CYBER TRAINING AND QUALIFICATION

COMDTINST 1500.2
October 2023

THIS PAGE INTENTIONALLY LEFT BLANK

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

U.S. Coast Guard Stop 7324
2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7324
Staff Symbol: CG-7
Phone: (202) 372-2024

COMDTINST 1500.2
23 OCT 2023

COMMANDANT INSTRUCTION 1500.2

Subj: CYBER TRAINING AND QUALIFICATION

Ref:
(a) CGCYBER: Mission Essential Task List (METL) Version 1.0
(b) Mandatory Use of the Training Management Tool, COMDTINST 5270.2 (series)
(c) Coast Guard Military Human Resource Record (CGMHRR) System, COMDTINST 1080.10 (series)
(d) U.S. Coast Guard Competency Management System Manual, COMDTINST M5300.2 (series)
(e) Performance, Training and Education Manual (PTEM), COMDTINST 1500.10 (series)
(f) Intelligence Training, COMDTINST 1500.26 (series)
(g) Cyber Master Training List (MTL), Apr 2023
(h) Cyberspace Workforce Qualification and Management Program, DoDM 8140.03

1. PURPOSE. This Instruction establishes the minimum training and qualification policies and requirements mandated by the Commandant for all personnel directly supporting Operational Cyber Missions.

2. ACTION. All Coast Guard Commanding Officers, Officers in Charge, Deputy/Assistant Commandants, and Chiefs of Headquarters Staff Elements shall comply with the provisions of this Instruction.

3. AUTHORIZED RELEASE. Internet release is authorized.

4. DIRECTIVES AFFECTED. None.

5. DISCUSSION. This Instruction establishes and consolidates the minimum training requirements mandated by Headquarters. However, the policies contained do not prevent the Cyber Operational Commander and subordinate units from specifying additional training requirements for Cyber personnel. The burden for funding any additional training initiatives lies with the organization or unit that mandated them.

6. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide administrative guidance for Coast Guard personnel and is not intended nor does it impose legally-binding requirements on any party outside the Coast Guard.

7. SCOPE AND AUTHORITIES. It is recommended that all personnel supporting the cyber training program become familiar with the directives and publications noted throughout this Instruction including References (d) and (e), the Cyberspace Workforce Qualification and Management Program, DoDM 8140.03, and the Coast Guard Cyber Master Training List.

8. IMPACT ASSESSMENT. The requirements contained in this Instruction apply to all personnel assigned to or supporting the accomplishment of Operational Cyber Missions. Funding for training required by this Instruction and the Master Training List (MTLs) is covered under the training funding provided to FORCECOM through the Intelligence and Cyber Program, Projects, and Activities (PPA) within the Operations and Support (O&S) appropriation.

9. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. The Office of Environmental Management, Commandant (CG-47) reviewed this Commandant Instruction and the general policies contained within and determined that this policy falls under the Department of Homeland Security (DHS) categorical exclusion A3. This Commandant Instruction will not result in any substantial change to existing environmental conditions or violation of any applicable federal, state, or local laws relating to the protection of the environment. It is the responsibility of the action proponent to evaluate all future specific actions resulting from this policy for compliance with the National Environmental Policy Act (NEPA), other applicable environmental requirements, and the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 (series).

10. DISTRIBUTION. Electronic distribution in the Directives System Library. Intranet/Pixel Dashboard: Directives Pubs, and Forms - PowerApps (appsplatform.us) . If Internet released: Commandant Instructions (uscg.mil), Coast Guard Forms (uscg.mil) .

11. RECORDS MANAGEMENT CONSIDERATIONS. Records created as a result of this Instruction, regardless of format or media, must be managed in accordance with Records & Information Management Program Roles and Responsibilities, COMDTINST 5212.12 (series) and the records retention schedule located on the Records Resource Center Microsoft SharePoint site at: https://uscg.sharepoint-mil.us/sites/cg61/SitePages/CG-611-RIM.aspx .

12. FORMS. Suggested changes and/or corrections for immediate action may be submitted to USCG.Forms@uscg.mil.

13. SECTION 508. This policy is created to adhere to accessibility guidelines and standards as promulgated by the U.S. Access Board with consideration of Information and Communications Technology (ICT) requirements. If accessibility modifications are needed for this artifact, please communicate with the Section 508 Program Management Office (PMO) at Section.508@uscg.mil. Concerns or complaints for non-compliance of policy and/or artifacts may be directed to the Section 508 PMO, the Civil Rights Directorate (https://www.uscg.mil/Resources/Civil-Rights/) for the Coast Guard, or to the U.S. Department of Homeland Security at accessibility@hq.dhs.gov.

14. REQUESTS FOR CHANGES. Units and individuals may formally recommend changes through the chain of command using the Coast Guard Memorandum. Comments and suggestions from users of the Instructions are welcomed. All such correspondence may be emailed to the Office of Cyberspace Capability, Commandant (CG-791) at HQS-SMB-CG-791-CyberspaceForces@uscg.mil.

/TODD C. WIEMERS/
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Capability

TABLE OF CONTENTS

Chapter 1. General

A. Purpose. This Chapter provides a general overview of the organizational structure that supports the cyber training program throughout the Coast Guard. Follow-on chapters of this Instruction and various references describe the cyber training program and its elements in detail.

B. Background.

1. General. Cyberspace is an operational domain that is continually growing in complexity and importance. As with other mission domains, operating and controlling this domain to the degree necessary to achieve mission success requires a highly specialized workforce that is trained to achieve superiority against our adversaries. In 2015, the Coast Guard published its Cyber Strategy, which asserted the requirement for a technically proficient cyber workforce. This was re-enforced in the Cyber Strategic Outlook in 2021. This requirement was also identified in the US Coast Guard Cyber, Chief Information Officer (CIO), and C4IT Governance and Transformation Blueprint (C3TF) final report. This report not only captured the need for training, but also included a recommendation for creating a unique cyber rating and accompanying Cyber Officer cadre. Doing so would establish a trained professional force equipped with the requisite skills to protect and defend the Coast Guard and the nation in cyberspace.

2. Mission Essential Task List (METL). The need to embrace a formal Cyber training structure was further defined by the creation of the Cyber METLs maintained on CG-791 SharePoint site. Accordingly, the METL specifically identifies the tasks critical to the Coast Guard's cyber mission. If they are not accomplished to an acceptable degree, mission outcomes will be degraded, exacerbating risk of failure.

    a. These tasks assist in measuring the service's mission readiness. In addition to laying out the operational tasks, this Instruction will help measure the success of the Cyber training program. Training is essential to sustaining the Service's missions.

    b. The Cyber METL establishes a direct requirement for Cyber Training through three overarching tasks. These tasks are further refined in Reference (a) with the conditions that will govern their performance and measure their effectiveness.

Training Related Cyber Mission Essential Tasks

Task:	**CG-SA 7.2.4: Assess Training and Education Effectiveness**
Descriptions:	To conduct an evaluation of education and training to measure the demonstrated performance of unit commanders, components, individuals, leaders, and units against specified education and training standards. This task, conducted by unit commanders, included after action reviews and organizational assessments, and provides feedback for altering policy.
Task	**CG-TA 4.7.2: Develop Training Plans and Programs**
Descriptions:	To prepare unit and individual training plans and programs Note: The Special Mission Training Qualification Manual (COMDTINST M3502.16) states that CGCYBER will develop its own training plans and programs.
Task:	**CG-TA 5.3.6: Conduct Exercises**
Descriptions:	To conduct exercises as required for Ready for Operation or other performance requirements for assigned missions. Exercises may be conducted by the entire force, by individual units, with other agencies, or with other countries and services

Figure 1- Training Related Cyber METLs

c. In addition to establishing the requirements for a Cyber Training Program, the METL defines the degree to which training influences the success of operational and mission support tasks. The METL provides a metric for performance expectations and sets a target when identifying training opportunities and when developing curricula and training tools. This information provides the foundation for the necessary knowledge, skills, and abilities required by all relevant operational and support personnel. METL for Cyber Protection Teams (CPT), Cyber Mission Teams (CMT), and Cybersecurity Service Providers (CSSP) are established by the Department of Defense (DoD).

d. The Office of Cyberspace Forces (CG-791) is responsible for staffing, equipping, and training the Coast Guard to meet the challenges of the asymmetrical threat posed by our adversaries in the Cyber domain. Accordingly, CG-791 drafted this Instruction and the tactics, techniques, and procedures for conducting cyber training herein.

3. Applicability. This Instruction focuses primarily on the newly established Cyber Mission Management (CMM) Warrant Officer Specialty and the Cyber Mission Specialist (CMS) enlisted rating assigned to an operational role performing Defensive Cyber Operations

(DCO) and Offensive Cyber Operations (OCO). DOD Information Network (DODIN) Operations are also covered. All US Coast Guard cyber operational missions can be contextualized in terms of the three lines of effort (LOEs) of the Cyber Strategic Outlook:

a. Defend and Operate the Enterprise Mission Platform (EMP)

b. Protect the Marine Transportation System (MTS)

c. Operate in and through Cyberspace

Multiple ratings and specialties perform essential operational and mission support functions that are critical to cyber mission success. Functioning training structure and methodology exists for this capability; this Instruction formalizes the training structure in alignment with service procedure. In future versions of this Instruction, and as the Cyber mission matures within the Coast Guard, the training philosophy will be updated and enhanced to embrace the total force.

