DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR COMBAT COMMAND
JOINT BASE LANGLEY-EUSTIS VA

ACCMAN17-2CVAHV1_ACCGM2024-01
26 FEBRUARY 2024

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FLDCOMs/FOAs/DRUs

FROM: ACC/A3
205 Dodd Blvd, Ste 121
Joint Base Langley-Eustis VA 23665-2789

SUBJECT: Air Combat Command Guidance Memorandum to ACCMAN17-2CVA/HV1

By Order of the Commander, Air Combat Command, this ACC Guidance Memorandum immediately changes ACCMAN 17-2CVAH Volume 1, *Cyber Vulnerability Assessment/Hunter (CVA/H) Training*. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other ACC publications, the information herein prevails, in accordance with DAFI 90-160, *Publications and Forms Management,* and DAFMAN 90-161, *Publishing Processes and Procedures*. This guidance is applicable to Air Force (AF) User Major Commands (MAJCOMs), Air Force Reserve Command (AFRC), National Guard Bureau (NGB), and third party governmental and contract support agencies in accordance with (IAW) appropriate provisions contained in support agreements and AF contracts.

This Guidance Memorandum brings ACCMAN 17-2 CVA/H V1 in line with current United States Cyber Command (USCYBERCOM) requirements and guidance for Cyber Protection Teams. It additionally aligns AF crew positions to USCYBERCOM work roles.

Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in the Air Force Records Management System.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon incorporation by interim change to, or rewrite of ACCMAN 17-2CVA/HV1, whichever is earlier.

DAVID G. SHOEMAKER, Maj Gen, USAF
Director of Operations

Attachment: Guidance Changes

Attachment

Guidance Changes

CYBERSPACE VULNERABILITY ASSESSMENT/HUNTER (CVA/H) – TRAINING

PURPOSE

This manual implements Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyber Warfare Operations, and references*, Air Combat Command Instruction (ACCI) 17-202 Volume 1, *Cybercrew Training*. It establishes the minimum Air Force (AF) standards for training and maintaining currency and proficiency for personnel performing crewmember duties on the Cyberspace Vulnerability Assessment/Hunter (CVA/H) weapon system. This publication applies to all Air Combat Command (ACC), AF Reserve Command (AFRC), National Guard Bureau (NGB), and third-party governmental and contract support agencies in accordance with (IAW) appropriate provisions contained in memoranda, support agreements, and AF contracts. Ensure that all records and processes prescribed in this publication are maintained IAW AFI 33-322, *Records Management and Information Governance Program*, and are disposed IAW the Air Force Records Disposition Schedule (RDS), located in the Air Force Records Information Management System. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination prior to certification and approval. Submit suggested improvements to this instruction on Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*, through command channels, to ACC/A3/2/6K. ACC will conduct publication reviews and/or revisions as necessary with other agencies as the Cyberspace mission expands. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, and T-3") number following the compliance statement. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures*, Attachment 10 for a description of the authorities associated with the Tier numbers. Waiver authority for non-tiered paragraphs remains with ACC/A3. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority. Compliance with **Attachment 1** is not mandatory.

Chapter 1

OVERVIEW/BACKGROUND

1.1. General. This manual prescribes policy and guidance for training CVA/H cybercrew members. Training policy, guidance, and requirements are set forth for each phase of crew training. The objective of training should be the progressive development of CVA/H crew readiness. This manual applies to all CVA/H cybercrew members, defined as individuals assigned to utilize the CVA/H weapon system in the achievement of tasked mission objectives and designated a specific crew position. Additionally, for the purposes of this manual and for uniformity with United States Cyber Command (USCYBERCOM) guidance, the term "crew position" will be synonymous with "work role." This manual also applies to members in formal training for immediate assignment to a CVA/H weapon system position. For any publications referenced in this manual, contact ACC/A3/2/6K.

1.2. Program Goals. The overall objective of the CVA/H training program is to develop and maintain a high state of readiness for the immediate and effective employment across a full range of military operations. Mission readiness and effective employment are achieved through the

development and mastery of core competencies for each of the crew positions aligned to the CVA/H weapon system.

1.3. Roles and Responsibilities.

1.3.1. ACC will:

1.3.1.1. Develop and manage, in coordination with affected commands, the appropriate guidance to establish cybercrew training requirements and standards IAW ACCI 17-202V1 and AFI 10-217, *Management of Air Force Operational Training and Undergraduate Aircrew Training Systems*.

1.3.1.2. Chair annual Training Planning Team (TPT) to review training requirements and programs for currency, applicability, compliance, and effectiveness and address issues in lead command-provided guidance documents as appropriate. Conference members should include representatives from Squadron Training, Weapons and Tactics, Standardization and Evaluation (Stan/Eval), Operations, Formal Training Unit (FTU), Program Management Office (PMO), and other areas as required.

1.3.1.3. Publish a Ready Cybercrew Program (RCP) Tasking Memorandum (RTM) annually prior to the start of the fiscal year. The RTM may contain supplemental training requirements or updated guidance.

1.3.1.4. Determine total force cybercrew training requirements in coordination with using Major Commands (MAJCOMs), NGB, and AFRC across Future Years Defense Program by forwarding requirements annually to Headquarters (HQ) ACC/A3/2/6K.

1.3.2. Numbered Air Forces (NAF) employing CVA/H will:

1.3.2.1. Maintain oversight of cybercrew training within its chain of command and for attached units.

1.3.2.2. Convene conferences and working groups, as necessary, to review and improve training policies and procedures.

1.3.2.3. Validate, approve, and provide guidance on the implementation and use of the master training task list (MTTL) items. NAFs will coordinate MTTLs with HQ ACC. **(T-2)**

1.3.2.4. Coordinate on the RTM. **(T-2)**

1.3.3. Wings or Groups employing CVA/H will:

1.3.3.1. Be responsible for managing the Wing's Operations Training program. In Wings or Groups with an Operations Support Squadron (OSS), an A staff that performs OSS-like functions, or equivalent organization, a training office will be manned with a Chief of Training and at least one instructor per cybercrew position IAW **paragraph1.3.5.3.2**. **(T-3)**

1.3.3.2. Forward an RTM training report to ACC/A3/2/6K every 6 months during the training cycle (on the 15th day of April and October IAW the RTM). Squadrons may submit an out of cycle report any time Higher Headquarters (HHQ) assistance is required. When preparing all reports, units will use the most current guidance/templates found on the ACC/A3TO SharePoint page.

1.3.3.3. Assist the Air Reserve Component (ARC) unit training programs as required or requested IAW applicable unit support programs, memorandums of agreement, or memorandums of understanding.

1.3.4. The Wing Chief of Training will:

1.3.4.1. Maintain Combat Mission Ready (CMR) status and be a qualified instructor in at least one crew position in the CVA/H Weapon System. **(T-3)**

1.3.4.2. Be responsible for leading training development efforts and standardizing training material and programs across the Wing and/or Group.

1.3.4.3. Develop programs to ensure training objectives are met.

1.3.4.4. Assist subordinate units in management of training programs to ensure programs meet mission needs and provide the necessary support.

1.3.4.5. Establish procedures for review, quality control, and approval of unit training documentation.

1.3.4.6. Implement the RCP and review/modify local implementation before the start of every fiscal year or upon publication of an out-of-cycle RTM. **(T-3)**

1.3.4.7. Ensure RCP events are oriented towards maintaining operationally relevant skills and tactical employment which simulate conditions anticipated in the unit mission. RCP event accomplishment is defined in the RTM.

1.3.4.8. Coordinate on the RTM.

1.3.5. Unit Training Organization:

1.3.5.1. Scope. For the purpose of this manual, “unit” includes levels of organizations under HHQ required to establish a training function. Most units are composed of cyber squadrons/detachments (henceforth in this publication, “squadron” will be used synonymously with “detachment”).

1.3.5.2. The Squadron Commander (SQ/CC) will:

1.3.5.2.1. Be responsible for the implementation of the squadron Cybercrew Training Program.

1.3.5.2.2. Ensure implementation of the unit-level training programs. **(T-3)**

1.3.5.2.3. Provide manpower to the unit training function to execute the duties directed by ACCI 17-202V1 and this volume. **(T-3)**

1.3.5.2.4. Designate cybercrew instructors. **(T-3)**

1.3.5.2.5. Ensure that all qualified instructors are awarded a “K” prefix to their Air Force Specialty Code.

1.3.5.2.6. Ensure cybercrews and individual cybercrew members are provided with adequate reconstitution time post-mission to enable completion of RCP requirements.

1.3.5.3. The Training Flight will:

1.3.5.3.1. Be administered and implemented from the unit level.

1.3.5.3.2. Be led by a Chief of Training who reports directly to the Director of Operations (DO).

1.3.5.3.3. Be staffed with a minimum of one qualified instructor for each cybercrew position. All instructors (including the Chief of Training) must maintain CMR status for the CVA/H cybercrew position for which they are aligned. **(T-3)**

1.3.5.3.4. Recommend candidates for instructor upgrade from the most suitable, highest qualified and most experienced personnel. Requisites for instructor upgrade are outlined in Chapter 4.

1.3.5.3.5. Process and maintain training records and forms in a MAJCOM-approved system IAW ACCI 17-202 Volume 2, *Cybercrew Standardization/Evaluation Program*, and ACCMAN 17-2CVA/H Volume 2, *Cyber Vulnerability Assessment/Hunter (CVA/H) Standardization/Evaluation Program*. An offline backup must be maintained, also.

1.3.5.3.6. Establish procedures for review and quality control of training documentation. **(T-3)**

1.3.5.3.7. Develop and document an instructor training program designed to train and prepare instructors for qualification. Instructor training programs must be reviewed and approved by the OSS prior to implementation and must meet the requirements of **Chapter 4**. **(T-3)** For units that do not have an OSS, complete approval through the supporting Group Commander or designated representative.

1.3.5.3.8. At least quarterly, provide a Status of Operations Training brief to unit leadership on unit cybercrew training statuses and requisite completion of Initial Qualification Training (IQT), Mission Qualification Training (MQT), and Continuation Training (CT) shortfalls, and missed suspenses.

1.3.6. Cybercrew members will:

1.3.6.1. Ensure records are transferred when changing units in order to maintain documentation of certification, qualification, and training. **(T-3)**

1.3.6.2. Complete training, currency, and proficiency requirements within the guidelines of this volume and applicable RTM. **(T-3)**

1.3.6.3. Only participate in cyber activities for which they are trained, qualified, or current unless under appropriate supervision.

1.3.6.4. Report any additional training gaps or shortfalls for required cyber activities to their supervision and training flight.

