bloom's Taxonomy of Educational Objectives\*](#). New York: Pearson, Allyn & Bacon.



Unclassified

## APPENDIX A – 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 3* 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](https://www.onetcenter.org/dl_files/2019/military_crosswalk.zip)

*Table 3: Military Occupation Specialties*

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



Unclassified

|               |                                                                               |          |
|---------------|-------------------------------------------------------------------------------|----------|
| <b>17S2Z</b>  | Cyberspace Effects Operations, C2ISREW (if Prefix N or P)                     | Officer  |
| <b>17S3Z</b>  | Cyberspace Effects Operations, C2ISREW (if Prefix N or P)                     | Officer  |
| <b>17S4Z</b>  | Cyberspace Effects Operations, C2ISREW (if Prefix N or P)                     | Officer  |
| <b>1D700</b>  | Cyber Defense Operations Manager                                              | Enlisted |
| <b>1D791</b>  | Cyber Defense Operations Superintendent                                       | Enlisted |
| <b>1D731R</b> | Cyber Defense Operations Apprentice, RF Operations                            | Enlisted |
| <b>1D731Z</b> | Cyber Defense Operations Apprentice, Software Development Operations          | Enlisted |
| <b>1D751R</b> | Cyber Defense Operations Journeyman, RF Operations                            | Enlisted |
| <b>1D751Z</b> | Cyber Defense Operations Journeyman, Software Development Operations          | Enlisted |
| <b>1D771R</b> | Cyber Defense Operations Craftsman, RF Operations                             | Enlisted |
| <b>1D771Z</b> | Cyber Defense Operations Craftsman, Software Development Operations           | Enlisted |
| <b>3D032</b>  | Cyber Systems Operations Apprentice                                           | Enlisted |
| <b>3D052</b>  | Cyber Systems Operations Journeyman                                           | Enlisted |
| <b>3D072</b>  | Cyber Systems Operations Craftsman                                            | Enlisted |
| <b>3D033</b>  | Cyber Surety Apprentice                                                       | Enlisted |
| <b>3D053</b>  | Cyber Surety Journeyman                                                       | Enlisted |
| <b>3D073</b>  | Cyber Surety Craftsman                                                        | Enlisted |
| <b>17C0</b>   | Cyberspace Warfare Operations Commander                                       | Officer  |
| <b>17D1A</b>  | Warfighter Communications Operations, Network Operations                      | Officer  |
| <b>17D3A</b>  | Warfighter Communications Operations, Network Operations                      | Officer  |
| <b>17D4A</b>  | Warfighter Communications Operations, Network Operations                      | Officer  |
| <b>17D1B</b>  | Warfighter Communications Operations, Expeditionary Communications Operations | Officer  |
| <b>17D3B</b>  | Warfighter Communications Operations, Expeditionary Communications Operations | Officer  |
| <b>17D4B</b>  | Warfighter Communications Operations, Expeditionary Communications Operations | Officer  |
| <b>17D1M</b>  | Warfighter Communications Operations, RPA                                     | Officer  |
| <b>17D1N</b>  | Warfighter Communications Operations, ABM                                     | Officer  |
| <b>17D1P</b>  | Warfighter Communications Operations, Fighter                                 | Officer  |
| <b>17D1Q</b>  | Warfighter Communications Operations, Trainer                                 | Officer  |
| <b>17D1R</b>  | Warfighter Communications Operations, Bomber                                  | Officer  |
| <b>17D1T</b>  | Warfighter Communications Operations, Airlift                                 | Officer  |
| <b>17D1V</b>  | Warfighter Communications Operations, Helicopter or EWO                       | Officer  |
| <b>17D1W</b>  | Warfighter Communications Operations, General CSO                             | Officer  |
| <b>17D3M</b>  | Warfighter Communications Operations, RPA                                     | Officer  |
| <b>17D3N</b>  | Warfighter Communications Operations, ABM                                     | Officer  |
| <b>17D3P</b>  | Warfighter Communications Operations, Fighter                                 | Officer  |