C. Cyber Training Requirements.

1. Minimum Requirements. This Instruction establishes the minimum training requirements for training needed to support the Cyber Mission and does not limit CGCYBER and other commanders tasked with the Cyber Operational mission from specifying additional training requirements that do not conflict with this guidance. However, only the Cyber Training PM can mandate a formal Class "A" or Class "C" school requirement.

   a. Validated and approved training and qualification requirements are documented in the Cyber MTL (Reference (g)). CG-791, CGCYBER, Cyber Course Managers (CM), CMS Rating Force Master Chief (RFMC), CMS Rating Knowledge Manager (RKM), and FORCECOM (FC-T, FC-A) shall continually review the MTL to ensure that they fully address all tasks critical to mission success, as identified in the Mission Essential Task List (METL) for Cyber Operations. They shall determine if the training and exercise requirements, frequencies, drill assessment and evaluation methodologies, and individual qualification programs meet the needs of the cyber operator and are providing them with the skills to successfully execute the Cyber Mission. The validated MTL is accessible through the CG-791 SharePoint.

   b. Supporting CG-791 in this effort, the Office of C5I Capabilities (CG-761) shall assess the effectiveness of cyber training, as related to fielded tools, during their annual Operation Analysis process and shall assist CG-791 in establishing requirements to resolve insufficient and/or ineffective training.

   c. Units identifying an operational cyber training need may submit them for consideration through the C5I Requirements Intake Process. Units with recommended changes to this Instruction shall submit them through a memo to CG-791, via their chains of command.

D. Cyber Training Organization.

1. Office of Cyberspace Forces, Commandant (CG-791).

a. Promulgates and maintains this Instruction.

b. Ensures validation, consolidation, standardization, and certification of all training requirements impacting cyber operations.

c. Establishes and maintains policies for the implementation of a unit cyber training program.

d. Consolidates formal class "C" school requirements based on input from Rating Training Advisory Council (RTAC).

e. Directs personnel to the CG Mandated Training (MT) requirements posted on FORCECOM's Learning Management System (LMS).

f. Establishes and maintains policies for cyber qualification programs.

g. Sets the requirements and standards for the cyber individual qualification program.

h. Oversees and evaluates cyber individual qualifications program(s).

i. Establishes priorities for cyber individual qualification program(s).

j. Reviews training plans/requirements for new commands/units, systems, and capabilities to ensure requirements for individual qualifications are identified and scheduled.

k. Plans and programs for the resources necessary to operate and administer the cyber individual qualification program.

l. Approves all final cyber individual qualification material to meet emergent mission requirements.

m. Issues messages to commands supporting the Cyber Mission regarding new, updated, or deleted qualification standards and issues in an annual report to the cyber community, which covers the status of the individual qualification program.

n. Establishes and maintains the policy governing the completion of drills/exercises within required periodicity and frequency.

o. Establishes and maintains the policy covering special training and recognition programs, acts as PM for cyber insignia program.

p. Maintains a centralized SharePoint site containing approved MTLs and pipeline training, Watch Station Qualification Standards (WQS), and drill frequency requirements.

q. Works with Headquarters PMs to ensure future resource proposals include training resources as appropriate.

2. Office of C5I Capabilities, Commandant (CG-761).

a. Acts as Commandant's Sponsor's Representative for Cyber and other training applications.

b. As the C5I Requirement "Front Door" (RFD), establishes, prioritizes, and delivers to the C5I PMO requirements that will ensure all approved competencies are available in TMT.

c. As the C5I RFD establishes, prioritizes, and delivers to the C5I PMO requirements.

d. Evaluates the effectiveness of cyber training relating to C5I systems and applications during the annual Operational Analysis process.

e. Debriefs the Cyber Training PM and assists them in establishing requirements for corrective actions.

3. Chief, C5I Program Management Office (PMO), Commandant (CG-68).

a. Implements technical solutions in response to C5I requirements established by CG-761.

b. Ensures Direct Access, TMT, and other Cyber Training capabilities conform to and are included in Enterprise Architecture.

c. Ensures Direct Access, TMT, and other Cyber Training capabilities are maintained including all actions required to maintain their accreditation.

d. Facilitates resolution of any technical issues or casualties to Direct Access and TMT.

4. Cyber Course Managers.

a. Manages all resident, non-resident, exportable and vendor-provided courses under their control.

b. Collaborates with CG-791, CGCYBER Training Officer, FORCECOM (FC-T) Education and Training Quota Management Command (ETQC), RFMCs, RKMs and subordinate field unit commanders to determine Coast Guard wide training needs.

c. Reference (e) contains a complete listing of CM responsibilities.

5. FORCECOM – Training Division (FC-T).

   a. Promulgates and adjudicates training policy, technical standards, processes, guidelines, and best practices.

   b. Conducts analyses and communicates acquired findings to HQ PM to foster a sense of clarity regarding next steps for training and performance support required to mitigate gaps.

   c. Measures effectiveness of Formal Training policies, procedures, and resource utilization to maximize the effectiveness of training and education.

   d. Ensures all Formal Training opportunities and solutions are responsive to service needs and are conducted in the most effective and efficient manner.

   e. Functions as the Inter-Service Training Office (ITO) in coordination with other services ITOs.

   f. Manages Formal Training for the Coast Guard to include throughput requirements, curriculum outlines, and other curriculum control documents. Act as waiver authority for all formal training course requirements. FC-T may delegate waiver authority to PM or CM.

   g. Manages the formal training build process to develop annual training throughput requirements for CG formal training.

   h. Serves as training technical authority for all aspects of formal training to include TRACEN Commercially contracted Class “C” schools, Other Government Agencies training, functions at the Education and Training Quota Command (ETQC), and use of Training Allowance Billets (TAB).

   i. Serves as technical authority over PSC and CGRC for Class “A” Schools and Accession Training.

6. FORCECOM - Business Operations Division (FC-B).

   a. Serves as program office for FORCECOM enterprise-wide training and education resources.

   b. Manages formal training and education funding made available to FORCECOM and the broader training and education enterprise.

c. Manages training quota control system and staffing to support formal training, and Accessions Programs. Manage budget (operating funds) and staffing for the FORCECOM Training System (TRASYS).

d. Provides tactical oversight of ETQC ensuring compliance with FC-CI education tactics, training policies, processes, and procedures.

e. Serves as requirements validator for new information technology (IT) capability gaps or IT acquisitions in accordance with FCEA.

f. Maintains authority over the Systems Engineering Lifecycle (SELC) and Acquisition Lifecycle Framework for all proposed and existing FORCECOM IT systems, to include simulators and training aids.

7. Education and Training Quota Management Command (ETQC).

a. Functions as the execution section of the Training System for Advanced Training executed within a temporary duty status.

b. Manages all Class "C" school students' status in the systems of record internal and external to the Coast Guard.

c. Issues Formal Training Travel Orders (TONOS) for Active Duty, Active Duty for Operational Support (ADOS) over 180 days, Extended Active Duty (EAD), Civilian, and Auxiliary members.

d. Issues No-cost training orders for Reservists. Reservists are responsible for acquiring Reserve Training Orders.

8. CGCYBER.

a. Coordinates training needs, job skills, and other education, certification, and qualification requirements to the Cyber Training PM (CG-791).

b. Maintains Cyber Mission readiness standards. Carries out an active unit training program based on the requirements of this Instruction and other CGCYBER and FORCECOM directives.

c. Advises unit personnel to frequently check their training summary in Direct Access to ensure that all formal training (Class "C" Schools) records are up to date.

d. Ensures entries are made in TMT and DA to document all individual training, unit training, and completed drills and exercises.

E. Training Administration.

1. Training Management Tool (TMT). Reference (b) discusses the mandatory use of this training management system throughout the U.S. Coast Guard. TMT is a web-based training, qualification, and certification data reporting application. TMT provides operational commanders with the ability to effectively identify and manage unit-level training and qualification requirements and to allocate appropriate resources for both active duty and reserve personnel. Though mandatory training requirements are pre-loaded into the system, they can be customized to best serve units and operational commanders. All unit training requirements approved by CGCYBER, or CG-791 shall be managed in TMT, except for formal schools.

    a. Use of TMT. Units shall capture all competencies, qualifications, certifications, and course completions in TMT, apart from those items listed above, pertaining to individual training, unit training, Mandated Training (MT), Watch station Qualification Standards (WQS), Personnel Qualification Standards (PQS), Job Qualification Requirements (JQR) completion, and completion of drills and exercises.

    b. The actual date of the certification or completion shall be entered, not the date the data was entered into TMT. The requirements set forth in References (c) and (d) remain in effect.