Chapter 2

GUIDANCE AND PROCEDURES

2.1. Qualification Training. This section defines CVA/H cybercrew operational statuses and outlines minimum training requirements for IQT, MQT, Upgrade Training, Special Mission Training (SMT), Difference Training, Senior Officer Qualification Training and Requalification Training (RQT) for all CVA/H cybercrew positions.

2.1.1. IQT. Formal training that is required to qualify for basic cybercrew duties in an assigned CVA/H crew position without regard for the unit's operational mission.

2.1.1.1. IQT Prerequisites. Prior to entering CVA/H formal training, trainees must complete required training courses as specified in the USCYBERCOM Cyber Mission Forces (CMF) Formal Training Pipeline for their assigned work role. Additionally, trainees must complete any prerequisites identified in the current CVA/H System Training Plan (STP), and the associated course syllabus. **(T-2)**

2.1.1.2. Method. The primary method of CVA/H IQT is to attend the FTU course(s) outlined in the CVA/H syllabus and listed in the Education and Training Course Announcement (ETCA)

system under United States Air Force (USAF) Formal Schools. ETCA can be reached via the Air Force Portal. **(T-3)**

2.1.1.3. In-Unit IQT. When formal course attendance is not practical or quotas are not available, units will request waivers to conduct in-unit IQT using formal school courseware. Accomplish in-unit training IAW applicable formal school courseware and the guidance contained in ACCI 17-202V1. **(T-2)**

2.1.1.4. IQT will be taught by qualified instructors as defined in **Chapter 4**.

2.1.1.5. Personnel in IQT will not have supervisory responsibilities or additional duties.

2.1.2. MQT. MQT is a unit-level formal training program developed IAW Instructional Systems Development (ISD) principles that prepares newly assigned cybercrew members to accomplish the unit's mission (see **paragraph 2.7** for operational statuses). This section prescribes the minimum training requirements to prepare individuals for qualification in their unit's missions and is provided to assist SQ/CCs in developing an MQT program.

2.1.2.1. MQT Pre-requisites. Each cybercrew member must complete all applicable IQT requirements IAW **paragraph 2.1.1** before entering MQT. **(T-3)**

2.1.2.2. Time Limit. The cybercrew member will begin in-unit MQT no later than (NLT) 45 days (90 days for the Air National Guard/Air Force Reserve) after completing IQT and reporting to a new duty station or unit. **(T-3)**

2.1.2.3. Method. The primary method of CVA/H MQT is to attend and complete an in-unit formal training course focused on unit-specific, mission-related training requirements. For all attendees, MQT will take priority over non-training related duties to include mission execution.

2.1.2.4. MQT will be taught by qualified instructors as defined in **Chapter 4**.

2.1.2.5. Mission-Related Training. Units will develop training addressing areas pertinent to the mission as determined by the SQ/CC. Mission-related training is informed by the mission, organizational concepts of employment, and other HHQ guidance. Additional mission-related training elements are addressed in Air Force Tactics, Techniques, and Procedures (AFTTP) 3-1, *Cyberspace Vulnerability Assessment/Hunter* (S//REL FVEY), AFTTP 3-1, *Advanced Cyber Threat Guide*, Chapter 13 (S//REL FVEY), AFTTP 3-1, *Integrated Planning and Employment* (S//REL FVEY), AFTTP 3-3, *Integrated Planning and Employment* (S//REL FVEY), AFTTP 3-3, *Cyberspace Vulnerability Assessment/Hunter* (U); AFTTP 3-3, *Integrated Planning and Employment* (U); USCYBERCOM Cyber Warfare Publication 3-33.4, *Cyber Protection Team (CPT) Organization, Functions, and Employment* (U); and other mission-related documents.

2.1.2.5.1. Operations Training Plan (OTP). Units will annually determine, review, and document MQT syllabi and other training requirements in an OTP. The OTP contains the knowledge, tasks, methods of training, and total training time (to include estimated and maximum training times and lapses between training and events). Schedule, conduct, and document MQT IAW the OTP. While MQT is mission specific, units will use standardized training whenever possible. Wings and/or Groups may develop a common, foundational OTP that Squadrons augment with additional mission specific training tasks. **(T-3)**

2.1.2.5.2. Mission Objectives. To develop OTPs, units must align mission objectives to and incorporate performance measures, mission essential tasks, and core functions outlined in USCYBERCOM Cyber Technical Manual (CTM) 7-0.2 (S//NF), *CMF Training and Readiness (T&R) Manual*, local area requirements, and procedures.

2.1.2.5.3. Specific Mission Tasks. Specific mission tasks are derived from mission objectives and include other relevant tasks determined by the unit. **(T-3)**

2.1.2.5.4. Mission objectives and tasks are minimum requirements for MQT. Additional training events based on gaps in student proficiency or training background or student non-progression should be made available within the constraints of the training plan and may be added at the SQ/CC's discretion. **(T-3)**

2.2. Upgrade Training. Cybercrew members pursuing a CVA/H upgrade position will complete Upgrade Training. **(T-3)**

2.2.1. The Certifying Official (CO) will determine and assign cybercrew members that will train for and maintain upgrade positions.

2.2.2. The CO will review and approve all Upgrade Training criteria. The Chief of Training will provide appropriate criterion to all candidates for upgrade.

2.2.3. Unless specifically prohibited or restricted by weapon system operating procedures, specific theater Operations Order (OPORD), or specific HHQ guidance, upgrade training may be conducted during operational missions with appropriate supervision and IAW instructor requirements found in **Chapter 4**. **(T-3)**

2.2.4. All Upgrade Training will be documented IAW **Chapter 5**.

2.3. Special Mission Training (SMT). SMT is given to cybercrew members obtaining a special mission qualification or certification on the CVA/H weapon system. SMT can also teach any special skill necessary to carry out the unit's assigned mission that is not required by every cybercrew member. Specialized training may consist of special tactics, weapon system capabilities, responsibilities, and operations on specific mission systems/terrain required to maintain proficiency.

2.3.1. Unless specifically prohibited or restricted by weapon system operating procedures, specific theater OPORD, or specific HHQ guidance, SMT may be conducted during operational missions with appropriate supervision by an instructor qualified/certified in the associated Special Mission Qualification (SMQ). **(T-3)**

2.3.2. Special Mission Training Plan (SMTP). Units will determine and document SMT syllabi and requirements in an SMTP. The SMTP contains the knowledge, tasks, methods of training, and total training time (to include estimated and maximum training times and lapses between training and events). Schedule, conduct, and document SMT IAW the SMTP. Units will use standardized training whenever possible. Wings and/or Groups may develop a common, foundational SMTP that Squadrons augment with additional special mission training tasks. **(T-3)**

2.3.3. The CO will determine and assign cybercrew members that will train for and maintain special mission qualifications.

2.3.4. The CO will determine and document any CT requirements needed to maintain special mission qualifications.

2.3.5. All SMT will be documented IAW **Chapter 5**.

2.4. Difference Training. Difference training will be required when major modifications or upgrades are made to the CVA/H weapon system.

2.4.1. HQ ACC will determine if a modification or upgrade to the CVA/H weapon system is deemed “major”.

2.4.2. Once a major modification or upgrade has been determined, the CVA/H PMO will develop and deliver Type 1 Training to the corresponding OSS (or equivalent organization), supporting Wings or Groups, and relevant Formal Training Units.

2.4.2.1. At a minimum, Type 1 Training will include product training (setup, configuration, operations, and teardown), training prerequisites, objectives, task lists, lesson plans/courseware, performance scenarios, and a train-the-trainer course to create initial cadre.

2.4.2.2. Type 1 Training time requirements will be included in the instructions delivered by the CVA/H PMO.

2.4.3. In Wings or Groups with an OSS (or equivalent organization), the OSS will determine what additional training, if any, is required beyond the Type 1 Training.

2.4.4. Difference Training will be integrated into unit OTPs.

2.4.5. Failure to complete difference training does not, by itself, disqualify members from maintaining CMR status. Untrained members, however, will not perform tasks associated with the new weapon system capabilities until trained, unless under the supervision of an instructor. **(T-2)**

2.4.6. All Difference Training will be documented IAW **Chapter 5**.

2.5. Senior Officer Qualification Training.

2.5.1. A Senior Officer is defined as a Deputy Group Commander or higher and must meet course entry pre-requisites as prescribed in **paragraph 2.1.1.5**. **(T-3)**

2.5.2. A Senior Officer in training, at the FTU or in-unit, is considered in a formal training status for the duration of the course. All non-training duties will be reassigned appropriately until training is completed. **(T-2)**

2.6. Requalification Training (RQT). RQT is any academic or positional training required to requalify to CMR status. IAW ACCI 17-202V2, a cybercrew member is considered unqualified upon expiration of the member’s required periodic evaluation or currency, whichever occurs first. The duration of unqualified time is measured from the date the cybercrew member became unqualified until the retraining start date.

2.6.1. A cybercrew member who is unqualified up to 6 months can requalify IAW ACCI 17-202V1 by accomplishing training in all delinquent items (as applicable) or performance of any additional training as directed by the CO. A Requalification Evaluation (RQ Eval) is required IAW ACCI 17-202V2 and ACCMAN 17-2CVA/HV2.

2.6.2. A cybercrew member who is unqualified for more than 6 months can requalify by re-accomplishing IQT and MQT or RQT and a RQ Eval IAW ACCI 17-202V2 and ACCMAN 17-2CVA/HV2. Applicable portions of MQT may be used to create a requalification program for cybercrew members who have been downgraded from CMR and/or Basic Mission Capable (BMC) statuses to specifically address the deficiencies which caused the downgrade.

2.7. CVA/H Cybercrew Operational Status. IAW ACCI 17-202V1, a cybercrew member may be assigned Basic Cyber Qualified (BCQ), CMR, BMC, Non-Combat Mission Ready (N-CMR), or N-BMC status.

2.7.1. BCQ. A cybercrew member who has completed their initial training and is being sent to their first operational unit. BCQ requirements:

2.7.1.1. Successful completion of all IQT requirements IAW **paragraph 2.1.1**.

2.7.1.2. Completed and certified USCYBERCOM Job Qualification Record (JQR) for target work role at the "Basic" proficiency level.

2.7.1.3. Individual currency (as applicable) IAW **paragraph 3.2**.

2.7.2. CMR. A CMR cybercrew member is available and qualified in the Squadron's mission. CMR requirements:

2.7.2.1. Successful completion of BCQ requirements IAW **paragraph 2.7.1**.

2.7.2.2. Successful completion of MQT requirements IAW **paragraph 2.1.2**.

2.7.2.3. Successful completion of Qualification Training (QUAL) and Mission (MSN) Evals IAW ACCI 17-202V2 and ACCMAN 17-2CVA/HV2.

