BY ORDER OF THE COMMANDER OF AIR COMBAT COMMAND

AIR COMBAT COMMAND MANUAL 17-2CVAH, VOLUME 2

28 OCTOBER 2024

Incorporating Change 1, 28 MAY 2026

Certified Current, 28 MAY 2026

Cyberspace Operations

CYBER VULNERABILITY ASSESSMENT/HUNTER (CVA/H) – STANDARDIZATION/EVALUATION PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at www.e-Publishing.af.mil.

RELEASABILITY: There are no release restrictions on this publication.

OPR: ACC/A3TV

Certified by: ACC/A3/26

Supersedes: ACCMAN17-2CVAHV2, 7 December 2020

Pages: 24

This manual implements the Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyber Warfare Operations*. It establishes the Cybercrew Standardization and Evaluation (Stan/Eval) procedures and evaluation criteria for qualifying crew members on the Cyber Vulnerability Assessment/Hunter (CVA/H) weapon system. This publication applies to all Air Combat Command (ACC), Air Force Reserve (AFR), Air National Guard (ANG), and third-party governmental and contract support agencies in accordance with (IAW) appropriate provisions contained in support agreements and Air Force (AF) contracts. It does not apply to the United States Space Force. This publication requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized by Air Force Instruction (AFI) 36-2608, *Military Personnel Records System*. The applicable System of Records Notice (SORN) F011 AF AFMC B, Patriot Excalibur (PEX) System Records, applies and is available at: **https://pclt.defense.gov/DIRECTORATES/Privacy-and-Civil-Liberties-Directorate/Privacy/SORNsIndex/DoD-Component-Notices/Air-Force-Article-List/**. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) (ACC Standardization Branch [ACC/A3TV]) using the Department of the Air Force (DAF) Form 847, *Recommendation for*

Change of Product; route DAF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all supplements must be routed to the OPR of this publication for coordination before certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures*, for a description of the authorities associated with the Tier numbers. Waiver authority for non-tiered paragraphs remains with the ACC Director of Operations (ACC/A3). Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority. Using the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the DAF.

SUMMARY OF CHANGES

This change removes ACC QUAL/MSN requirements for basic, senior, and master upgrades. US Cyber Command has requirements in place for basic, senior, and master upgrades that fulfil the ACC requirements.

Chapter 1

GENERAL INFORMATION

1.1. Objectives. The Cyber Vulnerability Assessment/Hunter (CVA/H) Stan/Eval Program is the commander's (CC's) tool to validate cybercrew member mission readiness and their effectiveness on live and simulated CVA/H missions, to include documentation of individual qualifications and capabilities.

1.2. General. This manual applies to all units with a readiness requirement for CVA/H. This publication establishes requirements and grading for all initial and periodic CVA/H cybercrew evaluations. All CVA/H evaluations will be conducted IAW this publication and ACC Instruction (ACCI) 17-202, Volume 2, *Cybercrew Standardization/Evaluation Program*, as supplemented. Specific areas of evaluation are prescribed to ensure an accurate assessment of the proficiency and capability of CVA/H operators. Additionally, for this manual and uniformity with United States Cyber Command (USCYBERCOM) guidance, the term "work role" will be synonymous with "crew position" as defined and used in ACCI 17-202, Volume 1, *Cybercrew Training*; ACCI 17-202V2 and ACCI 17-202, Volume 3, *Cybercrew Operations and Procedures*. Roles and responsibilities for executing this publication are IAW ACCI 17-202V2.

1.2.1. Alignment of ACC operational statuses to USCYBERCOM-defined terms. CVA/H is leveraged by US Air Force Cyber Protection Teams (CPT) to execute a USCYBERCOM mission. As such, this volume utilizes USCYBERCOM-defined terminology (such as the proficiency levels of Basic, Senior, and Master) in place of many standard ACC terms, including the use of operational statuses common across other USAF Mission Design Series (MDS) platforms (such as Basic Cyber Qualified (BCQ) and Combat Mission Ready (CMR)). The most accurate alignment of the ACC operational statuses to USCYBERCOM-defined terms is demonstrated in **Table 1.1** below.

Table 1.1. ACC and USCYBERCOM Terminology Alignment.

ACC	USCYBERCOM
BCQ	Fully Trained (FT)
CMR	Fully Mission Qualified (FMQ)-Basic and FMQ-Senior/Master

1.2.2. This publication does not apply to AF units executing joint cyber missions under operational control (OPCON) to the Cyber National Mission Force; however, unit CCs are encouraged to leverage guidance in this publication to the extent that it is consistent with joint guidance issued by proper authority.

1.3. Keywords and Definitions.

1.4. Waivers. Complete waivers IAW DAFMAN 90-161 and route IAW 16th AF (16 AF) guidance. Send copies of approved waivers to ACC/A3TV. Document waivers in Stan/Eval Board (SEB) minutes.