2. Coast Guard Business Intelligence (CGBI). Coast Guard Business Intelligence (CGBI) is the Coast Guard's primary reporting system and provides an efficient way to determine the training status of personnel assigned to Cyber-related commands. Additionally, CGBI provides a quick way to determine a command's completion status for unit-based requirements such as periodic drills and exercises and minimum required unit competencies.

3. Data Warehouse. CGBI is a front end for the Coast Guard's data warehouse. The data warehouse cannot be edited. CGBI, via the data warehouse, pulls data straight from the source systems altered only in format. There are only two reasons for a potential discrepancy; either the data has changed in the source (AOPS/TMT or DA) between the 24-hour refresh window for the data warehouse, or measures (performance algorithms) have been applied to the data in the data warehouse, by request, to present a different data output. If a measure needs to be changed, then a ticket must be submitted to CGBI.

Chapter 2. The Unit Training Program

A. Purpose. This Chapter establishes guidance for the development, administration, and execution, for CGCYBER and commands conducting cyber operations to creating and maintaining a unit training program.

B. Background.

1. Importance. The Coast Guard's greatest resource is its workforce. With limited resources and multiple missions, the importance of training, educating, and developing our personnel is vital to mission success. The unit training program is the single most important tool for carrying out these goals for meeting the demands of the Cyber mission. Educating the Cyber Workforce to meet the challenges of an ever-evolving adversarial environment requires a continuum of education and training opportunities. This pathway begins with classroom-based education provided through Class "A" or Class "C" schools, which provide each member with a broad knowledge base on Cyberspace Operations and its elements (Defensive and Offensive).

   a. The Unit Training Program provides a level of learning beyond foundational understanding. Through the Unit Training Program, Cyber Mission Specialists are capacitated to apply and correlate concepts learned in the classroom. Knowledge, skills, and abilities acquired will ensure the cyber workforce can secure, protect, and defend our computer systems and networks against foreign and domestic threats and conduct operations in and through cyberspace.

   b. The Unit Training Program utilizes various techniques and processes to hone acquired skills including on-the-job or over-the-shoulder training, drills, and exercises. To ensure high quality and standardized training, supervisors shall ensure utilization of Job Qualification Requirements (JQR), Personal Qualification Standards (PQS), and a continuous learning plan. Unit Training gives the ability to successfully perform within their billet in accordance with the MTL.

   c. An effective Unit Training Program is paramount in ensuring the Cyber mission workforce has the necessary education, training, and skills to successfully meet mission objectives. Continued development of people within the organization is always the top priority.

2. Training Scenarios. Training must be realistic, challenging, and performed to standards. Considering Defense Information Systems Agency (DISA)/Joint Force Headquarters Department of Defense Information Network (DODIN), and US Cyber Command requirements and protocols, training should be conducted using the latest equipment, capabilities, processes, procedures, and tools in the cybersecurity industry. Realistic training ensures the CMS workforce is equipped to prevent, detect, and respond to cyberattacks that can have wide-ranging effects on individuals, communities, the Coast Guard, and the nation.

a. The goal is to train the Cyber workforce using the latest technology and cyberspace operations tactics and techniques while using real-life scenarios. This is not always achievable as technological resources can be limited and existing technology may not have the capability for specialists to train with it. During these times, specialists will be trained using simulated environments, virtual reality, live exercises, or other future tools yet to be developed.

b. To meet the goals established by this Instruction, for all training tools designed, developed, and/or acquired, Commandant (CG-791) will coordinate with Commandant (CG-761) for new C5I capabilities.

3. Command Emphasis. A unit training program is only effective when cyber personnel are dedicated to continued growth and development within their specialty. Commanding Officers or command-designated authorities will emphasize the importance of each person's continued growth and development by implementing a monthly mandated training program.

4. Individual Training Record. TMT, Direct Access (DA), and USCYBERCOM workforce management tools are the primary depositories for recording individual and unit qualification and training completion. However, all personnel are strongly encouraged to maintain their own copy of their training records and completion certificates as they transfer units and progress through their career. Individual training records can be used to resolve inaccuracies in TMT and DA thereafter.

5. Unit Training Board. CGCYBER and commands conducting cyber operations will establish a Unit Training Board (UTB). Unit Training Board membership will be chartered and signed by command authority and will include the Unit Training Officer (UTO), Cyber Course Managers, and all Department Heads. The purpose of the UTB is to identify training gaps, ambiguities in training policies and requirements, and report their findings to the CMS Rating Force Master Chief (RFMC) and the CMS Rating Knowledge Manager (RKM). The UTB will also establish and maintain a unit instruction that sets requirements for training and a unit training plan and a qualification board to assess unit personnel's ability to perform at a higher level with increased levels of responsibility.

C. Unit Training Instruction.

1. Unit Training Instruction. CGCYBER and subordinate Commands will establish and maintain a Unit Training Instruction to addresses the following:

a. Unit Training Board.

b. Work role qualification requirements, standards, and procedures for obtainment of competencies for continued advancement within specialty.

c. Internal routing procedures for approval of Personnel Qualifications Standards (PQS)

and Job Qualifications (JQR) including drill/exercise evaluation and department/division training records.

d. UTO duties and responsibilities.

e. Unit Quarterly Training Plan.

f. Responsibilities, policies, and procedures associated with the command training program.

g. Requirements for maintenance of training records.

h. Qualification standards and timelines for obtainment.

2. Unit Training Plan. The Unit Training Plan is the foundation of the unit-training program, which is prepared by the UTB. The plan includes dates for each scheduled drill, exercise, all-hands training, and mandated training. These training evolutions should be indicated in the plan by drill number, course code, topic names, or specific identifiers. Unit Training Plans will be reviewed annually. Superseded training plans will be retained for two years.

D. Specific Responsibilities.

1. Commander CGCYBER. Ensures the unit has a training plan and the plan is reviewed annually by the UTB. They ensure the Unit Training Plan provides clear guidance to members on their roles and responsibilities. They ensure a UTB is established, and unit has a designated UTO, UTB, CTT and UTO in writing. COs are responsible for ensuring compliance of training plans in accordance with the latest policies, procedures, and instructions. They ensure members not complying with policies and procedures are held accountable via corrective action and/or removal of members from duties through decertification or other action deemed necessary.

2. Deputy Commander, CGCYBER.

a. Serves as chairman of the UTB.

b. Appoints and supervises the UTO.

c. Monitors the Unit Training Plan.

d. Establishes and administers the unit training program.

e. Monitors the training, qualification, and development of the CTT.

3. Unit Training Board.

   a. Meets monthly to review training program requirements and establish/update training Plans.

   b. Carries out the training objectives and defines scope of Unit Training Program in accordance with command guidelines.

   c. Schedules drills, exercises, training periods, and professional development training for accomplishing mandated training.

4. Unit Training Officer.

   a. Maintains the Unit Training Instruction in accordance with this Chapter.

   b. Reviews DA to ensure accuracy and completeness of formal school completion in accordance with Chapter 3 of this Instruction.

   c. Advises the Commander of any discrepancies and coordinates with appropriate training commands/ETQC to correct entries.

   d. Reviews TMT to ensure the accuracy and completeness of record documentation.

   e. Reviews TMT to ensure the accuracy, completeness, and currency status of all qualifications, certifications, decertification's, and recertifications.

   f. Reviews TMT to ensure the accuracy and completeness of record documentation of drills and exercises completed Reviews individual and unit training records to ensure the accuracy, completeness and currency status of certifications not already included in DA and TMT.

   g. Documents completion and maintains records of unit level drills and exercises.

   h. Manages the unit’s training program in accordance with Paragraph 2 of this Instruction.

   i. Maintains records of all Individual Development Plans in accordance with Reference (e).

   j. Implements and monitors professional qualification programs including but not limited to Officer Watch Position/Senior Enlisted Position, and the Cyberspace Insignia, and ensures appropriate documentation is completed.

   k. Verifies prospective student pre-requisites prior to submitting Electronic Training Requests (ETRs) for Class “C” Schools.

l. Annotates the unit training plan continually to reflect training completed.

m. For further guidance, Reference (e) includes the Coast Guard's Tactics, Techniques, and Procedures (CGTTP) for implementing a unit training program, monitoring mandated training completion, guiding student enrollment tasks, standardizing tasks, and navigating through online training site tools, duties, and responsibilities.

5. Department Head/Division Chief.

a. Appoints Department/Division Assistant Training Officer.

b. Ensures department/division training, PQS and JQR programs, and mandated training schedules are established and implemented.

c. Ensures the assignment of an instructor for each department/division for each mandated training period.

d. Ensures lesson plan outlines are developed for each training topic not covered by online courses.

e. Ensures lesson plan outlines are complete, accurate, and achieve desired training objectives.

f. Monitors the effectiveness of instruction. Provides appropriate guidance and feedback to UTB and UTO.

6. Department/Division Assistant Training Officer (ATO).

a. Assigns or acts as instructor(s) for department/division training periods.

b. Advises department/division officers of training progress and deficiencies.

c. Coordinates the development of lessons plan outlines within the department/division.

d. Assists the UTO/UTPO in maintaining a central file of all lesson plan outlines for department/division training topics.

e. Assists the UTO/UTPO in ensuring that TMT and DA entries are made to capture completed training for personnel within their department/division.