Unclassified

|              |                                                                               |          |
|--------------|-------------------------------------------------------------------------------|----------|
| <b>17D3Q</b> | Warfighter Communications Operations, Trainer                                 | Officer  |
| <b>17D3R</b> | Warfighter Communications Operations, Bomber                                  | Officer  |
| <b>17D3S</b> | Warfighter Communications Operations, Software Development                    | Officer  |
| <b>17D3T</b> | Warfighter Communications Operations, Airlift                                 | Officer  |
| <b>17D3V</b> | Warfighter Communications Operations, Helicopter or EWO                       | Officer  |
| <b>17D3W</b> | Warfighter Communications Operations, General CSO                             | Officer  |
| <b>17D3Y</b> | Warfighter Communications Operations, Special Operations CSO (if Prefix N)    | Officer  |
| <b>17D4M</b> | Warfighter Communications Operations, RPA                                     | Officer  |
| <b>17D4N</b> | Warfighter Communications Operations, ABM                                     | Officer  |
| <b>17D4P</b> | Warfighter Communications Operations, Fighter                                 | Officer  |
| <b>17D4Q</b> | Warfighter Communications Operations, Trainer                                 | Officer  |
| <b>17D4R</b> | Warfighter Communications Operations, Bomber                                  | Officer  |
| <b>17D4S</b> | Warfighter Communications Operations, Software Development                    | Officer  |
| <b>17D4T</b> | Warfighter Communications Operations, Airlift                                 | Officer  |
| <b>17D4V</b> | Warfighter Communications Operations, Helicopter or EWO                       | Officer  |
| <b>17D4W</b> | Warfighter Communications Operations, General CSO                             | Officer  |
| <b>1B000</b> | Cyber Warfare Operations Manager                                              | Enlisted |
| <b>1B491</b> | Cyber Warfare Operations Superintendent                                       | Enlisted |
| <b>1B431</b> | Cyber Warfare Operations Apprentice                                           | Enlisted |
| <b>1B451</b> | Cyber Warfare Operations Journeyman                                           | Enlisted |
| <b>1B471</b> | Cyber Warfare Operations Craftsman                                            | Enlisted |
| <b>17D2A</b> | Warfighter Communications Operations, Network Operations                      | Officer  |
| <b>17D2B</b> | Warfighter Communications Operations, Expeditionary Communications Operations | Officer  |
| <b>17D2M</b> | Warfighter Communications Operations, RPA                                     | Officer  |
| <b>17D2N</b> | Warfighter Communications Operations, ABM                                     | Officer  |
| <b>17D2P</b> | Warfighter Communications Operations, Fighter                                 | Officer  |
| <b>17D2Q</b> | Warfighter Communications Operations, Trainer                                 | Officer  |
| <b>17D2R</b> | Warfighter Communications Operations, Bomber                                  | Officer  |
| <b>17D2S</b> | Warfighter Communications Operations, Software Development                    | Officer  |
| <b>17D2T</b> | Warfighter Communications Operations, Airlift                                 | Officer  |
| <b>17D2V</b> | Warfighter Communications Operations, Helicopter or EWO                       | Officer  |
| <b>17D2W</b> | Warfighter Communications Operations, General CSO                             | Officer  |
| <b>17D3Z</b> | Warfighter Communications Operations, C2ISREW CSO                             | Officer  |
| <b>17S4B</b> | Cyberspace Effects Operations, Defensive Cyberspace Operator                  | Officer  |
| <b>17S4M</b> | Cyberspace Effects Operations, RPA                                            | Officer  |
| <b>17S4N</b> | Cyberspace Effects Operations, ABM                                            | Officer  |
| <b>17S4P</b> | Cyberspace Effects Operations, Fighter                                        | Officer  |