2.7.2.4. Completed and certified USCYBERCOM JQR for target work role at the "Senior" proficiency level.

2.7.2.5. Individual currency (as applicable) IAW **paragraph 3.2**.

2.7.2.6. CMR-level proficiency standards IAW **Chapter 3** and the RTM.

2.7.3. BMC. A BMC cybercrew member is typically assigned to a MAJCOM, NAF, FTU, Group/Wing-level function, Direct Reporting Unit, and supporting unit that employs the CVA/H weapon system. BMC status is meant to ease continuation training requirements for individuals needing to maintain a CVA/H operational status that do not conduct operations as their primary organizational mission. BMC requirements:

2.7.3.1. Successful completion of BCQ requirements IAW **paragraph 2.7.1**.

2.7.3.2. Successful completion of MQT requirements IAW **paragraph 2.1.2**.

2.7.3.3. Successful completion of QUAL and MSN Evals IAW ACCI 17-202V2 and ACCMAN 17-2CVA/HV2.

2.7.3.4. Completed and certified USCYBERCOM JQR for target work role at the "Senior" proficiency level.

2.7.3.5. Individual currency (as applicable) IAW **paragraph 3.2**.

2.7.3.6. BMC-level proficiency standards IAW **Chapter 3** and the RTM.

2.7.3.7. CVA/H cybercrew members in BMC status must be able to attain CMR status within 30 days. **(T-3)**

2.7.4. Non-CMR (N-CMR)/Non-BMC (N-BMC). A cybercrew member that has been downgraded from CMR/BMC status and requires additional training IAW **paragraphs 3.2.4** and **3.3.4.1**.

2.7.4.1. Cybercrew members in a N-CMR/N-BMC status will only operate in a supervised status IAW ACCI 17-202V1. **(T-2)**

2.7.5. The decision to suspend, retain, or downgrade a cybercrew member's status for failure to meet standards established by this manual, ACCMAN 17-2CVA/HV2, or ACCI 17-202V1 and V2 will be documented by citing all standards that apply. **(T-2)**

2.7.6. The CO's certification as well as certification of completion of unit-designated crew force management is required to obtain CMR/BMC statuses. Upon certification, the cybercrew member maintains CMR/BMC status based on CT requirements IAW **Chapter 3** and ACCMAN 17-2CVA/H V2.

Chapter 3

CONTINUATION TRAINING

3.1. Continuation Training (CT). CT consists of two aspects. The first provides cybercrew members with regular repetitions of the basic operational skills necessary to ensure safe operation of the weapon system (i.e., currency). The second consists of regular repetitions of specific mission-related events required to accomplish the unit's assigned mission (i.e., proficiency). This manual and the current CVA/H RTM establish the minimum volume, frequency, and mix of cybercrew training requirements to maintain currency and proficiency in the assigned crew position and at designated certification/qualification levels. The SQ/CC will ensure each cybercrew member receives sufficient training to maintain individual currency and proficiency. **(T-3)**

3.1.1. CT Requirements. Completion and tracking of CT is ultimately the responsibility of the individual crewmember. Cybercrew members should actively work with their supervisors, unit schedulers, and training offices to ensure accomplishment of CT requirements.

3.1.2. Cybercrew members are responsible for reporting all accomplished training events to their attached unit. **(T-3)**

3.2. Currency. The first component of CT, maintaining currency, involves regular repetitions of the basic operational skills necessary to ensure the safe operation of the CVA/H weapon system. **Tables 3.1** and **3.2** establish the minimum currency requirements for a CVA/H cybercrew member to maintain BCQ, CMR, or BMC statuses.

3.2.1. Currency may be established or updated by:

3.2.1.1. Accomplishing an event as a qualified cybercrew member whose currency has not expired. **(T-3)**

3.2.1.2. Accomplishing an event as a qualified cybercrew member under supervision of a current instructor. **(T-3)**

3.2.1.3. Events satisfactorily performed on any evaluation may be used to establish or update currency in that event. **(T-3)**

3.2.1.4. All relevant operational activity should be counted and credited toward a cybercrew member's currency regardless of location (e.g., home station, exercise, contingency operations, training simulator).

3.2.2. Multi-position certified individuals must meet currency requirements for each cybercrew position in order to maintain operational statuses for assigned positions.

3.2.3. Recurrency. If a cybercrew member loses a particular currency, that event may not be performed by the member except for the purpose of regaining currency as noted. Cybercrew

members accomplish overdue training requirements as specified in **Tables 3.1** and **3.2** before they are considered recertified to perform the task.

3.2.3.1. When cybercrew members become overdue on training requirements identified in

Tables 3.1 and **3.2**, CMR/BMC status is affected, and regression to N-CMR/N-BMC is required.

3.2.3.2. Members downgraded to N-CMR/N-BMC status due to overdue currency must regain currency by performing the necessary training event under instructor supervision. **(T-3)**

Table 3.1. Network Analyst Currencies.

Event	Accomplished In	Inexperienced *	Experienced **	Affects CMR	To Regain Currency	Notes
Execute Emergency Response Actions	Any event	90 days	180 days	Y	JCTM***	2, 3
Configure Windows Firewall	Any event	90 days	180 days	N	Any event	1, 2, 3
Configure *NIX Firewall	Any event	90 days	180 days	Y	Any event	1, 2, 3
Extract file from PCAP	Any event	90 days	180 days	N	Any event	2, 3
Extract Network Device Configuration File	Any Event	90 days	180 days	N	Any event	2, 3
Conduct Network Enumeration	Any event	90 days	180 days	N	Any event	2, 3
Conduct Vulnerability Scan	Any event	90 days	180 days	N	Any event	2, 3
MIP Sanitization	Any event	90 days	180 days	Y	Any event	2, 3
Network Malware Handling	Any event	90 days	180 days	Y	Any event	2,3
Instructor	Any event	N/A	180 days	N	Any event	4

Notes:

* Denotes cybercrew members who are BCQ

** Denotes cybercrew members who are CMR or BMC

*** Joint Cyber Tactics Manual (JCTM) contains the emergency response actions.

1 – Squadrons can make this currency unit-specific (e.g., manually, scripted).

2 – CVA/H currencies can be accomplished during a mission, exercise, simulator event, or post mission analysis.

3 – Performance or instruction will update currency.

4 – Instructors will only teach events in which they are current and qualified. With SQ/CC approval, instructors who become N-CMR/N-BMC may still teach events in which they are current and qualified (IAW ACCMAN17- 2CVA/H V1, **Section 4.2**).

Table 3.2. Host Analyst Currencies.

Event	Accomplished In	Inexperienced *	Experienced **	Affects CMR	To Regain Currency	Notes
Execute Emergency Response Actions	Any event	90 days	180 days	Y	JCTM***	2, 3

Configure/Validate Windows Firewalls	Any event	90 days	180 days	Y	Any event	1, 2, 3
Configure/Validate *NIX Firewalls	Any event	90 days	180 days	Y	Any event	1, 2, 3
MIP Sanitization	Any event	90 days	180 days	Y	Any event	2, 3
Conduct System Enumeration	Any event	90 days	180 days	N	Any event	2, 3
Conduct Vulnerability Scan	Any event	90 days	180 days	N	Any event	2, 3
Deploy Agents	Any event	90 days	180 days	Y	Any event	2, 3
Conduct Investigation based on an IOC Using an Agentless Method	Any event	90 days	180 days	Y	Any event	2, 3
Triage Malware	Any event	90 days	180 days	Y	Any event	2, 3
Collect Linux® Memory Dump & Disk Artifacts	Any event	90 days	180 days	Y	Any event	2, 3
Collect Windows Memory Dump & Disk Artifacts	Any event	90 days	180 days	Y	Any event	2, 3
Eradicate Detected Malicious Activity	Any event	90 days	180 days	Y	Any event	2, 3
Instructor	Any event	N/A	180 days	N	Any event	4

Notes:

* Denotes cybercrew members who are BCQ

** Denotes cybercrew members who are CMR or BMC

*** Joint Cyber Tactics Manual (JCTM) contains the emergency response actions.

1 – Squadrons can make this currency unit-specific (e.g., manually, scripted).

2 – CVA/H currencies can be accomplished during a mission, exercise, simulator event, or post mission analysis.

3 – Performance or instruction will update currency.

4 – Instructors will only teach events in which they are current and qualified. With SQ/CC approval, instructors who become N-CMR/N-BMC may still teach events in which they are current and qualified (IAW ACCMAN17- 2CVA/H V1, **Section 4.2**).

3.3. Ready Cybercrew Program (RCP) Proficiency. The second component of CT, maintaining proficiency, consists of regular repetitions of specific mission-related events required to accomplish the unit's assigned mission. The RTM provides the baseline for SQ/CCs to develop a realistic training program to prioritize all Designed Operations Capabilities (DOC) tasked requirements to ensure team proficiency.

3.3.1. The RTM establishes the minimum proficiency requirements for a CVA/H cybercrew to maintain CMR or BMC status. Standardized training event identifiers and descriptions are located in Attachment 1 of the RTM. Units may add unit-specific events as required. Descriptions of these events will be included in local training documentation. **(T-3)**

3.3.2. All operational activity should be counted and credited toward a cybercrew member's proficiency if the activity meets the RTM definitions for "effective," regardless of the location

(e.g., home station, exercise, contingency operations, training simulator).

3.3.3. Individuals qualified in multiple crew positions will only receive credit for RCP events that align to the specific duties performed by the individual (i.e., a dual-qualified host and network analyst would satisfy host analyst proficiency requirements only for an event during which the member performed the duties of a host analyst).

3.3.4. End of Cycle Requirements. Cybercrew members who fail to complete event requirements by the end of the training cycle may require additional training depending on the type and magnitude of the deficiency. Refer to **paragraph 3.4** for proration guidance. In all cases, shortfalls will be reported to the Operations Group (OG)/CC.

3.3.4.1. Failure to meet specific proficiency requirements will result in one of the following:

3.3.4.1.1. The SQ/CC determines if the deficiency is significant enough to warrant downgrade to N-CMR or N-BMC. CMR status may be regained by satisfactorily performing all proficiency requirements under instructor supervision. These missions may also count toward the total requirements for the new training cycle. **(T-3)**

3.3.4.1.2. Continuation of CMR status may be authorized by the SQ/CC provided the member only accomplishes operational tasks that do not align to the incomplete event requirements. Training shortfalls will be noted in End-of-Cycle Reports, and cybercrew members will satisfactorily complete all training requirements as operations tempo allows and before performing any operational tasks that align to incomplete events.