E. Unit Training Program Elements

1. Training Program. The overall unit training consists of the following elements. Each element is covered in detail within a separate chapter of this Instruction.

a. Formal Schools. Formal Training and Mandated Training requirements and

applicable administrative guidelines are set forth in Chapter 3 of this Instruction.

b. Individual Qualification Programs. PQS and JQR requirements and applicable administrative guidelines are set forth in Chapter 4 of this Instruction.

c. Professional Development. Requirements and applicable administrative guidelines for several professional qualification programs are set forth in Chapter 4.

F. Training Program.

1. General Requirements. All CYBER Units, Departments, Branches, Team, and subordinate commands will develop and implement a training program. The purpose of the training program is to familiarize each new member with the basic administration, organization, and standard operating procedures of the command. Specific attention will be given to critical safety related issues and programs. Training programs include, but are not limited to, the following:

a. Assignment of a mentor or running mate to guide the new member through the unit's workday and watch station qualification process.

b. Commencement of specific PQS or JQRs.

c. Completion of "check-in" sheets and initial interviews with department/division chiefs and others in the chain-of-command, as appropriate.

d. Assignment of qualifications or competencies required by the billet or command to ensure minimum required watch rotations and to maintain operational readiness.

e. Assignment of the estimated timeline of progression of qualifications and the expected timing of completion of each.

2. Completion. The initial training program (indoctrination) will be structured so that it can be completed within two weeks of the member reporting aboard. Completion of assigned PQS or JQR qualifications will of course take longer.

Chapter 3. Cyber Formal School Requirements

A. Purpose. The purpose of this Chapter is to publish formal (Class "A" and Class "C") school requirements and establish policy regarding the context, assignment, and management of training quotas for personnel transitioning into or advancing within the Cyber Mission Specialist (CMS) enlisted rating or the Cyber Mission Management (CMM) Chief Warrant Officer (CWO) Specialty.

B. Background.

1. Applicability. In accordance with Reference (e), Class "A" schools traditionally prepare members to perform at the entry level of their chosen specialty. For CMS rated personnel, the Class "A" school pipeline provides the transitioning member with the foundational knowledge required to perform Cyberspace Operations duties at the apprentice level. In contrast, Class "C" school training opportunities are designed to provide advanced/specialized skills and knowledge to perform a task, or a group of tasks required by a Cyberspace Operations billet or unit.

2. Mission Essential Task List (METL). The Cyber METLs (Reference (a)) describe the tasks that must be performed for mission success, outlines the conditions under which the function is performed, and establishes measures for gauging the performance and operational effectiveness of the task. These measures help form the minimum threshold requirements for training establishing performance expectations and identifying the degree to which the cyber operator is expected to perform the task. CG-791, CGCYBER, Course Manager, and FORCECOM routinely assess the curriculum and performance of selected courses to ensure they remain fit for purpose and function. Additionally, they ensure mission requirements are considered during the creation and maintenance of the Cyber Master Training List (MTL).

3. Master Training List (MTL). The Cyber MTL (Reference (g)) is an administrative tool used to present formal school and qualification requirements for each billet. The Cyber MTL lists training requirements by position, course codes and course descriptions, Course Managers, and the type of training for each course (see definitions below). The Cyber MTL is maintained by CG-791 and is posted on its SharePoint Portal site. Changes to the Cyber MTL are approved by CG-791 after a review by CGCYBER, FORCECOM (FC-T), Education & Training Quota Management Command (ETQC), and appropriate Program Managers/Course Managers. Approved Cyber MTLs will be announced by message to the Cyber Community.

C. Definitions.

1. Foundational Training. Class "A" school provides the foundational knowledge required for a Cyber Mission Specialist to perform their duties. Candidates selected for transition to the rating must successfully complete the Class "A" school prior to being officially designated as a CMS.

2. Pre-Arrival/Pipeline Training. Training deemed essential for a member to complete prior

to arriving at a new unit. Traditionally, this type of training is conducted on a Temporary Duty (TDY) basis prior to the member's Permanent Change of Station (PCS) but may instead be conducted enroute. In some cases, the course length will necessitate PCS orders. Education & Training Quota Management Command works directly with the Personnel Service Center (PSC) to issue orders for Pre-Arrival Training. Members work directly with EQTC to address scheduling conflicts. If a member cannot attend Pre-Arrival Training, the member's current command must provide a request with justification to CGCYBER explaining the circumstances.

3. Advanced Training. Training deemed essential for a specific billet, mission, or requirement. In most cases, Class "C" schools, in accordance with Figure 2 and Table 2, or other advanced training may also be considered Pre-Arrival Training since the associated knowledge, skills, and abilities (KSAs) are required to perform the functions of the position to be filled.

4. Required Training. Required training should be completed during the tour of duty at the new unit. Units must submit Electronic Training Requests (ETRs) to request required training after the member has reported aboard to the unit. In most cases, Class "C" schools or other advanced training will be considered required training, specifically when the member needs to achieve foundational knowledge or other pre-requisites prior to attending training.

D. Class "A" School.

1. General. The Cyber Operations Specialist Course (COS) Phase I, sponsored by the U.S. Army, serves as the Coast Guard Cyber Mission Specialist Class "A" school. The U.S. Navy's Joint Cyber Analysis Course (JCAC) is a suitable alternative.

2. Requesting CMS Class "A" School.

   a. Upon a member being approved to transition to the CMS rate, ETQC and PSC's Enlisted Personnel Management (EPM) branch coordinate to determine class placement. Due to the duration of the CMS Class "A" school, official PCS orders are required. Figure 1 below outlines the foundational training pipeline.

   b. Once a member's Change in Rate request has been approved and their Security Clearance has been favorably adjudicated, they will be assigned a billet in CMS Class "A" school (COS Phase I) at U.S. Army's Fort Eisenhower, GA.

   c. Upon completion of COS Phase I, students are eligible and will have the prerequisite knowledge and skills to pass the Computer Network Assessment Battery (CNAB) exam. Participation is optional.

   d. Upon successfully completing the Class "A" school, most CMS personnel will receive orders to a Cyber billet in the Cyberspace Operations career path (NOSC, CSOC, COAB, RSI, TMB).

e. An alternate pathway may be available for exceptional performers to move directly into more advanced billets. Details will be promulgated in separate correspondence by the CMS Rating Force Master Chief.

f. CMS career paths are flexible, after completion of a member's first tour as a CMS, or any subsequent assignment, members may choose to compete for an "advanced" Cyber billet, either on a Cyber Mission Team (CMT), a Cyber Protection Team (CPT), or an assignment to CISA or USCYBERCOM and will receive the associated training in accordance with the Master Training List (MTL).

g. Members receiving orders to a CPT, CISA, or USCYBERCOM will receive orders to Cyber Common Core Technical Core (CCTC) at Fort Eisenhower in accordance with MTL.

h. Members selected to serve on a CMT will receive orders for COS Phase II at FT Eisenhower for advanced training. Then, depending on their specialty, upon completion of Phase II they will report to Title 10 Basic Operator Course (BOC) or Title 10 Exploitation Analyst (EA).