1.5. Supplements. Units are encouraged to supplement this instruction with Stan/Eval profiles that best fit the unit's mission, equipment, and location. Cyberspace Operations Groups (COGs) will forward their supplements to the ACC Flight Operations Division (ACC/A3T) for approval before publication. Units will forward one copy of each unit supplement to ACC/A3TV for prepublication review before approval.

1.6. Evaluation Procedures. Stan/Eval Examiners (SEEs) will brief the examinee on the conduct, purpose, and requirements of the evaluation, as well as all applicable evaluation criteria, before mission execution. The examinee will accomplish all required mission planning relevant to the position they are being evaluated on. The SEE should not occupy a work role during evaluations. If an assessment is conducted during operations, the evaluator will inform the Mission Element Lead (MEL) of any special requirements and must ensure they prioritize the evaluations and only involve themselves in operations when necessary.

1.6.1. SEEs will ensure required training and documentation is complete prior to all evaluations.

1.6.2. The examinee will meet currency requirements as required prior to all evaluations.

1.6.3. SEEs will thoroughly debrief/critique all aspects of the evaluation. During the critique, the SEE will review the examinee's overall rating, specific deviations, area/subarea grades assigned, and any additional training required. If additional training is required for areas outside of the evaluation, it will be documented under the appropriate section on ACC Form 4418, *Certificate of Cybercrew Qualification,* or AF Form 8, *Certificate of Aircrew Qualification*.

1.6.4. All evaluation activity should be scheduled on one event to the greatest extent possible. If a required event is not accomplished during a mission, the event may be completed in a part-task training scenario and documented on ACC Form 4418 or AF Form 8. If required portions of an evaluation cannot be observed during a single mission/event, they may be evaluated as a separate event (e.g., training event or simulator profile). However, the evaluation will not remain open for greater than 14 calendar days (60 days for AFR/ANG) without Certifying Official approval.

1.6.5. Unit examiners may give evaluations outside their organization, including administering evaluations between ACC, AFR, and ANG, provided written agreements/understandings between the affected organizations are in place. Written agreements/understandings will be reviewed and updated annually by the involved organizations.

1.6.6. SEEs may be used as instructors for any phase of training for which they are qualified to capitalize on expertise and experience. SEEs will not evaluate students with whom they have instructed 50% or more of the qualification/upgrade training or those they recommend for qualification/upgrade evaluation without unit Certifying Official approval. Additionally, SEEs will not evaluate direct supervisors or supervisees without unit Certifying Official approval.

1.6.7. All crewmembers of the mission/event (to include students, instructors, examinees, and evaluators) will participate in and adhere to all required mission planning, mission briefing, mission execution, and mission debriefing requirements for their respective roles. **(T-3)**

1.7. Grading Instructions. SEEs will use the grading policies in ACCI 17-202V2, as supplemented, and the evaluation criteria in this instruction for conducting all performance evaluations. All evaluations assume a stable operating environment and normal operating conditions. To ensure standard and objective evaluations, SEEs will be thoroughly familiar with the prescribed evaluation criteria.

1.8. Evaluation Requirements.

1.8.1. Squadrons will design and maintain evaluation profiles incorporating requirements in the applicable grading criteria. Evaluation profiles will follow Higher Headquarters (HHQ) guidance and be approved by the group Stan/Eval (OGV). They will outline the minimum number and type of events to be performed and observed to complete the evaluation. Periodic evaluations will only be required for the highest qualification level obtained; this means that a Master is presumptively qualified as a Senior and will not be periodically evaluated as a Senior, and a Senior is presumptively qualified as a Basic and will not be periodically evaluated as a Basic.

1.8.2. Evaluation tables are provided in **Chapter 2** and **Chapter 3** to summarize evaluation areas.

1.8.3. Written Examinations. The written examination will be accomplished before the performance phase unless in conjunction with a No-Notice (N/N) QUAL. **(T-3)**

1.8.4. Emergency Procedures Evaluation (EPE). Every MSN evaluation will include EPE. EPE will evaluate the crewmember's knowledge and performance of emergency procedures.

1.8.5. Qualification Evaluations (QUALs). These evaluations measure a crewmember's ability to meet graded areas listed in this publication, in accordance with IAW ACCI 17-202V2. QUALs validate a core set of tasks and knowledge that are common amongst all operators.

1.8.5.1. There are no technical areas of specialization within these grading areas where one member, based on their work role qualification, is expected to know more than another operator with a different qualification.

1.8.5.2. The 100-series graded areas for QUALs are listed on **Table 2.1** and defined in **paragraph 2.3** of this manual.