3.4. Proration of Training.

3.4.1. The SQ/CC should prorate any training requirements precluded by the following events: initial arrival date in Squadron, non-chargeable leave periods (i.e. parental, emergency, convalescent, etc.), non-mission Temporary Duty (TDY), Permanent Change of Station (PCS), or non-mission exercises or deployments. Other extenuating circumstances, as determined by the SQ/CC, that prevent the crewmember from mission duties for more than 15 consecutive days may be considered as non-availability for proration purposes. **(T-3)** The following guidelines apply:

3.4.1.1. Proration will not be used to mask training or planning deficiencies.

3.4.1.2. Proration does not apply to the ARC unless mobilized in support of an operational mission.

3.4.1.3. Proration is based on cumulative days of non-availability for mission duties in the training cycle and does not apply to individuals who are available for 15 days or less. Use **Table**

3.3 to determine the number of months to be prorated based on each period of cumulative non-mission duty calendar days IAW ACCI 17-202 V1. **(T-3)**

3.4.1.4. If MQT is re-accomplished, a crewmember's training cycle will start over following successful completion. **(T-3)**

3.4.1.5. Newly assigned cybercrew members achieving CMR/BMC status after the 15th of the month are in CT on the first day of the following month for proration purposes. A prorated share of RCP events must be completed. **(T-3)**

3.4.1.6. A cybercrew member's last month on station prior to a PCS may be prorated, provided 1 month's proration is not exceeded. Individuals who are PCS-ing may be considered CMR for

reporting purposes during a period of 60 days from date of last training event, or until loss of CMR qualification, sign-in at new duty station, or whichever occurs first.

Table 3.3. Proration Allowance.

Cumulative Days of Non-Mission Activity	Proration Allowed (Months)
0 – 15	0
16 – 45	1
46 – 75	2
76 – 105	3
106 – 135	4
136 – 165	5
166 – 195	6
196 – 225	7
226 – 255	8
256 – 285	9
286 – 315	10
316 – 345	11
Over 345	12
Note: As an example, Capt Blix was granted 17 days of emergency leave in January and attended SOS in residence from March through April for 56 consecutive calendar days. The SQ/CC authorized a total of two months proration from his training cycle (two months for the 73 cumulative days of non-availability)	

3.5. Additional Training. Any training that is recommended by the Stan/Eval Examiner to remedy deficiencies identified during an evaluation.

3.6. Currency and Proficiency Reporting. Currency and Proficiency are reported (IAW the RTM) through the Mid-Cycle and End-of-Cycle Reports, as directed by ACC/A326K. RTM Reporting instructions will take precedence over this volume.

3.6.1. Each cybercrew member will be reported as current or not current IAW **Table 3.1** and **Table 3.2**. All currency requirements must be up-to-date for the cybercrew member to count as current. The number of cybercrew members who are not current is then divided by the total number of cybercrew members.

3.6.2. Each cybercrew member will be reported as proficient or not proficient per event type (i.e., Hunt, Clear, Enable Hardening, and Assess) IAW the current RTM. All proficiency requirements must be up-to-date for the cybercrew member to count as proficient. The number of cybercrew members who are not proficient is divided by the total number of cybercrew members.

3.6.3. Example: In a CPT with 27 qualified cybercrew members, 1 cybercrew member has not configured a Linux® (Linus Torvlad's UNIX®(Uniplex Information and Computing System)) firewall within the currency timelines. This cybercrew member is not current. Divide 1 by 27 (1

÷ 27 = 0.037) and then multiply by 100 (0.037 x 100 = 3.7%). Record this percentage on the report. The unit will then perform the same calculation for proficiency requirements per event type.

Chapter 4

INSTRUCTOR TRAINING AND QUALIFICATION

4.1. Requirements. A qualified CVA/H Instructor shall be a competent subject matter expert adept in the methodology of instruction. The instructor shall be proficient in evaluating, diagnosing, and critiquing student performance, identifying learning objectives and difficulties, and prescribing and conducting remedial instruction. The instructor must be able to conduct instruction across all training venues (e.g., classroom, training devices, ops floor, mission execution). Instructor trainees will be observed and supervised by a qualified instructor. **(T-2)**

4.1.1. All instructors must be CMR for at least 12 months prior to nomination (Wing level and below). Instructors must be current and qualified in any event they instruct. **(T-3)**

4.1.2. FTU instructors, including USAF Weapons School instructors, are only required to maintain BMC. Waiver authority will not be delegated. **(T-2)**

4.1.3. All instructors must adhere to USCYBERCOM Trainer certification requirements IAW USCYBERCOM CTM 7-0.1 *Joint Cyberspace Training and Certification Standards (JCT&CS), Annex C*. Instructors will also meet additional USCYBERCOM and Air Force Cyber Command (AFCYBER) requirements for United States Cyber Command (USCC) work role training and instruction when published.

4.1.4. IAW ACCI 17-202V1, units will develop instructor upgrade syllabus that is approved by the OG/CC. It will minimally include:

4.1.4.1. Applicable equipment configurations and scheduling procedures (e.g., simulator and on-line equipment configuration, and instruction scenario control procedures). **(T-2)**

4.1.4.2. ISD processes and procedures. **(T-2)**

4.1.4.3. Requirements for trainees to develop, conduct and administer classroom and field training, and configure simulators and operations (ops) floors, as appropriate. **(T-2)**

4.1.4.4. Supervision by at least one certified instructor when academic training is conducted. **(T-2)**

4.1.5. The SQ/CC will select instructor candidates based on experience, judgement, maturity, communication skills, operational skills, and technical knowledge of the weapon system.

4.2. Failure to Meet Instructor Requirements. Instructors may lose instructor status for the following:

4.2.1. Failure to instruct a course or event at least once every 180 days.

4.2.2. The CO deems that loss of currency is of sufficient importance to require complete decertification (but not a complete loss of qualification).

4.2.2.1. If the affected cybercrew member retains instructor qualification, recertification will be at the CO's discretion IAW ACCI 17-202V2 and ACCMAN 17-2CVA/HV2.

4.2.2.2. If an instructor loses currency, and the SQ/CC does not require decertification and removal from CMR or BMC status, instructor status may be retained. The instructor will not

instruct that mission or event until currency is regained.

4.2.3. Instructor lack of ability. Instructors serve solely at the discretion of the SQ/CC. Instructors will exemplify a high level of performance and present themselves as reliable and authoritative experts. Instructors exhibiting substandard performance should be candidates for a suitability review for continued instructor duty.

4.2.3.1. Instructors will be decertified if the SQ/CC deems instructor is substandard, ineffective, or providing incorrect procedures, techniques, or policy guidance.

4.2.3.2. Recertification requirements will be at the discretion and direction of the CO.

Chapter 5

DOCUMENTATION

5.1. Requirements. In all instances, the use of electronic forms, digital signatures, and electronic format Individual Training Folders (ITF) is authorized.

5.1.1. Each block of training will be documented and maintained in the cybercrew member's ITF.

5.1.2. A cybercrew member's CT and additional training events are maintained in the member's ITF. Electronic format ITFs are authorized provided proper security measures, backup capability, and sustainment plans are in place.

5.1.3. Dispose of ITFs and other related material according to the RDS and AF guidance concerning the protection of Personally Identifiable Information.

5.2. Helpful Forms.

5.2.1. ACC Form 4419, *Record of Training*. Cybercrew member training events/tasks can be documented on the ACC Form 4419.

5.2.2. ACC Form 4420, *Individual's Record of Duties and Qualifications*. The ACC Form 4420 is an index providing pertinent training information extracted from all the ACC Forms 4419 accomplished by the cybercrew member.

DAVID G. SHOEMAKER, Maj Gen, USAF
Director of Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

ACCI 17-202 Volume 1, *Cybercrew Training*, 12 January 2021

ACCI 17-202 Volume 2, *Cybercrew Standardization/Evaluation Program*, 12 January 2021

ACCMAN 17-2CVAHV2, *Cyber Vulnerability Assessment/Hunter (CVA/H) - Standardization/Evaluation Program*, 12 January 2021

AFI 10-217, *Management of Air Force Operational Training and Undergraduate Aircrew Training Systems*, 22 December 2023

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFTTP 3-1., (U) *CVA/Hunter*, 6 August 2021 (Contents are S//NF)

AFTTP 3-1., *Advanced Cyber Threat Guide Chapter 13*, 10 December 2018

AFTTP 3-1., *Integrated Planning and Employment*, 3 April 2020 (Contents are S//NF)

AFTTP 3-3., *CVA/Hunter*, 6 August 2021

AFTTP 3-3., *Integrated Planning and Employment*, 3 April 2020 (U)

CTM 7-0.2, *Cyber Mission Force Training & Readiness Manual, Appendix 2, Addendum 1, "CPT Training and Evaluation Outline"*, 28 May 2019

Cyber Vulnerability Assessment/Hunter (CVA/H) Ready Cybercrew Program (RCP) Tasking Memorandum (RTM), Fiscal Year (FY) 2024, 01 October 2023

Cyberspace Vulnerability Assessment/Hunter Weapon System Configuration Management Plan, Annex version 2.2., February 2018

Cyber Warfare Publication 3-33.4, *Cyber Protection Team Organization, Functions, and Employment*, 28 January 2020

DAFPD 17-2, *Cyber Warfare Operations*, 27 October 2020

DAFMAN 90-161, *Publishing Processes and Procedures*, 18 October 2023

Adopted Forms

ACC Form 4418, *Certificate of Cybercrew Qualification*

ACC Form 4419, *Record of Training*

ACC Form 4420, *Individual's Record of Duties and Qualifications*

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

ACC—Air Combat Command

ACCI—Air Combat Command Instruction

ACCMAN—Air Combat Command Manual

AFCYBER—Air Force Cyber Command

AF—Air Force

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

AFTTP—Air Force Tactics, Techniques, and Procedures

ARC—Air Reserve Components

BCQ—Basic Cyber Qualified

BMC—Basic Mission Capable

CC—Commander

CCL—Cyber Crew Lead

CMF—Cyber Mission Force

CMR—Combat Mission Ready

CO—Certifying Official

CT—Continuation Training

CTA—Exploitation Threat Analyst

CTM—Cyber Training Manual

CVA/H—Cyber Vulnerability Assessment/Hunter

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DAFMAN—Department of the Air Force Manual