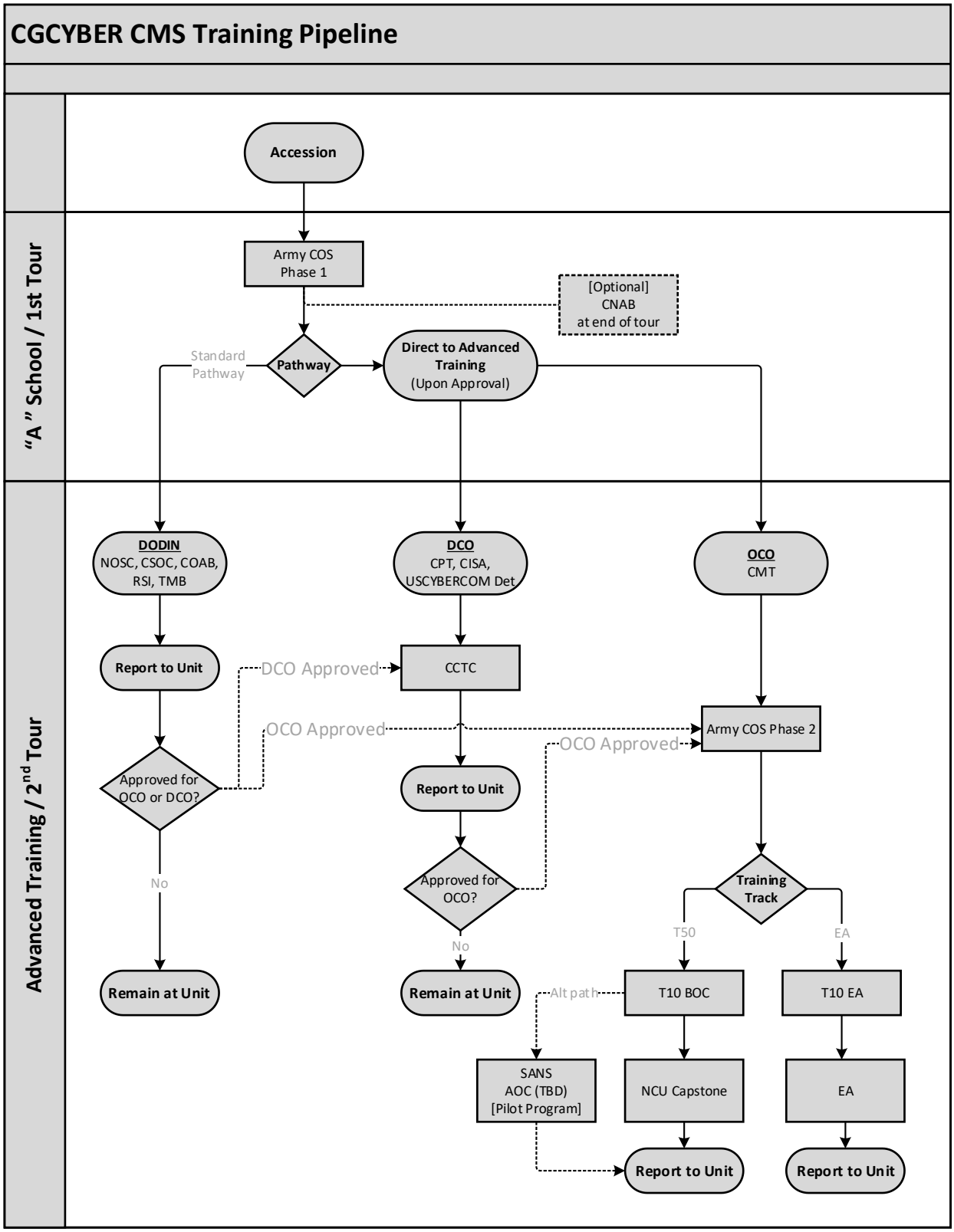

Figure 2: Training Pipeline

3. Additional Information.

   a. Members applying for the CMS rate must be eligible for a Top-Secret clearance with access to Sensitive Compartmented Information (SCI). Clearance eligibility extends through enrollment in the Class "A" school pipeline. A SCI pre-nomination interview shall be conducted to determine whether the member's credentials for SCI eligibility are favorable. If interview results are favorable, the member shall complete an SF-86 (security clearance package) by contacting the Security Center (SECCEN). On each Class "A" school application, the command must certify completion of a SCI pre-nomination interview and that their security package was completed with SECCEN. The following statement must accompany each application: "This command certifies that member is a U.S. Citizen, SCI pre-nomination interview conducted on (date) and SSBI security package was completed with SECCEN on (date)." If this statement is not received, the member will be placed on a security hold until the command can certify completion.

   b. Members must complete the Class "A" school pipeline to complete their transition to CMS. If for any reason a member is disenrolled prior to successful completion, they will be returned to their previous rating and made eligible for orders.

E. Class "C" School.

1. Requesting CMS Class "C" School. Class "C" school requirements for CMS billets are defined in the Cyber MTL. As with the Class "A" schools, if a "C" school is designated as pre-arrival training, which is normally conducted on a TDY basis prior to the member's PCS but may also be conducted in route. Education & Training Quota Management Command works directly with the PSC to issue orders for Pre-Arrival Training. Figure 2 above depicts the complete training pipeline.

Chapter 4. Cyber Operations Workforce Development

A. Purpose. To establish policy and responsibilities for Cyber Operations Workforce Development for commands supporting the Cyberspace Mission.

B. Background.

1. Training Introduction. Members fulfilling cyberspace work-roles execute worldwide operations in support of the Coast Guard Cyberspace missions. This Chapter provides an overview of the policies and requirements, in tandem with USCYBERCOM policies and requirements, of the training and qualification system necessary to assure the continued development and availability of cyber professionals.

   a. This Chapter also provides a broad overview of the training infrastructure and how it relates to the cyber training program. Follow-on sections of this Chapter describe the unit training program and its various elements in greater detail.

   c. The following paragraphs also provide a general description of various training sources and programs used to assist Cyber Command in the execution of its unit training program. The availability of individual training sources for each unit may be dependent on course availability, unit budgets, etc.

   d. The Coast Guard Cyber mission sets are diverse; therefore, Coast Guard commands and units conducting cyber operations are diverse in skill requirements and capabilities. This Chapter shall serve as governing authority in creating standards for the development of Coast Guard cyberspace work roles while allowing flexibility at the unit level in how to meet the standard.

C. Unit Training Program.

1. Introduction. A worthwhile unit training program is realized through the dedicated efforts and commitment of all unit personnel. It begins with the Commanders, Commanding Officers, and Officers in Charge who must provide appropriate levels of "command emphasis" to ensure a viable training program. Implementing that program then becomes largely an all-hands responsibility. The training program for Coast Guard cyberspace work roles involves two essential elements: (1) qualification, and (2) certification.

   a. Qualification. The Cyber Operations Qualification element represents the continuation of the training and professional development of cyberspace work-roles to meet a particular qualification standard. The qualification process generally includes a written form of personnel qualification standards (PQS), required courses and schools, on-the-job experience, and a qualification examination board.

b. Certification. The Cyber Operations Certification element represents the Command-level process undertaken to affirm that a watch standing candidate truly meets the standards established within the qualification process and that the individual possesses a level of technical competency, experience, judgement, and maturity required for the position.

D. Training Program Written Guidance.

1. Policy. Each unit conducting cyberspace operations shall maintain written guidance for their Training Program that, at a minimum, addresses the following.

a. Internal procedures and guidelines concerning the conduct of the Unit Training Board, including the required frequency of meetings.

b. Unit Training Board memberships by name and position title.

c. Qualification Examination Board (QEB) memberships by name and position/title.

d. Qualification expectations/timeframes for each cyberspace work-role position.

e. Processes for successful completion of PQS tasks.

f. Processes for practical evaluation of trainees (i.e., scenario-based knowledge evaluation, technical performance evaluation, etc.).

g. Processes for requesting and completing required training required per the PQS.

h. Processes for conduct of QEBs per prescribed procedures.

i. Procedures for development of the Unit Training Plan.

E. Unit Training Board.

1. Unit Training Board Requirement. All commands and units conducting cyberspace operations shall establish individual Unit Training Boards and may choose to establish specialized training boards within departments, divisions, or branches of the command or unit. Responsibilities of these boards shall include:

a. Prepare the individual training plan to establish training policies and priorities; define the unit needs and specify training objectives to meet mission and training requirements.

b. Perform periodic review of Coast Guard promulgated PQSs, Job Qualification Requirements (JQR), and other training standards for accuracy and relevance to cyber missions.

c. Supervise and control training and periodically review and modify training policies and programs to adapt to changing needs and conditions.

d. Manage the training plan by scheduling training and exercise periods and professional development training.

F. Qualifications.

1. General. Cyber personnel require thorough training to function as a safe, competent, and effective in a specific cyberspace work-role. All individuals assigned to a billet aligned to a cyberspace work-role shall undergo a qualification process to certify for the specific position.

a. Commanders, Commanding Officers, and Officers in Charge of units conducting cyber space operations are responsible for establishing a qualification process that requires completion of relevant USCYBERCOM and Coast Guard Cyber PQSs, appropriate on-the-job training, timely assignment to "C" school or advanced training required for the cyberspace work-role position, and a qualification examination board.

b. US Cyber Command & The Office of Cyberspace Forces, Commandant (CG-791), have established comprehensive PQSs to support the qualification process for all cyberspace work-roles. Commands shall use the requirements listed in the various Cyber PQSs towards qualification. Trainees shall satisfactorily complete the applicable cyberspace work-role PQS for which the trainee is being qualified. Units conducting cyberspace operations shall not edit or alter the required PQS for any reason.

c. Units shall not edit or alter the required PQS promulgated by USCYBERCOM or CG-791. Units conducting cyberspace operations have the authority to promulgate additional requirements necessary to address operational needs for qualification for specific cyberspace work-role positions. Commands and Units that promulgate additional requirements to address mission or operational needs shall add these requirements to the required PQS as a separate appendix or annex.