1.8.6. Mission Evaluations (MSNs). The MSN evaluation will reflect the type and difficulty of tasks required to fulfill the CVA/H operational mission and align with the performance measures, mission essential tasks, and core functions outlined in the Cyber Technical Manual (CTM) 7-02, *Cyber Mission Force Training and Readiness Manual*.

1.8.6.1. Evaluation profiles will reflect a sampling of the unit's mission taskings and will be approved by the COG/OGV or equivalent. Squadrons will design and maintain at least two approved evaluation profiles for each work role. Squadrons may use OGV general mission evaluation profiles if they are a suitable representation of the unit's mission.

1.8.6.2. For cybercrew members to maintain multiple crew qualifications, periodic MSN evaluations must be conducted for each qualification. **(T-2)**

1.8.6.3. The 200-series graded areas for MSN evaluations are listed on **Table 2.2** and defined in **paragraph 2.5** of this manual.

1.8.7. To promote efficient use of resources, QUAL and MSN evaluations will be administered in conjunction with each other. When practical, evaluations may be completed during mission execution.

1.8.8. Instructor Evaluations (INSTRs). These evaluations measure a crewmember's ability to meet graded areas listed in this publication, IAW ACCI 17-202V2.

1.8.8.1. Awarding a "U" in any Instructor Grading Criteria areas will result in a Q3 for the overall instructor grade. When instruction is combined with a QUAL and MSN evaluation, the overall grade for the instructor portion of the evaluation will be no higher than the lowest overall grade awarded under QUAL and MSN. **(T-2)**

1.8.8.2. The 300-series graded areas for INSTR evaluations are listed on **Table 3.1**.

1.8.9. When practical, periodic INSTR evaluations should be combined with periodic QUAL or MSN evaluations, as applicable to the work role.

1.8.10. SEE Objectivity Evaluations. SEE Objectivity Evaluation grading criteria can be found in **Attachment 5** of ACCI 17-202V2.

1.8.11. N/N Evaluations. OGV will determine N/N evaluation procedures/goals.

1.8.12. SPOT Evaluations. These evaluate specific criteria or requirements without intending to satisfy the periodic and initial evaluation requirements. They are most often used to assess areas highlighted in the trend analysis program and to re-assess areas that have been marked down during an evaluation.

1.8.13. Additional Training. SEEs are responsible for assigning additional training at their discretion. Document additional training and completion IAW ACCI 17-202V2.

Chapter 2

WORK ROLE EVALUATIONS AND GRADING CRITERIA

2.1. General. The grading criteria contained in this chapter apply to evaluations for CVA/H HA and NA. Any work role that falls outside of the below grading criteria may be accounted for on the unit Letter of Certifications (LOX) and, if required, may have grading criteria outlined in a supplement to this manual. These criteria were derived from experience, policies, and procedures outlined in weapon/mission system manuals and other directives. Evaluators must realize that the grading criteria herein cannot accommodate every situation. Written parameters must be tempered with mission objectives and, more importantly, mission/task accomplishment to determine overall cybercrew performance. Requirements for each evaluation phase are explained in the following sections.

2.2. Performance phase: The SEE will follow a pre-planned script/scenario using an evaluation profile to evaluate a member and ensure standardization and consistency of the evaluation process.

Table 2.1. Work role Specific Requirements - Performance Phase QUAL Evaluations.

Area	Title	HA	NA
Pre-Event / Mission Actions			
101	Verify Go / No-Go Status	R	R
102	Conduct Mission Planning	R	R
103	System Operations Check (**Critical**)	R	R
Crew Integration			
111	Crew Coordination	R	R
112	Crew Discipline (**Critical**)	R	R
113	Situational Awareness	R	R
Post-Event / Mission Actions			
121	Debrief	R	R

Work role	**Requirement Abbreviations**
NA – Network Analyst HA – Host Analyst	R – Required

2.3. Qualification Evaluation (QUAL) Criteria. 100-series Areas are common to all work roles and will be used for all applicable evaluations.

2.3.1. **Area 101, Verify Go/No-Go Status.**

2.3.1.1. Q. Verified status for Go/No-Go IAW local procedures. If necessary, complete any required tasks necessary to meet the Go status.

2.3.1.2. Q-. Completed some, but not all required tasks to meet Go status.

2.3.1.3. U. Failed to complete Go/No-Go requisites. Lack of actions caused significant delays or a lack of ability to execute the mission. Inadequate actions impacted mission effectiveness.

2.3.2. **Area 102, Conduct Mission Planning.**

2.3.2.1. Q. Participated in mission planning efforts IAW procedures prescribed in applicable guidance manuals, instructions, and directives. Tasks developed in planning were appropriate for the work role being evaluated, can be reasonably accomplished during evaluation, and are suitable for the given mission profile. Minor errors/deviations/omissions that did not negatively affect mission effectiveness.