DAFPD—Department of the Air Force Policy Directive

DOC—Designed Operational Capability

DO—Director of Operations

DoD—Department of Defense

ETCA—Education and Training Course

FTU—Formal Training Unit

HA—Host Analyst

HHQ—Higher Headquarters

HQ—Headquarters

IAW—In Accordance With

IOC—Indicator of Compromise

IQT—Initial Qualification Training

ISD—Instructional Systems Development

ITF—Individual Training Folder

JCTM—Joint Cyber Tactics Manual

JQR—Job Qualification Record

LINUX®—Linus Torvald's UNIX®

MAJCOM—Major Command

MIP—Mobile Interceptor

MQT—Mission Qualification Training

MSN—Mission

MTTL—Master Training Task List

NA—Network Analyst

NAF—Numbered Air Force

N-BMC—Non-Basic Mission Capable

N-CMR—Non-Combat Mission Ready

NGB—National Guard Bureau

***NIX**—UNIX®/LINUX®

NLT—No Later Than

OG—Operations Group

OPORD—Operations Order

OPR—Office of Primary Responsibility

ops—Operations

OSS—Operations Support Squadron

OTP—Operations Training Plan

PBED—Planning, Briefing, Execution, and Debriefing

PCAP—Packet Capture

PCS—Permanent Change of Station

PEX—Patriot Excalibur

PII—Personally Identifiable Information

PMO—Program Management Office

QUAL—Qualification

RCP—Ready Cybercrew Program

RDS—Records Disposition Schedule

RQT—Requalification Training

RTM—Ready Cybercrew Program Tasking Memorandum

SMTP—Special Mission Training Plan

SMQ—Special Mission Qualification

SMT—Special Mission Training

SQ—Squadron

Stan/Eval—Standardization and Evaluation

STP—System Training Plan

T&R—Training and Readiness

TDY—Temporary Duty

TPT—Target Planning Team

UNIX®—Uniplex Information and Computing System

USAF—United States Air Force

USCC—United States Cyber Command

USCYBERCOM—United State Cyber Command

BY ORDER OF THE COMMANDER
AIR COMBAT COMMAND

AIR COMBAT COMMAND MANUAL 17-2CVA/H, VOLUME 1

19 JANUARY 2021

Cyberspace

CYBER VULNERABILITY ASSESSMENT/HUNTER (CVA/H) - TRAINING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading on the e-Publishing website at **www.e-publishing.af.mil**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: USAF/ACC/A3/2/6K

Certified by: USAF/ACC/A3/2/6K
(Col Eric C. Paulson)

Pages: 23

This manual implements Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyber Warfare Operations*, and references Air Combat Command (ACC) Instruction (ACCI) 17-202, Volume 1, *Cybercrew Training*. It establishes the minimum Air Force (AF) standards for training and qualifying/certifying personnel for performing crewmember duties on the Cyber Vulnerability Assessment/Hunter (CVA/H) weapon system. This publication applies to all Air Combat Command (ACC), AF Reserve Command (AFRC), Air National Guard, and third-party governmental and contract support agencies in accordance with (IAW) appropriate provisions contained in memoranda, support agreements and AF contracts. This publication requires the collection and or maintenance of information protected by the Privacy Act of 1974, as amended, authorized by Air Force Instruction (AFI) 36-2608, *Military Personnel Records System*. Ensure that all records and processes prescribed in this publication are maintained IAW AFI 33-322, *Records Management and Information Governance Program*, and are disposed IAW the Air Force Records Disposition Schedule (RDS), located in the Air Force Records Information Management System (AFRIMS). System of Records Notice F011 AF AFMC B, *Patriot Excalibur (PEX) System Records*, applies and is available at **https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/Air-Force-Article-List/**. Vigilance must be taken to protect Personally Identifiable Information when submitting or sending nominations, applications or other documents to Department of Defense (DoD) agencies through government Internet, software applications, systems, e-mail, postal, faxing or scanning. Refer to the following directives for additional guidance: AFI 33-332, *Air Force Privacy and Civil Liberties Program*, DoD 5400.11-R, *Department of Defense Privacy Program*. Forms containing Personally Identifiable Information

require Privacy Act Statements. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination prior to certification and approval. Submit suggested improvements to this instruction on AF Form 847, *Recommendation for Change of Publication*, through command channels, to ACC/A3/2/6K. ACC will conduct publication reviews and/or revisions as necessary with other agencies as the Cyberspace mission expands. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, and T-3") number following the compliance statement. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See DAFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. Waiver authority for non-tiered paragraphs remains with ACC/A3. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander (CC) for non-tiered compliance items. Compliance with **Attachment 1** in this publication is optional.

Chapter 1

OVERVIEW/BACKGROUND

1.1. General. This manual prescribes policy and guidance for training CVA/H cybercrew members. Training policy, guidance, and requirements are set forth for each phase of crew training. The objective of training should be the progressive development of CVA/H crew readiness. This manual applies to all CVA/H cybercrew members, defined as individuals assigned to utilize the CVA/H weapon system in the achievement of tasked mission objectives and designated a specific crew position and/or work role. This manual also applies to members in formal training for immediate assignment to a CVA/H weapon system position.

1.2. Program Goals. The overall objective of the CVA/H training program is to develop and maintain a high state of readiness for the immediate and effective employment across a full range of military operations. Mission readiness and effective employment are achieved through the development and mastery of core competencies for each of the crew positions aligned with the CVA/H weapon system.

1.3. Roles and Responsibilities.

1.3.1. ACC will:

1.3.1.1. Develop and manage, in coordination with affected commands, the appropriate guidance to establish cybercrew training requirements and standards IAW ACCI 17-202V1 and AFI 16-1007, *Management of Air Force Operational Training Systems*.

1.3.1.2. Chair annual Training Planning Team to review training requirements and programs for currency, applicability, compliance, and effectiveness and address issues in lead command-provided guidance documents as appropriate. Conference members should include representatives from squadron Training, Weapons and Tactics, Stan/Eval, Operations, Formal Training Unit, Program Management Office, and other areas as required.

1.3.1.3. Publish a Ready Cybercrew Program Tasking Memorandum (RTM) annually prior to the start of the fiscal year. The RTM may contain supplemental training requirements or updated guidance.

1.3.1.4. Determine total force cybercrew training requirements in coordination with using Major Commands (MAJCOMs), NGB, and AFRC across Future Years Defense Program. Forward requirements annually to Headquarters (HQ) ACC/A3/2/6K via the Program Requirements Document for validation and inclusion in the Undergraduate and Graduate Program Guidance Letters.

1.3.2. Numbered Air Force (NAF) employing CVA/H will:

1.3.2.1. Maintain oversight of cybercrew training within its chain of command and for attached units.

1.3.2.2. Convene conferences and working groups, as necessary, to review and improve training policies and procedures.

1.3.2.3. Validate, approve, and provide guidance on the implementation and use of the master training task list (MTTL) items. NAFs will coordinate MTTLs with the HQ ACC. **(T-2)**

1.3.2.4. Coordinate on the RTM. **(T-2)**

1.3.3. Wings and groups employing CVA/H will:

1.3.3.1. Be responsible for managing the wing's Operations Training program. In Wings or Groups with an Operations Support Squadron (OSS), the OSS will have a training office with a Chief of Training and at least one instructor per cybercrew position. **(T-3).**

1.3.3.2. Wings will submit a training report to ACC/A3/2/6K every 6 months during the training cycle (on the 15th day of April and October IAW the RTM). Squadrons may submit an out of cycle report at any time Higher Headquarters (HHQ) assistance is required. When preparing all reports, units will use the most current guidance/templates found on the ACC/A3TO SharePoint page. **(T-3).**

1.3.3.3. Wings will also assist Air Reserve Components (ARC) unit training programs as required or requested IAW applicable unit support programs, memorandums of agreement or memorandums of understanding.

1.3.4. The Wing Chief of Training:

1.3.4.1. The Chief of Training and all instructors will maintain Combat Mission Ready (CMR) status in at least one crew position in the CVA/H Weapon System.

1.3.4.2. The Chief of Training will attend an Instructional Systems Development (ISD) course IAW ACCI 17-202V1. **(T-3).**

1.3.4.2.1. Is responsible for leading training development efforts and standardizing training material and programs across the wing and/or group.

1.3.4.2.2. Develops programs to ensure training objectives are met.

1.3.4.2.3. Assists subordinate units in management of training programs to ensure programs meet mission needs and provide the necessary support. **(T-3).**

1.3.4.2.4. Establish procedures for review, quality control, and approval of unit training documentation.

1.3.4.2.5. Establish the RCP and review/modify implementation before the start of every fiscal year or upon publication of out-of-cycle, IAW the RTM. **(T-3).**

1.3.4.2.6. Ensure RCP events are oriented towards maintaining operationally relevant skills or tactical employment simulating conditions anticipated in the unit mission. RCP event accomplishment is defined in the RTM.

1.3.4.2.7. Coordinate on the RTM. **(T-3).**

1.3.5. Unit Training Organization:

1.3.5.1. Scope. For the purpose of this manual, "unit" includes levels of organizations under HHQ required to establish a training function. Most units are composed of cyber squadrons/detachments.

1.3.5.2. Squadron (SQ)/CC. The commander is responsible for the implementation of the squadron Cybercrew Training Program. The commander:

1.3.5.2.1. Directs the conduct of the unit-level training programs. **(T-3).**

1.3.5.2.2. Provides manpower to the unit training function to execute the duties directed by ACCI 17-202V1 and this volume. **(T-3).**

1.3.5.2.3. Designates cybercrew instructors. **(T-3).**

1.3.5.2.4. Ensure cybercrews and individual operators are provided with adequate reconstitution time post-mission to enable completion of RCP requirements. **(T-3).**

1.3.5.3. Operations Training Flight. The operations training flight will be administered and implemented from the unit level with the Chief of Training reporting directly to the Director of Operations (DO). The operations training flight will:

1.3.5.3.1. Be led by a Chief of Training reporting directly to the DO.

1.3.5.3.2. Be staffed with a minimum of one instructor for each cybercrew position. **(T-3).**

1.3.5.3.3. The Chief of Training and instructors will maintain Mission Ready (MR)/CMR status. **(T-3).**

1.3.5.3.4. Select instructors from the most suitable, highest qualified and most experienced personnel. Requisites for instructor upgrade are outlined in **Chapter 4**.

1.3.5.3.5. Process and maintain training records and forms or electronic equivalent such as PEX.

1.3.5.3.6. Establish procedures for review and quality control of training documentation. **(T-3).**

1.3.5.3.7. Develop and document the instructor training program designed to train and certify instructors on training cybercrew personnel. Instructor training programs must be reviewed and approved by the OSS prior to implementation and must meet the requirements of **Chapter 4**. **(T-3).** For units who do not have an OSS, complete approval through the supporting group commander or designated representative.