2. Qualification Definitions.

a. The Cyber Operations Qualification Program: The Cyber Operations Individual Qualification Program is a continuous cycle that results in qualifications, removal of qualifications, and re-qualifications.

b. Personnel Qualification Standards (PQS): A PQS is a compilation of minimum knowledge tasks and skills an individual must demonstrate to qualify to stand watches or perform other specific routine duties necessary for them to perform securely, within assigned authorities, and maintain ethical responsibilities while correctly accomplishing responsibilities within the cyber watch team.

c. Job Qualification Requirements (JQR): A JQR is an additional list of specific tasks required by the Commanding Officer or Command-Designated Authority for qualifying on a watch station or work role or performing a specific task. A JQR can be used to augment existing PQS to tailor specifically to a command's needs, create a qualification process for a work role that has no applicable PQS, and/or fulfill immediate operational needs of the cyber mission.

d. Work Role Qualifiers: Work Role Qualifiers for PQS and JQRs are acknowledged experts in a specific area or qualification. Qualifiers are entrusted with protecting the integrity of the Cyber Operations Individual Qualification system by guiding trainees to references and not simply giving away answers or signatures. At a minimum, a qualifier is certified up to and including the work role they are authorized to sign off.

e. Qualification: A qualification is the official endorsement of the Command-Designated Representative that a member possesses the minimum required knowledge and skill for the position or designation. In the case of PQS, the minimum requirement to be a candidate for certification is a passing test score, demonstration of competency in the required qualification tasks and successful completion of an oral board.

f. Removal of Qualification: Removal of Qualification is the loss of a qualification due to security violation, permanent change of station, failure to meet currency requirements, revocation, or command discretion.

g. Requalification: Requalification consists of the steps a member must take to regain command authorization to serve in an assigned work role for which the member was previously qualified.

h. Currency: Currency is the completion of qualification tasks designated to be repeated at a specific interval to build and maintain certification in a specific work role.

G. Qualification Examination Board (QEB).

1. General. Prior to becoming certified in a cyberspace work-role position, a Qualification Examination Board (QEB) shall evaluate a prospective candidate for a cyberspace work-role. The primary function of the QEB is to conduct comprehensive knowledge and technical competency evaluations and recommend prospective candidates for a cyberspace work-role for certification in a cyberspace work-role position. The QEBs are responsible for the administration of these comprehensive knowledge evaluations and serves as the quality control for cyberspace work-roles.

2. Responsibilities. Commands and units conducting cyber operations shall establish and maintain a QEB for each cyberspace work-role with the following responsibilities:

a. Evaluates the candidate's leadership, ability, judgement, maturity, technical competence, and knowledge.

b. Evaluates the candidate's knowledge regarding policies, procedures, mission specific knowledge, technical skill, and risk management standards and concepts.

c. Verifies all requirements of the qualification process have been successfully completed in the manner prescribed by qualification guides, PQS, and this Instruction.

d. Makes recommendations to the Commander, Commanding Officer, or Officer in Charge for certification.

e. Provides guidance to the members for additional training, if needed.

f. Advises the Commander, Commanding Officer, or Officer in Charge on matters pertaining to the qualification process.

g. Evaluates the full scope of the mandated Cyber PQS and JQR during the QEB process.

3. Board Composition. The Unit Training Board shall promulgate QEB membership for each cyber-space work role.

4. Checklists. The QEB should prepare and use standard QEB checklists to assess the required knowledge and skill identified in the PQS and JQR for each given cyberspace work role. The use of QEB checklists during the board ensures the board is consistently and uniformly evaluating prospective watch-standers. The Unit Training Board shall govern all QEB checklists.

5. Recommending Certification. Once a candidate has completed the QEB, the board shall document the results in the Cyber training system of record. If the QEB does not recommend the prospective cyberspace work-role for certification, the QEB shall state why and what areas of knowledge, technical skill, or performance were not acceptable. The QEB should discuss specific recommendations for increased training and/or practical experience for the prospective candidate for a cyberspace work-role.

H. Interim Qualification. Commanders, Commanding Officers, and Officers in Charge of units conducting cyberspace operations shall not designate cyberspace work-role with an interim qualification. Commands or Units unable to meet this standard shall seek guidance from their chain of command on how to provide for continuity of operations.

I. Trainee Status. Commands and units shall not use personnel in a trainee status to work as, or substitute for, a certified member in the cyberspace work-role. Commanders, Commanding Officers, and Officers in Charge of units conducting cyberspace operations shall ensure expected qualification timeframes are outlined in appropriate training program written guidance and communicated to trainees prior to the commencement of qualification.

J. Certification.

1. General. The certification process is where the Commanders, Commanding Officers, and Officers in Charge of units conducting cyberspace operations takes an individual's maturity, technical competence, and judgement into account. The Commanders, Commanding Officers, and Officers in Charge shall consider members for certification for cyberspace work-role only after they have successfully completed the qualification process outlined in this Instruction. Final written certification from the Commanders, Commanding Officers, and Officers in Charge is required for all cyberspace work-roles. Final certification is the official statement of the Commanders, Commanding Officers, and Officers in Charge of units conducting cyberspace operations that the member has demonstrated:

   a. The minimum required knowledge and skill for the cyberspace work-roles as evident by the completed PQS, knowledge evaluation, skill evaluation, and positive recommendation of the QEB.

   b. The judgement and maturity required to act responsibly.

   c. The judgement and maturity required to perform assigned duties in the manner prescribed by Coast Guard and USCYBERCOM directives and regulations.

   d. The ability to function as a team member.

   e. The capacity to interact positively with the public in the execution of Coast Guard duties.

K. Revoking Certifications.

1. Guidance. Commanders, Commanding Officers, and Officers in Charge shall rescind certification when members do not maintain USCYBERCOM or Commandant standards for certification or fail to meet cyberspace work-role position specific currency or training standards.

2. Authority. Commanders, Commanding Officers, and Officers in Charge have the authority to revoke the certification(s) of any individual attached to the respective command or unit. Commanders, Commanding Officers, and Officers in Charge shall rescind certification upon loss of trust or confidence in the member's ability to perform assigned duties. Members may be allowed to recertify at the discretion of the Commander, Commanding Officer, or Officer in Charge.

L. Decertification. Due to the complexity and diverse nature of the various Coast Guard cyberspace work-role skillsets, each Unit Training Board shall promulgate standards for decertification. Decertification should normally occur during a permanent change of duties or extended period away from the cyberspace work role. All decertification standards shall receive concurrence from Commandant (CG-791) and be aligned with USCYBERCOM policy.

M. Responsibility.

1. Commandant (CG-791).

a. Establishes overall policy for the Cyber Individual Qualification Program.

b. Sets requirements and standards and oversees and evaluates the Cyber Individual Qualification Program.

c. Establishes priorities for the Cyber Individual Qualification Program.

d. Reviews training plans/requirements for new cyber operational commands or systems to ensure requirements for the cyber individual qualification program are identified and scheduled.

e. Plans and programs for the resources necessary to operate and administer the cyber individual qualification program.

f. Approves all PQS materials prior to distribution.

g. Approves urgent changes to cyber individual qualification tools to meet emergent requirements.

h. Issues messages to the cyber forces regarding new, updated or deleted cyber qualifications.

i. Uses the Department of Defense Cyber Workforce Framework (DCWF), along with other appropriate references, to develop a DoD cyberspace workforce with a common understanding of cyberspace concepts, principles, and applications.

j. Requires that USCG personnel filling cyberspace workforce positions are qualified to perform these duties and that they operate in coordination with stakeholders.

k. Reviews and updates KSAs of the cyberspace workforce on a continuous basis.

l. Implements a cyberspace workforce development and sustainment process comprised of foundational (i.e., education, training, personnel certification, or experience qualification alternatives); resident; and Continuous Professional Development (CPD) requirements.

2. CGCYBER.

   a. Implements and manages cyber individual qualification and certification processes in accordance with this guidance.

   b. Ensures Officers/Petty Officers acting in the capacity of a work role qualifier be E-5 or above and certified in that work role, designated in writing, and made known to all members of the Command.

   c. Acknowledges all cyber individual qualifications and signs all work role qualifications or work role via individual or blanket qualification letters.

   d. Ensures timely entry of all completion/certification data into TMT or DA.

   e. Ensures current records of all certified watch standers are kept current.

   f. Maintains Unit Training List (UTL).

N. Department of Defense Cyber Workforce Framework (DCWF).

1. Guidance. CGCYBER and CG-791 shall maintain the Coast Guard's Cyberspace Workforce Structure per DoD Manual 8140.03 for military, civilian, and contract personnel. The DoD cyberspace workforce structure is based on work roles outlined in the Department of Defense Cyber Workforce Framework (DCWF). The DCWF includes work performed by the entire cyberspace workforce, to include personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources, conduct related intelligence activities, enable future operations, and project power in and through cyberspace in accordance with DoD Directive 8140.01. Each cyberspace work role will include an associated qualification matrix. The qualification matrix will identify the relevant options available to achieve qualification as described in this section and illustrated in Figure 3 below. Additional information regarding the location and management of these matrices can be found on the DoD Cyber Exchange site (DoD Cyber Workforce Qualification Matrices).

		Proficiency Levels		
		Basic	Intermediate	Advanced
Foundational Qualification Options – Demonstration of knowledge	Education	Option -or-	Option -or-	Option -or-
	Training	Option -or-	Option -or-	Option -or-
	Personnel Certification	Option	Option	Option
Foundational Qualification Alternative	Experience	Conditional Alternative	Conditional Alternative	Conditional Alternative
Residential Qualification – Demonstration of Capability	On-the-Job Qualification	Always Required	Always Required	Always Required
	Environment Specific Requirements	Component Discretion	Component Discretion	Component Discretion
Current with technology, hostile actor tactics	Continuous Professional Development	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.