Unclassified

|              |                                                              |         |
|--------------|--------------------------------------------------------------|---------|
| <b>17S4Q</b> | Cyberspace Effects Operations, Trainer                       | Officer |
| <b>17S4R</b> | Cyberspace Effects Operations, Bomber                        | Officer |
| <b>17S4S</b> | Cyberspace Effects Operations, Tanker (if Prefix N or P)     | Officer |
| <b>17S4T</b> | Cyberspace Effects Operations, Airlift                       | Officer |
| <b>17S4V</b> | Cyberspace Effects Operations, Helicopter or EWO             | Officer |
| <b>17S4W</b> | Cyberspace Effects Operations, General (if Prefix N or P)    | Officer |
| <b>17S4C</b> | Cyberspace Effects Operations, Capabilities Development      | Officer |
| <b>17S2A</b> | Cyberspace Effects Operations, Offensive Cyberspace Operator | Officer |
| <b>17S2B</b> | Cyberspace Effects Operations, Defensive Cyberspace Operator | Officer |
| <b>17S2M</b> | Cyberspace Effects Operations, RPA                           | Officer |
| <b>17S2N</b> | Cyberspace Effects Operations, ABM                           | Officer |
| <b>17S2P</b> | Cyberspace Effects Operations, Fighter                       | Officer |
| <b>17S2Q</b> | Cyberspace Effects Operations, Trainer                       | Officer |
| <b>17S2R</b> | Cyberspace Effects Operations, Bomber                        | Officer |
| <b>17S2S</b> | Cyberspace Effects Operations, Tanker (if Prefix N or P)     | Officer |
| <b>17S2T</b> | Cyberspace Effects Operations, Airlift                       | Officer |
| <b>17S2V</b> | Cyberspace Effects Operations, Helicopter or EWO             | Officer |
| <b>17S2W</b> | Cyberspace Effects Operations, General (if Prefix N or P)    | Officer |
| <b>17S2Y</b> | Cyberspace Effects Operations, General                       | Officer |
| <b>17S1Y</b> | Cyberspace Effects Operations, General                       | Officer |
| <b>17S3Y</b> | Cyberspace Effects Operations, General                       | Officer |
| <b>17S4Y</b> | Cyberspace Effects Operations, General                       | Officer |
| <b>17S1A</b> | Cyberspace Effects Operations, Offensive Cyberspace Operator | Officer |
| <b>17S1B</b> | Cyberspace Effects Operations, Defensive Cyberspace Operator | Officer |
| <b>17S1M</b> | Cyberspace Effects Operations, RPA                           | Officer |
| <b>17S1N</b> | Cyberspace Effects Operations, ABM                           | Officer |
| <b>17S1P</b> | Cyberspace Effects Operations, Fighter                       | Officer |
| <b>17S1Q</b> | Cyberspace Effects Operations, Trainer                       | Officer |
| <b>17S1R</b> | Cyberspace Effects Operations, Bomber                        | Officer |
| <b>17S1S</b> | Cyberspace Effects Operations, Tanker (if Prefix N or P)     | Officer |
| <b>17S1T</b> | Cyberspace Effects Operations, Airlift                       | Officer |
| <b>17S1V</b> | Cyberspace Effects Operations, Helicopter or EWO             | Officer |
| <b>17S1W</b> | Cyberspace Effects Operations, General (if Prefix N or P)    | Officer |
| <b>17S3A</b> | Cyberspace Effects Operations, Offensive Cyberspace Operator | Officer |
| <b>17S3B</b> | Cyberspace Effects Operations, Defensive Cyberspace Operator | Officer |
| <b>17S3M</b> | Cyberspace Effects Operations, RPA                           | Officer |
| <b>17S3N</b> | Cyberspace Effects Operations, ABM                           | Officer |
| <b>17S3P</b> | Cyberspace Effects Operations, Fighter                       | Officer |
| <b>17S3Q</b> | Cyberspace Effects Operations, Trainer                       | Officer |