1.3.5.3.8. At least quarterly, advise unit leadership on unit cybercrew training status and requisite completion of Initial Qualification Training (IQT)/Mission Qualification Training (MQT) shortfalls, and missed suspense.

1.3.6. Cybercrew members will:

1.3.6.1. Be responsible for monitoring and completing all training requirements.

1.3.6.2. Ensure they participate only in missions, events, and tasks for which they are qualified/certified. **(T-3).**

Chapter 2

GUIDANCE AND PROCEDURES

2.1. Qualification Training. This section defines CVA/H cybercrew operational statuses and outlines minimum training requirements for IQT, MQT, upgrade/special mission training, difference qualification training, senior officer qualification training and requalification training for all CVA/H cybercrew positions.

2.1.1. IQT. Formal training required in order to qualify for basic cybercrew duties in an assigned crew position without regard for the unit's operational mission.

2.1.1.1. Method. The primary method of CVA/H IQT is to attend and complete the Formal Training Unit (FTU) course(s) outlined in the CVA/H syllabus and listed in the Education and Training Course Announcement (ETCA) system under United States Air Force (USAF) Formal Schools. ETCA can be reached via the Air Force Portal. Completing the appropriate formal course(s) satisfies all IQT requirements. In lieu of a formal IQT course, authority resides with Unit Commanders for assessment, evaluation and certification criteria based on implementation of HHQ guidance.

2.1.1.2. In-Unit IQT. When formal course attendance is not practical or quotas are not available, units will request waivers to conduct in-unit IQT using formal school courseware. Accomplish in-unit training IAW applicable formal school courseware and the guidance contained in ACCI 17-202 Vol 1. **(T-2).**

2.1.1.3. Personnel in IQT should not have AF supervisory responsibility or additional duties.

2.1.1.4. Personnel with previous CVA/H experience but most recently assigned to a non-CVA/H unit, must re-accomplish the CVA/H portion of IQT. Units can assess the individual's knowledge and direct the cybercrew member to accomplish all IQT requirements. **(T-3).**

2.1.1.5. Cybercrew members previously assigned to a different weapon system, but who attended IOS-CWO 001 Cyber Warfare Operations, are not required to attend that portion of IQT. **(T-3).**

2.1.1.6. IQT Prerequisites. Units must ensure each cybercrew member complies with initial qualification prerequisites IAW ACCI 17-202V1, the current CVA/H System Training Plan (STP), and associated course syllabi before entering qualification training. **(T-2).**

2.1.2. MQT. The purpose of MQT is to qualify cybercrew members in assigned cybercrew positions to perform the unit mission. This section prescribes the minimum training requirements to qualify individuals in unit missions and is provided to assist SQ/CCs in developing their MQT program.

2.1.2.1. Method. MQT is a unit-developed formal training program developed IAW Instructional Systems Development principles that prepares newly assigned cyber operators to accomplish the unit mission (see **paragraph 2.6** for operational statuses). The culmination of MQT is an evaluation IAW Air Combat Command Manual (ACCMAN) 17-2V2. Units determine MQT requirements IAW HHQ policy and guidance, wing policy

and guidance, and train to crew position requirements not covered in IQT. Cybercrew members participating in MQT are dedicated to that training which takes priority over non-training related duties to include mission execution. MQT will be taught by qualified instructors as defined in **Chapter 4**.

2.1.2.2. MQT must be completed prior to cybercrew member employment of CVA/H in operational events.

2.1.2.3. Mission-Related Training. Units will develop instructions addressing areas pertinent to the mission as determined by the SQ/CC.

2.1.2.3.1. Guidance. Mission-related training is informed by the mission, organizational concepts of employment and other higher HQ guidance. Additional mission-related training elements are addressed in Air Force Tactics, Techniques, and Procedures (AFTTP) 3-1. *Cyber Vulnerability Assessment/Hunter,* AFTTP 3-1. *Advanced Cyber Threat Guide Chapter 13,* AFTTP 3-3. (U) *Integrated Planning and Employment* (Contents are (S//NF)), AFTTP 3-3. *Integrated Planning and Employment (*Contents Unclassified), Cyber Warfare Publication 3-33.4, and other mission-related documents. **(T-3).**

2.1.2.3.2. Operations Training Plan (OTP). Units will determine and document MQT syllabi and requirements in a master OTP. While MQT is mission specific, units will use standardized training whenever possible. Wings (if applicable) will develop a core OTP syllabus and squadrons will develop additional mission specific OTPs. The OTP contains the knowledge, tasks, method of training, and total training time (to include estimated and maximum training times, lapse between training events/tasks etc.). Schedule, conduct, and document MQT IAW the OTP. **(T-3).**

2.1.2.3.3. Mission Objectives: Familiarity with performance measures, mission essential tasks, and core functions outlined in Cyber Technical Manual (CTM) 7-0.2, *Cyber Mission Force (CMF) Training and Readiness (T&R) Manual*, local area requirements, and procedures. **(T-3).**

2.1.2.3.4. Specific Mission Tasks: Mission essential tasks derived from the CTM 7-0.2 *CMF T&R Manual*, local area familiarization, emergency procedures, and other tasks determined by the unit. **(T-3).**

2.1.2.3.5. Mission objectives and tasks are minimum requirements for MQT. Additional training events based on student proficiency and background or due to student non-progression is available within the constraints of the OTP and may be added at SQ/CC discretion. **(T-3)**

2.1.2.3.6. Time Limits. The cybercrew member will begin in-unit MQT NLT 30 days (90 days for the Air Guard/Reserve Component) after completing IQT and reporting to a new duty station or unit. **(T-2).**

2.1.2.3.7. Certification. MQT is complete upon successful completion of the Host Analyst (HA) or Network Analyst (NA) evaluation IAW ACCMAN 17-2V2and certification by the certifying official. **Note:** For the purposes of this instruction "certification" denotes a Squadron Commander (SQ/CC)'s action; whereas

"qualification" denotes a formal Standardization and Evaluation (Stan/Eval) evaluation IAW ACCMAN 17-2V2.

2.1.2.3.8. MQT Pre-requisites. Each cybercrew member must complete all applicable IQT requirements IAW **para 2.1.1** before entering MQT. **(T-2).**

2.2. Upgrade/Special Mission Training. Unless specifically prohibited or restricted by weapon system operating procedures, specific theater operations order (OPORD), or specific HHQ guidance, the Operations Group (OG)/CC exercising operational control may approve upgrade or certification/qualification training during operational missions under the supervision of an instructor qualified/certified in that position. **(T-3).**

2.2.1. Upgrade Training. Upgrade training is given to operators upgrading from their current crew position to a different position within the CVA/H. The upgrade position will require additional qualification criteria and must contain all of the requirements of the initial position. Tasks common to both positions do not need to be retrained if the knowledge and skills are duplicated. Continuation training (CT) requirements will only be levied against the upgrade position as it is utilized in place of the original position, however the operator can perform operations for either the original or upgraded position.

2.2.1.1. See **Chapter 4** for information on instructor upgrade information/requirements.

2.2.2. Special Mission Training. Special mission training is given to operators obtaining a second qualification or certification on the CVA/H weapon system. The second qualification or certification has additional requirements that do not completely overlap with the initial qualification and requires a baseline MR/CMR qualification to obtain. CT requirements apply to the initial and second qualification. A loss of qualification in the initial position will cause a loss of qualification in the second position

2.2.2.1. Special mission training can also teach any special skill necessary to carry out the unit's assigned mission that is not required by every cybercrew member. Specialized training may consist of special tactics, weapon system capabilities, responsibilities, and specific mission systems in order to maintain proficiency in unit tasked special capabilities and missions.

2.2.2.2. The certifying official will determine and assign cybercrew members that will train for and maintain special mission qualifications and cybercrew position certifications.

2.3. Difference Qualification Training. Difference qualification training will be required upon major upgrade/modification to the CVA/H weapon system.

2.3.1. A major modification/upgrade is IAW with Program Management Office (PMO) definitions of version control contained in the CVA/H Configuration Management Plan, Annex version 2.2 and is defined as:

2.3.1.1. Any change to the Application Programming Interface (API)

2.3.1.2. Any change causing forward incompatibility

2.3.1.3. Change resulting from a complete re-write of code

2.3.1.4. Change resulting in the addition of capability

2.3.1.5. Change forcing hardware update/modification

2.3.2. Upon major modification/upgrade the PMO will deliver Type 1 formal technical training in order to train select personnel to operate and/or maintain new systems. This will serve as initial operator training.

2.3.2.1. PMO Type 1 training will be integrated into unit training programs.

2.3.3. Difference Training does not disqualify members from MR/CMR status. However, all untrained members cannot performs tasks associated with the new guidance until trained, unless under the supervision of an instructor/evaluator. **(T-2).**

2.3.4. All training will be documented IAW **Chapter 5**.

2.4. Senior Officer Qualification Training.

2.4.1. Senior officer is defined as deputy group commander or higher, must meet course entry pre-requisites as prescribed in **paragraph 2.1.1.6** and will complete all syllabus requirements unless waived IAW ACCI 17-202V1 by the Wing/CC.

2.4.2. Senior officer in training, at the FTU or in-unit, is considered in formal training status for the duration of the course. Their AF duties will be delegated to appropriate deputies until training is completed. **(T-2).**

2.5. Requalification Training (RQT). Academic and positional training required to requalify to MR/CMR status. IAW ACCI 17-202V1, a cybercrew member is considered unqualified upon expiration of currency exceeding six months or expiration of his or her qualification evaluation, whoever occurs first. The duration of unqualified time is measured from the date the cybercrew member became unqualified until the retraining start date.

2.5.1. An unqualified cybercrew member up to 6 months can requalify IAW ACCI 17-202V1by accomplishing training in all delinquent items (as applicable) or any additional training as directed by the certifying official. Requalification evaluation required IAW ACCI 17-202V2 and ACCMAN 17-2V2.

2.5.2. An unqualified cybercrew member exceeding 6 months can requalify by re-accomplishing IQT/MQT or RQT and a requalification evaluation IAW ACCI 17-202V2 and ACCMAN 17-2V2. Applicable portions of MQT may be used to create a requalification program for cybercrew members who have been downgraded from CMR and or Basic Mission Capable (BMC) to specifically address deficiencies which caused downgrade.

2.6. CVA/H Cybercrew Operational Status. IAW ACCI 17-202V1, a cybercrew member may be assigned Basic Cyber Qualified (BCQ), BMC, or Mission Ready (MR)/CMR status.

2.6.1. Basic Cyber Qualified. A cybercrew member who has satisfactorily completed IQT but has not yet completed MQT is BCQ. BCQ cybercrew members are not to perform RCP-tasked events or missions without instructor supervision.