Figure 3 - Sample Work Role Qualification Matrix

Chapter 5. Cyber Training Quota Allocation Process

A. Purpose. This Chapter establishes the roles and responsibilities and outlines the process to secure sufficient Class "C" School and Advanced Training quotas to maintain a professional workforce that is fully trained prepared to protect and defend the Coast Guard and the nation in cyberspace.

B. Roles and Responsibilities.

1. FORCECOM-T. CYBER Portfolio Training Manager.

2. Commandant (CG-791). Program Manager for Cyber Training Program. Communicates the program's training needs to FORCECOM and aligns resources to support CYBER training.

3. CYBER Unit Training Board. Identifies and prioritizes training requirements for CGCYBER personnel.

4. CGCYBER Training Officer. Manages CYBER Unit Training Board in accordance with Reference (e) and Chapter 2 of this Instruction.

5. FORCECOM ETQC. Enters orders in Direct Access for members and slates individual personnel to attend courses in DoD systems of record.

C. Process.

1. FORCECOM. Regularly meets with CG-7911 to validate the number of quotas needed for courses identified by Reference (f) and Chapter 3 of this document as Class "C" Schools.

2. CGCYBER Training Officer.

   a. Aggregates training needs forecast from the Cyber Unit Training Board and submits prioritized training requirements to CG-791 who validates training quota requirements.

   b. Submits training quota requirements through CG-791 for upcoming FY to FORCECOM Cyber Portfolio Training Manager.

   c. Assigning Personnel to Training Billets.

   d. Provides candidates to ETQC to fill open training quota.

   e. Updates the Cyber Billet Allocation spreadsheet with course attendee information.

D. Administrative Tasks.

1. Commandant (CG-791).

   a. Maintains the CYBER Training TEAMS site.

   b. Develops and maintains the Cyber Billet Allocation spreadsheet.

   c. Develops resource training requirements according to stakeholder input.

Chapter 6. Cyber Training Allowance Billets

A. Purpose. This Chapter establishes roles and responsibilities and outlines the process for member allocation to Cyber Training courses.

B. Roles and Responsibilities.

1. FORCECOM.

   a. Assigned as the Training Manager for all courses contained in the CYBER Portfolio.

   b. Manages Cyber Training billets allocated to the Coast Guard by the U.S. Navy (See Appendix C), U.S. Army (See Appendix B & C) and other training opportunities such as JCOPC.

2. Commandant (CG-791).

   a. Program Manager for Cyber Training Program.

   b. Program Manager for U.S. Army and U.S. Navy sponsored Cyber training courses. (See Appendix B & C).

   c. Serves as Course Manager for all Cyber training courses (See Appendix B & C).

   d. Oversees the execution and resolution of the administrative requirements for all students attending a cyber training course.

   e. Facilitates bi-weekly coordination meetings to allocate training quotas to individuals.

3. CGCYBER. Assigns CGCYBER Training Officer, Assistant Training Officer, and Cyber Special Security Officer (SSO).

4. EPM-2 (Assignment Officer). Enters orders in Direct Access for members attending cyber training courses either U.S. Navy or U.S. Army sponsored.

5. CG-PSC. Issues orders, PCS or TDY, for personnel attending training.

C. Process.

1. Prioritization – Six Months prior to class convening date.

   a. CG-791, FORCECOM, and CGCYBER meet bi-weekly to identify and prioritize members for course offerings. FORCECOM will provide CG-791 and CGCYBER with training availability.

   b. CG-791 submits a consolidated listing of preferred member enrollment to ETQC.

2. Enrollment and Orders – 3 Months prior to class convening date.

   a. ETQC coordinates with the Program Managers to collect members' information, enters in the DoD system (ENTRS), and enrolls student in Direct Access (DA).

   b. FORCECOM and CGCYBER, tracks students' enrollment to ensure proper billeting of Coast Guard personnel.

   c. ETQC will advise when members are scheduled and communicate to the detailers (EPM-2) orders are ready to be issued, giving CG-791 and CGCYBER visibility.

   d. EPM issues orders to students, giving CG-791 and CGCYBER visibility.

   e. CGCYBER SSO verifies clearance information and sends it to the training commands, Security Office, and USCG Student Liaison.

   f. CG-791 updates tracking spreadsheet to indicate prerequisite administrative actions have been completed for members' training.

3. Prerequisites – 1 Month prior to class convening date. Member completes/confirms prerequisite requirements for course.

4. Student Arrival. Coast Guard support personnel (instructors and/or administrative staff) assigned to Corry Station and Ft Eisenhower ensure students are onboarded and complete all command specific arrival requirements/processes.

5. During Course.

   a. If a member is not on track to complete their course academically, the Training Command will provide updates to CG-791. CG-791 notifies EPM to begin assignment decisions.

   b. Members must complete the Class "A" school pipeline to complete their transition to CMS. If for any reason a member is disenrolled prior to successful completion, they will be returned to their previous rating and made eligible for orders.

   c. If a student is recycled, that allocated seat is lost and the student assigned to it must be reassigned. FORCECOM or CGCYBER will initiate the process to move their student to a new seat.

Appendix A. List of Acronyms

Table 1- List of Acronyms

ATO	Assistant Training Officer
C3TF	Command, Control, and Cyber Task Force
CGBI	Coast Guard Business Intelligence
CGTTP	Coast Guard Tactics, Techniques, and Procedures
CISA	Cybersecurity and Infrastructure Security Agency
CM	Cyber Course Manager
CMM	Cyber Mission Manager
CMS	Cyber Mission Specialist
CMT	Cyber Mission Team
COAB	Cyber Operational and Assessment Branch
COS	Cyber Operations Specialist
CPT	Cyber Protection Team
CQEB	Cyber Qualification Examination Board
CSOC	Cybersecurity Operations Center
CSSP	Cybersecurity Service Provider
CTT	Cyber Training Team
CWO	Chief Warrant Officer
DA	Direct Access
DCMS	Deputy Commandant for Mission Support
DCO	Deputy Commandant for Operations
DCO	Defensive Cyber Operations
DISA	Defense Information System Agency
DODIN	DoD Information Network
EMP	Enterprise Mission Platform
EPM	Enlisted Personnel Management
ETQC	Education and Training Quota Management Center
ETR	Electronic Training Request
JCAC	Joint Cyber Analyst Course
JQR	Job Qualification Requirements
KSA	Knowledge, Skills, and Abilities
LMS	Learning Management System
LOE	Lines of Effort
METL	Mission Essential Task List
MT	Mandated Training
MTL	Master Training List
MTS	Maritime Transportation System
NOSC	Network Operations and Security Center
OCO	Offensive Cyber Operations
PCS	Permanent Change of Station
PCS	Personnel Service Center
PM	Program Manager

PMO	Program Management Office
PQS	Personnel Qualification Standards
RFD	Requirements Front Door
RFMC	Rating Force Master Chief
RKM	Rating Knowledge Manager
RSI	Readiness and Security Inspection
TMB	Technical Management Branch
TMT	Training Management Tool
TPC	Training Program Codes
USCYBERCOM	United States Cyber Command
UT	Unit Training
UTB	Unit Training Board
UTO	Unit Training Office
UTPO	Unit Training Petty Officer
WQS	Watch Station Qualification Standards

Appendix B. Cyber Mission Specialist Class “A” Schools

Table 2- Class "A" Schools

Course Title	Course Description
Cyber Operations Specialist (COS) (Phase 1)	COS Phase I prepares the Cyber Mission Specialist (CMS) to ensure the freedom of maneuver within the cyberspace domain and deny the same to adversaries. The CMS enables Offensive Cyberspace Operations (OCO) intended to project power by the application of force in and through cyberspace by targeting enemy and hostile adversary activities and capabilities. The CMS enables Defensive Cyberspace Operations (DCO) to protect data, networks, net-centric capabilities, and other designated systems by detecting, identifying, and responding to attacks against friendly networks. The CMS will conduct OCO and DCO integrated and synchronized with other lethal and nonlethal actions to enable commanders to mass effects and gain advantages in cyberspace and across other domains which directly or indirectly support objectives on other operational domains by employing devices, computer programs, or techniques, including combinations of software, firmware, or hardware designed to create an effect in or through cyberspace.