Unclassified

|               |                                                                            |          |
|---------------|----------------------------------------------------------------------------|----------|
| <b>17S3R</b>  | Cyberspace Effects Operations, Bomber                                      | Officer  |
| <b>17S3S</b>  | Cyberspace Effects Operations, Tanker (if Prefix N or P)                   | Officer  |
| <b>17S3T</b>  | Cyberspace Effects Operations, Airlift                                     | Officer  |
| <b>17S3V</b>  | Cyberspace Effects Operations, Helicopter or EWO                           | Officer  |
| <b>17S3W</b>  | Cyberspace Effects Operations, General (if Prefix N or P)                  | Officer  |
| <b>17S4A</b>  | Cyberspace Effects Operations, Offensive Cyberspace Operator               | Officer  |
| <b>17S3C</b>  | Cyberspace Effects Operations, Capabilities Development                    | Officer  |
| <b>17S2C</b>  | Cyberspace Effects Operations, Capabilities Development                    | Officer  |
| <b>17S1C</b>  | Cyberspace Effects Operations, Capabilities Development                    | Officer  |
| <b>17D4C</b>  | Warfighter Communications Operations, Capabilities Development             | Officer  |
| <b>17D3C</b>  | Warfighter Communications Operations, Capabilities Development             | Officer  |
| <b>17D2C</b>  | Warfighter Communications Operations, Capabilities Development             | Officer  |
| <b>17D1C</b>  | Warfighter Communications Operations, Capabilities Development             | Officer  |
| <b>17D2Y</b>  | Warfighter Communications Operations, Special Operations CSO (if Prefix N) | Officer  |
| <b>17D2Y</b>  | Warfighter Communications Operations, General                              | Officer  |
| <b>17D2Z</b>  | Warfighter Communications Operations, C2ISREW CSO                          | Officer  |
| <b>17D3Y</b>  | Warfighter Communications Operations, General                              | Officer  |
| <b>17D4Y</b>  | Warfighter Communications Operations, General                              | Officer  |
| <b>17D4Z</b>  | Warfighter Communications Operations, C2ISREW CSO                          | Officer  |
| <b>17D1Z</b>  | Warfighter Communications Operations, C2ISREW CSO                          | Officer  |
| <b>17D4Y</b>  | Warfighter Communications Operations, Special Operations CSO (if Prefix N) | Officer  |
| <b>1D731D</b> | Cyber Defense Operations Apprentice, Security Operations                   | Enlisted |
| <b>1D731E</b> | Cyber Defense Operations Apprentice, Client Systems Operations             | Enlisted |
| <b>1D731K</b> | Cyber Defense Operations Apprentice, Knowledge Operations                  | Enlisted |
| <b>1D751D</b> | Cyber Defense Operations Journeyman, Security Operations                   | Enlisted |
| <b>1D751E</b> | Cyber Defense Operations Journeyman, Client Systems Operations             | Enlisted |
| <b>1D751K</b> | Cyber Defense Operations Journeyman, Knowledge Operations                  | Enlisted |
| <b>1D771D</b> | Cyber Defense Operations Craftsman, Security Operations                    | Enlisted |
| <b>1D771E</b> | Cyber Defense Operations Craftsman, Client Systems Operations              | Enlisted |
| <b>1D771K</b> | Cyber Defense Operations Craftsman, Knowledge Operations                   | Enlisted |
| <b>1D732</b>  | Spectrum Defense Operations Apprentice                                     | Enlisted |
| <b>1D752</b>  | Spectrum Defense Operations Journeyman                                     | Enlisted |
| <b>1D772</b>  | Spectrum Defense Operations Craftsman                                      | Enlisted |
| <b>1D732F</b> | Spectrum Defense Operations Apprentice, Spectrum Operations                | Enlisted |
| <b>1D752F</b> | Spectrum Defense Operations Journeyman, Spectrum Operations                | Enlisted |
| <b>1D772F</b> | Spectrum Defense Operations Craftsman, Spectrum Operations                 | Enlisted |
| <b>1D733</b>  | Cable and Antenna Defense Operations Apprentice                            | Enlisted |