2.6.2. Basic Mission Capable. A cybercrew member that has satisfactorily completed the minimum IQT, MQT, a full Stan/Eval evaluation, maintains certification, currency, and proficiency in the unit's operational mission is BMC.

2.6.2.1. CVA/H cybercrew members in BMC status must be able to attain CMR status to meet operational tasks within 30 days (90 days for Air Reserve Component). **(T-2).**

2.6.2.2. BMC cybercrew members are typically assigned to MAJCOM headquarters, NAF, FTU, Group/Wing functions, OSS, Direct Reporting Unit, and supporting units that employ the CVA/H weapon system.

2.6.2.3. BMC cybercrew members may log instructor or evaluator time for the portion of the mission for which they are current and qualified and performing instructor or evaluator duties.

2.6.3. MR/CMR. An MR/CMR cybercrew member is available and qualified in the squadron's mission. A CMR cybercrew member has completed CVA/H IQT, MQT, and maintains qualification and proficiency in the command or unit operational mission. The cybercrew member must be certified and current on training requirements as described in **Chapter 3**.

2.6.3.1. The Certifying Official is the first operational commander in the member's chain of command or as designated. Member certification as well as certification of completion of unit-designated crew force management requirements to obtain BMC/MR/CMR operational status. Upon certification, the cybercrew member maintains BMC/MR/CMR status based on CT requirements IAW **Chapter 3**.

Chapter 3

CONTINUATION TRAINING (CT)

3.1. CT. The CVA/H RTM and this manual establishes the minimum volume, frequency, and mix of cybercrew training requirements to maintain proficiency in the assigned crew position and at designated certification/qualification levels. The SQ/CC will ensure each cybercrew member receives sufficient training to maintain individual currency and proficiency. **(T-3).**

3.2. Currency. This section establishes the minimum cybercrew member training requirements to maintain BMC or CMR operational status.

3.2.1. The RCP is the formal continuation-training program that provides the baseline for squadrons to use in developing a realistic training program to meet all tasked requirements. The RCP training cycle is 12 months in duration, aligned with the fiscal year, and is executed IAW the RTM. Specific RCP events/tasks are defined in the RTM. The RTM takes precedence over this volume when conflicts exist.

3.2.2. Currency is defined by a total number of RCP training events. Failure to accomplish all training requirements in the RTM may lead to an individual's downgrade by the SQ/CC considering HHQ guidance and the individual's capabilities. **(T-3).**

3.2.2.1. The minimum criteria to log an effective RCP training event requires accomplishing a complete tactical mission profile or building block type mission and tracking RCP sorties IAW the RTM. Each mission must successfully complete a succinct number of events, as detailed in Attachment 1 of the RTM, applicable to the mission type, as determined by the SQ/CC. **(T-3).**

3.2.2.2. Currency may be established or updated by:

3.2.2.2.1. Accomplishing the event as a qualified cybercrew member provided member's currency has not expired. **(T-3).**

3.2.2.2.2. Accomplishing the event as a qualified cybercrew member under supervision of a current instructor. **(T-3).**

3.2.2.2.3. Events satisfactorily performed on any evaluation may be used to establish or update currency in that event. **(T-3).**

3.2.2.2.4. If a crewmember loses a currency the mission or event may not be performed except for the purpose of regaining currency. Non-current events must be satisfied before the crewmember is considered certified/qualified (as applicable) to perform those tasks unsupervised. Loss of currencies affecting CMR status will require downgrade to Non-Combat Mission Ready (N-CMR).

3.2.2.2.5. Multi-position certified individuals must meet currency requirements for each cybercrew position to maintain operational status in all cybercrew positions.

3.2.2.2.6. Cybercrews are expected to maximize all training opportunities. This does not require cybercrew members to log effective RCP missions when minimal RCP training occurs.

3.2.2.2.7. Instructors and evaluators may credit up to 50 percent of their total CT requirements while instructing or evaluating (see the RTM). **(T-2).**

3.2.3. CT Requirements. Completion and tracking of CT is ultimately the responsibility of the individual crewmember. Cybercrew members should actively work with their supervisors, unit schedulers, and training offices to ensure accomplishment of their CT requirements. Cybercrew members attached to units are responsible for reporting accomplished training events to their attached unit. **(T-3).**

3.2.3.1. See the RTM for current CT requirements for all cybercrew positions. Standardized training event identifiers and descriptions are located in Attachment 1 of the RTM. Units will add unit-specific events as required to include a description in their local training documents. **(T-3).**

3.2.4. End of Cycle Requirements. Cybercrew members whom fail to complete mission or event requirements by the end of the training cycle may require additional training depending on the type and magnitude of the deficiency. Refer to **paragraph 3.3** for proration guidance. In all cases, shortfalls are reported to the OG/CC.

3.2.4.1. Failure to meet specific CMR mission type requirements will result in one of the following:

3.2.4.1.1. The SQ/CC determines if the mission type deficiency is significant enough to warrant downgrade to N-MR or N-CMR. To regain CMR the cybercrew member will perform all deficient mission types. These missions may also count toward the total requirements for the new training cycle. **(T-3).**

3.2.4.1.2. Continuation at CMR may be warranted if total RCP missions are maintained and the mission type deficiencies are deemed insignificant by the SQ/CC.

3.2.4.2. Failure to accomplish mission events required for certifications, tradecraft, or capabilities will result in loss of that qualification/certification. The SQ/CC will determine recertification requirements. Requalification requirements are IAW ACCI 17-202 V2, applicable HHQ guidance, and ACCMAN 17-2V2.

3.3. Recurrency Training. A cybercrew member is considered not current upon failure to accomplish CT as specified in **paragraph 3.1**.

3.3.1. Loss of Currency up to 6 Months. A cybercrew member must demonstrate proficiency with an instructor (or designated supervisor) in all delinquent items IAW the RTM. **(T-3).**

3.3.2. Loss of Currency Exceeding 6 Months. Requalification will be accomplished according to **paragraph 2.5**. **(T-3).**

3.4. Proration of Training.

3.4.1. The SQ/CC may prorate any training requirements precluded by the following events: initial arrival date in squadron, emergency leave, non-mission Temporary Duty (TDY), Permanent Change of Station (PCS), or non-mission exercises or deployments. Ordinary annual leave will not be considered as non-availability. Other extenuating circumstances, as determined by the SQ/CC, that prevent the crewmember from mission duties for more than 15 consecutive days may be considered as non-availability for proration purposes. **(T-3).** The following guidelines apply:

3.4.1.1. Proration will not be used to mask training or planning deficiencies.

3.4.1.2. Proration is based on cumulative days of non-availability for mission duties in the training cycle. Proration does not apply to individuals who are available for 15 days or less. Use **Table 3.1** to determine the number of months to be prorated based on each period of cumulative non-mission duty calendar days IAW ACCI 17-202V1. **(T-3).**

3.4.1.3. If MQT is re-accomplished, a crewmember's training cycle will start over at a prorated share following completion of MQT. **(T-3).**

3.4.1.4. Newly assigned cybercrew member achieving CMR or BMC status after the 15th of the month are considered to be in CT on the first day of the following month for proration purposes. A prorated share of RCP events must be completed in CT. **(T-3).**

3.4.1.5. A cybercrew member's last month on station prior to PCSing may be prorated provided 1 month's proration is not exceeded. Individuals PCSing may be considered CMR for reporting purposes during a period of 60 days from date of last training event, or until loss of CMR currency, port call date, sign in at new duty station, or whichever occurs first.

3.4.1.6. Example: Capt Blix was granted 17 days of emergency leave in January and attended SOS in residence from March through April for 56 consecutive calendar days. The SQ/CC authorized a total of two months proration from his training cycle (two months for the 73 cumulative days of non-availability).

Table 3.1. Proration Allowance.

Cumulative Days Of Non-Mission Activity	Proration Allowed (Months)
0 – 15	0
16 – 45	1
46 – 75	2
76 – 105	3
106 – 135	4
136 – 165	5
166 – 195	6
196 – 225	7
226 – 255	8
256 – 285	9
286 – 315	10
316 – 345	11
Over 345	12

3.5. Additional Training. Any training recommended by the Stan/Eval Examiner to remedy deficiencies identified during an evaluation.

3.6. Failure to Complete CT Requirements. Individuals who fail to meet minimum event requirements will be downgraded from a qualified operational status and must perform appropriate actions as identified below to recover qualification.

3.6.1. Declare an individual non-mission ready (N-MR) or non-combat mission ready (N-CMR) if CT requirements are not met for more than 90 Calendar Days (180 Days for BMC and ARC). Downgraded status will begin on the 91st day (181st day for Non-Basic Mission Capability (N-BMC) and N-CMR ARC personnel) following the last training event. **(T-2).**

3.6.1.1. The cybercrew member regains currency by performing the necessary training event under instructor supervision. **(T-3).**

3.6.2. Cybercrew members that fail to accomplish CT requirements and lose currency must only operate in a supervised status IAW ACCI 17-202V1. **(T-2).**

3.6.3. The decision to suspend, retain, or downgrade a cybercrew member's status for failure to meet the standards established by this manual, ACCI 17-202 V1, V2 or ACCMAN 17-2V2 will be documented by citing all which apply. **(T-2)**

Chapter 4

INSTRUCTOR TRAINING AND QUALIFICATION

4.1. Requirements. A qualified CVA/H Instructor shall be a competent subject matter expert adept in the methodology of instruction. The instructor shall be proficient in evaluating, diagnosing, and critiquing student performance, identifying learning objectives and difficulties, and prescribing and conducting remedial instruction. The instructor must be able to conduct instruction in all training venues (e.g., classroom, training devices, ops floor, mission execution, etc.). Instructor trainees will be observed and supervised by a qualified instructor. (T-2).

4.1.1. All instructors should be CMR (wing level and below). Instructors must be current and qualified in any event they instruct. FTU instructors, including USAF Weapons instructors, are only required to maintain BMC.

4.1.2. IAW ACCI 17-202V1 units will develop instructor upgrade syllabi approved by the OG/CC that encompasses at a minimum:

4.1.2.1. Applicable equipment configuration and scheduling procedures (e.g., simulator and on-line equipment configuration, and instruction scenario control procedures). (T-2).

4.1.2.2. Instructional Systems Development (ISD) process and procedures. (T-2).

4.1.2.3. Development, conduct, and administration of classroom training, simulator, ops floor, and field training as appropriate. (T-2).

4.2. Selection and Prerequisites. The SQ/CC will select instructor candidates based on experience, judgement, potential ability to instruct, operating skills, and technical knowledge of the weapon system.