Appendix C. Cyber Mission Specialist Class "C" Schools

Table 3- Class "C" Schools

Course Title	Course Description
U.S. Army Sponsored Training	
Cyber Operations Specialist (COS) Phase 2	COS Phase 2 consists of Cyber Common Technical Core, Cyber Protection Team Methodologies, Offensive Cyberspace Operations Analysis, and immersive, team-based Cyberspace Operations (CO) exercises. Graduates will possess foundational and intermediate knowledge, skills, and abilities for conducting CO on Windows, Unix, and Linux operating systems, as well as utilizing networking fundamentals and security concepts. Additionally, graduates will be able to fill entry-level positions on both offensive and defensive Cyber Mission Forces teams.
Cyber Common Core Technical Core (CCTC)	Provides enlisted, officer, and civilian personnel with intermediate skills in Cyberspace Operations involving the analysis, exploitation, and remediation of Windows, Linux, Networking, and Security systems. Course Outcome: Upon completion of this course, the student will possess the necessary technical knowledge and skill required to perform network analysis of Windows and Linux-based systems and provide recommended solutions to reduce network vulnerabilities.
Title 10 Interactive On-Net Operator (T10 BOC/ION)	This course includes education and training on the following functional areas topics to include Linux Fundamentals, Windows Fundamentals, Exploitation Methodology, Army Cyber Operations, and Operational Planning
Cyber Operations Planner Course (COPC)	The Cyber Mission Force (CMF) operators will demonstrate the ability to plan and brief Cyber Operations (CO); define, plan, and advise for Defensive Cyberspace Operations (DCO); define, plan, and advise for Offensive Cyberspace Operations (OCO); define Cyber Mission Force (CMF) structure and organizations; define, plan, and advise for cyber support to the USCG enterprise; and demonstrate a proficiency to target in Cyberspace.
Cyber Effects Application Course (CEAC)	Designed to educate Cyber personnel on intrinsic aspects of targeting in cyberspace. Using the Joint Targeting Cycle as the framework for the course, CEAC emphasizes characteristics of targeting in cyberspace that are doctrinally unique and/or require an amended process not codified in joint targeting doctrine.
Mission Commander Course	Consists of an overview of cyber mission force organizations and structure, authorities, collection requirements, mission profiles, capabilities, joint planning process, targeting, mission planning, operation procedures, operational tools, tactical planning, and a final capstone. At the end of the course, students are prepared to lead National Mission Teams and Combat Mission Teams in cyberspace operations.

Course Title	Course Description
U.S. Navy Sponsored Training	
Joint Cyber Analysis Course (JCAC) (Alternate Class "A" School)	Trains enlisted personnel (E1-E8), in the knowledge, skills, and abilities required to perform technical network analysis in the functional areas of Cyberspace Operations to the apprentice level. Duties and tasks are performed using appropriate references under moderate supervision.
Cyber Defense Analyst - Basic	Designed to prepare Cyber Analysts, (Military E1-O3, DoD, US Coast Guard, and Government Civilians) with the basic cyber methodologies required for Defensive Cyber Operations (DCO) and Cyber Protection Team (CPT) operations. Trainees will learn to perform risk management, analyze architectures, conduct vulnerability assessments, perform threat mitigation, conduct security audits, monitor environment, analyze traffic, respond to threat activity, develop, and implement countermeasures, and conduct media and malware analysis. Graduates are expected to perform to the proficiency level of apprentice, with limited supervision.
Cyber Defense Analyst - Host	Designed to prepare Cyber Analysts, (Military E1-O3, DoD, US Coast Guard, and Government Civilians) with the basic cyber methodologies required for Defensive Cyber Operations (DCO) and Cyber Protection Team (CPT) operations. Trainees will learn to perform risk management, analyze architectures, conduct vulnerability assessments, perform threat mitigation, conduct security audits, monitor environment, analyze traffic, respond to threat activity, develop, and implement countermeasures, and conduct media and malware analysis. Graduates are expected to perform to the proficiency level of apprentice, with limited supervision
Cyber Defense Analyst – Network	Designed to prepare joint Defensive Cyber Operations (DCO) Cyber Protection Team (CPT) analysts (Military E1-O3, DoD, US Coast Guard, and Government Civilians) with the basic knowledge and skills required to support CPT mission element roles. Trainees will be trained to support the four primary duties: hunt, enable hardening, clear, and assess. Graduates are expected to perform to the proficiency level of apprentice, with limited supervision.
Cyber Threat Intelligence Analyst	Designed to prepare Intelligence Analysts (E3-E8, DoD and US Coast Guard civilians) to support Cyberspace Operations. Trainees will learn to implement defensive and offensive cyberspace mission tasking, collect and process intelligence for the generation of intelligence products to satisfy cyberspace intelligence requirements and Essential Elements of Information (EEIs), develop target packages to support Cyberspace Operations, and disseminate cyber intelligence information via briefings, written reports, and messages. Graduates are expected to perform at the journeyman level with limited supervision.

Course Title	Course Description
USCYBERCOM Sponsored Training	
Joint Cyberspace Operational Planners Course (JCOPC)	Managed and offered by USCYBERCOM J7. JCOPC is presented at the FVEY level to Combatant Commands (CCMD) and Cyber Centers of Excellence in response to their specified training requirements. The course curriculum covers a variety of topics of interest to help staff build and integrate cyberspace operations into the overall planning process. Topics range from the Joint Planning Process (JPP), Joint Intelligence Preparation of the Operational Environment (JIPOE), Information Operations (IO), Special Technical Operations (STO), OPLANS/OPORDERS, Targeting/ Joint Fires, and Legal considerations. Additionally, the course will facilitate staff action at the joint level to provide training on USCYBERCOM business processes, DODIN Operations, DCO and OCO.

Appendix D. Cyber Voucher Program

A. Training Sources.

1. General. Multiple resident and online course providers are available to prepare members for certification exams, many of which are provided free of charge. Force Readiness Command (FORCECOM) provides foundational and advanced performance-based training, working with CG-7911, based on the requirements of certain cyberspace work roles. Additionally, The Office of Cyberspace Forces (CG-791) holds a limited number of on demand training licenses as well as seats in instructor-led classes. Specific guidance on applying for sponsored training, as well as a list of subsidized and free training sources, can be found on the Commandant (CG-791) Portal page. Training not available from the above sources is not centrally funded but may be available on a unit-funded basis. For courses with limited availability, priority will be given to members in cyberspace coded billets that require training and certification to meet billet requirements. However, all interested parties are encouraged to request access to training courses. Members should consult the Commandant (CG-791) Portal page for additional guidance on training requests.

B. Funding For Exams.

1. General. The Office of Cyberspace Forces (CG-791) manages the cyberspace workforce certification program and the Annual Maintenance Fee (AMF) process for the payment or reimbursement of fees associated with Workforce certifications. Pending available resources, Coast Guard military and civilian Cyberspace Workforce personnel and Coast Guard Academy cadets enrolled in cyber courses may request vouchers for professional certification exams and associated AMF. Commandant (CG-791) does not fund training or exam vouchers for contractors.

    a. All requests for vouchers and/or AMFs must be submitted via electronic request located on Commandant (CG-791) CG-Portal page. The electronic request must be completed in its entirety and have Supervisor/Department Head approval.

    b. All voucher requests for initial certification exams must be accompanied by a certificate of preparatory class completion or verification that course has been scheduled if planning to take the exam immediately after the course ends.

    c. Only one exam voucher can be requested for the candidate's current Cyber role. If the requestor advances, transfers, or changes positions and requires an additional certification, the requestor may submit a request for another voucher.

    d. An exam must be chosen from the required competency level. No waivers will be accepted.

    e. If a member is at their first unit following IT "A" school and was given a voucher for CompTIA A+ or Network+, that member is not authorized to receive another voucher until advancing to E-5.

f. Commandant (CG-791) will review member certification and competency information in DA prior to issuing vouchers. Members are expected to ensure DA is up to date with relevant information.

g. Each member will normally be afforded one Coast Guard-funded exam per competency to complete a single certification exam meeting the member's current role and competency requirements. The member is responsible for any additional testing attempts.

h. If a member's current role and competency requirement can be fulfilled with their choice of multiple certifications, Commandant (CG-791) will only provide a voucher and/or AMF for one of the certifications This includes testing vouchers received as part of Commandant (CG-791) procured instructor-led training.

i. Upon completion of the Coast Guard-funded exam, members will provide exam results via email to HQS-SMB-CG-7911@uscg.mil. Members will also provide their training officer and administrative division with a copy of their exam results for entry into the Training Management Tool (TMT) and DA.

j. If a member does not pass the initial Coast Guard-funded exam, subsequent attempts for initial certification will be the sole responsibility of the member. However, if a member does retake and pass the examination, they may submit a Claim for Reimbursement for Expenditures on Official Business, Form SF-1164, to Commandant (CG-791). Reimbursement for subsequent attempts will be subject to Commandant (CG-791) approval and will be based on available funds.

k. Certification testing and maintenance fees for military and government employees may also be funded by the member's unit. The member or the member's unit may fund travel for training or testing. Members are encouraged to choose a training or exam site within local travel distance.

C. Position Competencies. Units are encouraged to routinely review the competencies required by their Cyberspace Workforce positions. Rather than submitting a Request to Assign Competencies, Education, or Officer Specialty to a Position, Form CG-5311 for each position requiring updates, units may use the supplemental spreadsheet posted on the CG Portal Site to update competencies for multiple positions. Contact Commandant (CG-791) for additional information.

D. Continuing Professional Education. Multiple free sources exist for members to attain the Continuing Professional Education (CPE) hours required by certification authorities. If a member chooses to attain CPE hours through sources such as classes or conference attendance, funding will be at the discretion of the member's unit.