Unclassified

|                     |                                                                                                                |          |
|---------------------|----------------------------------------------------------------------------------------------------------------|----------|
| <b>1D753</b>        | Cable and Antenna Defense Operations Journeyman                                                                | Enlisted |
| <b>1D773</b>        | Cable and Antenna Defense Operations Craftsman                                                                 | Enlisted |
| <b>1D733C</b>       | Cable and Antenna Defense Operations Apprentice, Cable and Antenna Operations                                  | Enlisted |
| <b>1D753C</b>       | Cable and Antennae Defense Operations Journeyman, Cable and Antenna Operations                                 | Enlisted |
| <b>1D773C</b>       | Cable and Antenna Defense Operations Craftsman, Cable and Antenna Operations                                   | Enlisted |
| <b>Marine Corps</b> |                                                                                                                |          |
| <b>0659</b>         | Cyber Network Systems Chief                                                                                    | Enlisted |
| <b>2611</b>         | Cryptologic Cyberspace Analyst                                                                                 | Enlisted |
| <b>0605</b>         | Cyber Network Operations Officer                                                                               | Officer  |
| <b>1702</b>         | Cyberspace Warfare Officer                                                                                     | Officer  |
| <b>1705</b>         | Cyberspace Warfare Development Officer                                                                         | Officer  |
| <b>1710</b>         | Offensive Cyberspace Warfare Officer                                                                           | Warrant  |
| <b>1720</b>         | Defensive Cyberspace Warfare Officer                                                                           | Warrant  |
| <b>1711</b>         | Offensive Cyberspace Warfare Operator                                                                          | Enlisted |
| <b>1721</b>         | Defensive Cyberspace Warfare Operator                                                                          | Enlisted |
| <b>1799</b>         | Cyberspace Warfare Chief                                                                                       | Enlisted |
| <b>Navy</b>         |                                                                                                                |          |
| <b>H32A</b>         | Cyber Threat Emulation Operator (CTEO)                                                                         | Enlisted |
| <b>H30A</b>         | Cyber Defense Analyst                                                                                          | Enlisted |
| <b>H42A</b>         | Cyber Research and Development Specialist                                                                      | Enlisted |
| <b>735A</b>         | Consolidated Afloat Networks and Enterprise Services (CANES) Administrator                                     | Enlisted |
| <b>746A</b>         | Information Systems Administrator                                                                              | Enlisted |
| <b>737A</b>         | Naval Tactical Command Support System (NTCSS) II Manager                                                       | Enlisted |
| <b>738A</b>         | Global Command and Control System Maritime (GCCS-M) (Force Level 4.1) Increment 2 System Administrator         | Enlisted |
| <b>H05A</b>         | Joint Force Air Component Commander (JFACC) System Administrator                                               | Enlisted |
| <b>H06A</b>         | MQ-4C Unmanned Aircraft System (UAS) Forward Operating Base (FOB) Mission Control System (MD-38) Administrator | Enlisted |
| <b>H08A</b>         | Advanced Network Analyst                                                                                       | Enlisted |
| <b>742A</b>         | Network Security Vulnerability Technician                                                                      | Enlisted |
| <b>H33A</b>         | Cyber Network Defense Infrastructure Specialist (CNDIS)                                                        | Enlisted |
| <b>741A</b>         | Information System Security Manager                                                                            | Enlisted |
| <b>H04A</b>         | Transmission System Technician                                                                                 | Enlisted |
| <b>H33A</b>         | Cyber Network Defense Infrastructure Specialist (CNDIS)                                                        | Enlisted |
| <b>H08A</b>         | Advanced Network Analyst                                                                                       | Enlisted |
| <b>H07A</b>         | Applied Cyber Operations Master                                                                                | Enlisted |



Unclassified

|             |                                                                                            |          |
|-------------|--------------------------------------------------------------------------------------------|----------|
| 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 |
| <b>Army</b> |                                                                                            |          |
| 17B         | Cyber and Electronic Warfare Officer                                                       | Officer  |
| 25D         | Cyber Network Defender                                                                     | Enlisted |



Unclassified

|                    |                                         |          |
|--------------------|-----------------------------------------|----------|
| <b>17A</b>         | Cyber Warfare Officer                   | Officer  |
| <b>17C</b>         | Cyber Operations Specialist             | Enlisted |
| <b>170A</b>        | Cyber Warfare Technician                | Warrant  |
| <b>17D</b>         | Cyber Capabilities Development Officer  | Officer  |
| <b>170D</b>        | Cyber Capabilities Developer Technician | Warrant  |
| <b>Coast Guard</b> |                                         |          |
| <b>CYB10</b>       | Cyber                                   | Officer  |
| <b>CYB12</b>       | Cybersecurity                           | Officer  |
| <b>CYB13</b>       | Cyber Effects                           | Officer  |