4.2.1. A cybercrew member must be CMR in their crew position for at least 12 months prior to upgrading to an instructor for that crew position. **(T-3).**

4.3. Failure to Meet Instructor Requirements. Instructors may lose instructor status for the following:

4.3.1. Not instructing a course or event at least once every 180 days.

4.3.2. The certifying official deems that loss of currency is of sufficient importance to require complete decertification (but not a complete loss of qualification).

4.3.2.1. As long as the affected cybercrew member retains instructor qualification, recertification will be at the certifying official's discretion IAW ACCI 17-202V2 and ACCMAN 17-2V2.

4.3.2.2. If an instructor loses currency in missions or events, for which the SQ/CC does not require decertification and removal from CMR or BMC status, instructor status may be retained. However the individual will not instruct that mission or event until currency is regained.

4.3.3. Instructor lack of ability. Instructors serve solely at the discretion of the SQ/CC. Instructors will exemplify a higher level of performance and present themselves as reliable and authoritative experts in their respective duty positions. Instructors exhibiting substandard performance should be reviewed for suitability of continued instructor duty.

4.3.3.1. Instructors will be decertified if the SQ/CC deems instructor is substandard, ineffective, or providing incorrect procedures, techniques, or policy guidance.

4.3.3.1.1. Recertification requirements will be at the discretion and direction of the certifying official.

Chapter 5

DOCUMENTATION

5.1. Requirements. In all instances the use of electronic forms, digital signatures and electronic format Individual Training Folders (ITF) is authorized for use. Computer-generated forms must mirror AF Forms as published on the USAF E-Publishing web site as of the date of their use.

5.1.1. Each block of training is documented and maintained in the cybercrew member ITF.

5.1.2. Cybercrew member CT and additional training events are maintained in an ITF. Electronic format ITFs are authorized provided proper security measures, backup capability, and sustainment plans are in place.

5.1.3. Dispose of ITFs and other related material according to the RDS, and AF guidance concerning the protection of Personally Identifiable Information.

5.1.4. ACC Form 4419, *Record of Training*. Cybercrew member training events/tasks can be documented on the ACC Form 4419.

5.1.5. ACC Form 4420, *Individual's Record of Duties and Qualifications*. The ACC Form 4420 is an index providing pertinent training information extracted from all the ACC Forms 4419 accomplished by the cybercrew member.

MARK H. SLOCUM, Maj Gen, USAF
Director of Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

ACCI 17-202 Volume 1, *Cybercrew Training*, 12 January 2021

ACCI 17-202 Volume 2, *Cybercrew Standardization/Evaluation Program*, 12 January 2021

ACCMAN 17-2CVAHV2, *Cyber Vulnerability Assessment/Hunter (CVA/H) - Standardization/Evaluation Program*, 7 December 2020

AFI 16-1007, *Management of Air Force Operational Training Systems*, 1 October 2019

AFI 33-322, *Records Management and Information Governance Program, 23* March 2020

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 March 2020

AFTTP 3-1. *Cyber Vulnerability Assessment/Hunter*, 12 June 2018

AFTTP 3-1. *Advanced Cyber Threat Guide Chapter 13,* 10 December 2018

AFTTP 3-3. (U) *Integrated Planning and Employment*, 3 April 2020 (Contents are (S//NF))

AFTTP 3-3. *Integrated Planning and Employment*, 3 April 2020 (U)

Cyber Technical Manual 7-0.2, *Cyber Mission Force Training & Readiness Manual, Appendix 2, Addendum 1, "CPT Training and Evaluation Outline*," 28 May 2019

Cyber Vulnerability Assessment/Hunter (CVA/H) Ready Cybercrew Program (RCP) Tasking Memorandum (RTM), Fiscal Year (FY) 2021, 25 September 2020

Cyberspace Vulnerability Assessment/Hunter Weapon System Configuration Management Plan, Annex version 2.2., February 2018

Cyber Warfare Publication 3-33.4, *Cyber Protection Team Organization, Functions, and Employment*, 28 January 2020

DAFPD 17-2, *Cyber Warfare Operations*, 27 October 2020

DAFI 33-360, *Publications and Forms Management*, 1 December 2015

DoDI 5400.11, *DoD Privacy and Civil Liberties Program*, 29 January 2019

Privacy Act of 1974 (5 USC § 552a, *Records Maintained on Individuals*), 31 December 1974

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

ACC Form 4418, *Certificate of Cybercrew Qualification*

ACC Form 4419, *Record of Training*

ACC Form 4420, *Individual's Record of Duties and Qualifications*

Abbreviations and Acronyms

ACC—Air Combat Command

ACCI—Air Combat Command Instruction

ACCMAN—Air Combat Command Manual

AF—Air Force

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

AFTTP—Air Force Tactics, Techniques, and Procedures

ARC—Air Reserve Components

BCQ—Basic Cyber Qualified

BMC—Basic Mission Capable

CC—Commander

CCL—Cyber Crew Lead

CMR—Combat Mission Ready

CT—Continuation Training

CTA—Exploitation Threat Analyst

CVA/H—Cyber Vulnerability Assessment/Hunter

DAFI—Department of the Air Force Instruction

DOC—Designed Operational Capability

DO—Director of Operations

DoD—Department of Defense

FTU—Formal Training Unit

HA—Host Analyst

HQ—Headquarters

HHQ—Higher Headquarters

IAW—In Accordance With

IQT—Initial Qualification Training

ISD—Instructional Systems Development

MAJCOM—Major Command

MQT—Mission Qualification Training

MTTL—Master Training Task List

NA—Network Analyst

NAF—Numbered Air Force

N-BMC—Non-Basic Mission Capable

N-CMR—Non-Combat Mission Ready

OG—Operations Group

OPORD—Operations Order

OPR—Office of Primary Responsibility

OSS—Operations Support Squadron

PBED—Planning, Briefing, Execution, and Debriefing

PEX—Patriot Excalibur

PCS—Permanent Change of Station

RCP—Ready Cybercrew Program

RDS—Records Disposition Schedule

RTM—Ready Cybercrew Program Tasking Memorandum

Stan/Eval—Standardization and Evaluation

SQ—Squadron

USAF—United States Air Force

Terms

Basic Cyber Qualified (BCQ)—A cybercrew member who has satisfactorily completed IQT.

Basic Mission Capable (BMC)—A cybercrew member that has received the minimum IQT and MQT training required to be familiar with all missions, but only required to be qualified/certified and proficient in some of the primary Designed Operational Capability (DOC) mission requirements of their assigned unit. This status is normally assigned to crew members with staff functions directly supporting cyber operations (e.g., Wing staff, Operations Support Squadron personnel, etc.).

Certification—Procedure used to document competency in a particular task as determined by a certifying official. Not interchangeable with "qualification", which requires ACC Form 4418, *Certificate of Cybercrew Qualification*, documentation.

Combat Mission Ready (CMR)—A cybercrew member who has satisfactorily completed IQT and MQT, and maintains certification, currency, and proficiency in the command or unit operational mission.

Continuation Training (CT)—Training which provides crew members with the volume, frequency, and mix of training necessary to maintain currency and proficiency in the assigned qualification level.

Currency—A measure of how frequently and/or recently a task is completed. Currency requirements should ensure the average cybercrew member maintains a minimum level of proficiency in a given area.

CVA/H Event—A cyber event (combat or training) constitutes the actions an individual cyberspace force takes to accomplish a tasked mission or effect. Routinely directed actions, maintenance, or hygiene tasks executed IAW established procedures (e.g., blocking an Internet Protocol (IP) address, loading signatures, Domain Name Server blackholing) are not considered events.

CVA/H Mission—The employment of cyberspace capabilities during real-world operations to include CVA/H missions include Discovery and Counter Infiltration, Cyber Readiness, Cyber Support, Cyber Threat Emulation, Mission Protection, and other higher headquarter directed missions.

Cyber Crew Lead—A CVA/H cybercrew member who leads a cybercrew during events. CCL is an upgrade position and be HA or NA

Cyber Threat Analyst (CTA) Special Mission Qualification—A CVA/H CTA tests and evaluates the security of network devices and host systems through the use of advanced exploitation techniques and forensic analysis. A CTA's skills are focused on emulating threats in order to demonstrate vulnerability and risks present on a system or network. They use these same skills, to emulate the threat, to help identify adversary activity or attacks against host or networks systems. Like the HA they have the ability to create scripts, but they are focused on creating them for their test and evaluation purposes and across multiple types of systems in the environment.

Host Analyst—A CVA/H HA specializes in advanced vulnerabilities and threats in hardware and software of host systems. They have the skills & knowledge to assess the configuration, settings, and activity of a targeted host system to identify weak security, vulnerabilities, or maliciously configured systems. They have the expertise to utilize for investigations into an incident or counter threat actions agnostic of operating system. They can assess a targeted host system for health and gather information which other operators can analyze or use to determine actions.

Mission—A set of tasks that lead to a cyber-objective, to include associated planning, brief, execution, and debrief (PBED) events.

Network Analyst—A CVA/H NA specializes in advanced vulnerabilities and threats of network architectures, hardware, technologies, and associated systems. Their knowledge is to the level where they can reconstruct a network by analyzing the data collected from packet captures and flow data. They can identify misconfiguration & malicious activity based on the observable network traffic. They assess the configuration, settings, and activity of a network to identify weak security, vulnerabilities, or maliciously configured network infrastructure. They are the experts to utilize for investigations into an incident or counter threat actions on network infrastructure.

Proficiency—A measure of how well a task is completed. A cybercrew member is considered proficient when they can perform tasks at the minimum acceptable levels of speed, accuracy, and safety.

Qualification Evaluation—Qualifies a cybercrew member to perform the duties of a particular crew position in the specified MDS. Requires ACC Form 4418 documentation.

Ready Cybercrew Program (RCP)—Annual event training requirements for cybercrew to maintain CMR status.

Ready Cybercrew Program Tasking Memorandum (RTM)—Formal document that outlines the RCP continuation training (CT) program for the fiscal year. This memorandum will be updated no later than two months before each new 12-month training cycle.

Specialized Mission Training—Training in any special skills (e.g., tactics, weapon system capabilities, responsibilities, etc.) necessary to carry out the unit's assigned missions that are not required by every crew member. Specialized training is normally accomplished after the crew member is assigned CMR or BMC status, and is normally in addition to CMR or BMC requirements. May be an additional certification and/or qualification event as determined by the SQ/CC.

Status—Assigned to individuals based on the continuation training status (basic cyber qualification, basic mission capable, or mission ready) they are required to maintain.

Training Period—Any training period determined by the Wing in which training requirements are performed.