2.3.2.2. Q-. Errors, deviations, and omissions had a minor impact on mission effectiveness or efficiencies but did not negatively affect mission accomplishment or jeopardize mission success.

2.3.2.3. U. Failed to lead or contribute to mission-planning effort adequately. Failure to comply with procedures prescribed in applicable guidance manuals, instructions, and directives contributed to significant deficiencies in mission execution/accomplishment.

2.3.3. **Area 103, System Operations Check (Critical).**

2.3.3.1. Q. Performed all weapon system configurations, operations checks, and mission tasks required according to mission/mission profile. Ensured, determined, and verified weapon system operational state before execution actions. Showed competency in the weapon system's characteristics and appropriate application of weapon system capabilities to meet mission objectives. Minor errors or deviations did not detract from mission performance or completion of objectives.

2.3.3.2. U. Did not perform mission/operations checks or monitoring systems to the degree that an emergency/unsafe condition could have developed and damage to equipment could have occurred if allowed to continue uncorrected. Did not understand the employment of core weapon system capabilities toward completing mission objectives. Excessive delay in completing required checklists or employing weapon system capabilities. Errors/deviations/omissions contributed to jeopardizing mission success.

2.3.4. **Area 111, Crew Coordination.**

2.3.4.1. Q. Effectively coordinated with other crewmembers or evaluator acting as a specific crewmember during all phases of the mission enabling efficient, well-coordinated actions. Demonstrated basic knowledge of other crewmembers' duties and responsibilities. Proactively provided direction and/or information to the crew or evaluator acting as a crewmember; communicated in a clear and effective manner and requested or provided constructive feedback as necessary.

2.3.4.2. Q-. There were some breakdowns in communication, but they did not detract from the overall mission success. They were limited in basic knowledge of other crewmembers' duties/responsibilities. Unclear communication at times caused confusion and limited crew interaction. Some unnecessary prompting is required from other crewmembers and or evaluator.

2.3.4.3. U. Severe breakdowns in coordination led to possible mission ineffectiveness/failure or jeopardized safety of crewmembers. Lacked basic knowledge of other crewmember's duties and responsibilities. Unclear and lack of communication or excessive prompting required by crewmembers or evaluator put the mission and safety of others at risk.

2.3.5. **Area 112, Crew Discipline (Critical).**

2.3.5.1. Q. Demonstrated strict professional crew discipline throughout all phases of the mission. Led or supported (based on work role) the planning, briefing, execution, and debriefing of the mission IAW applicable instructions and directives.

2.3.5.2. U. Failed to demonstrate strict professional crew discipline during any phase of the mission. Violated or failed to comply with applicable instructions and directives, which jeopardized safety of crewmembers or mission accomplishment.

2.3.6. **Area 113, Situational Awareness.**

2.3.6.1. Q. Conducted the mission with a sense of understanding/comprehension and in a timely, efficient manner. Anticipated situations that would have adversely affected the mission and made appropriate decisions based on available information. Maintained overall good situational awareness. Recognized temporary loss of situational awareness in self or others and take appropriate action to regain awareness without detracting from mission accomplishment or jeopardizing safety.

2.3.6.2. Q-. Conducted the mission with some anticipation of situations. Situational awareness of some events or situations had a minor impact on mission effectiveness but did not jeopardize mission success.

2.3.6.3. U. Actions were performed that directly resulted in mission failure. Situational awareness was not corrected in a timely, efficient manner, in a way that contributed to safety or mission accomplishment being compromised.

2.3.7. **Area 121, Debrief.**

2.3.7.1. Q. Thoroughly debriefed the mission and/or contributed to the briefing content to ensure it included all pertinent items. Provided MEL with applicable input on all required mission/crew/system-related events, including mission log/report information. Used applicable checklist(s) as required. Minor errors/omissions/deviations did not negatively affect mission effectiveness or efficiencies.

2.3.7.2. Q-. Led or contributed to debriefing effort with minor errors, omissions, and deviations. Some events out of sequence with some unnecessary redundancy. Briefing or input anomalies had minor impact on mission effectiveness but did not jeopardize mission success.

2.3.7.3. U. Inadequate leadership or participation in briefing development and/or presentation. Errors, omissions, or deviations jeopardized mission success.

2.4. MSN Evaluations:

2.4.1. The written examination will consist of an open-book or closed-book examination with a minimum of 15 questions from the unit Secure Question Bank (SQB) or CVA/H MQF,

respectively. All written exams will be approved by OGV or designee and will only contain questions specific to the work role being evaluated.

2.4.1.1. If utilized, open-book examinations will be derived from applicable operations manuals and governing directives related to operations guidance, as well as any references contained therein.

2.4.2. Performance phase: The SEE will use a pre-planned script or scenario following an evaluation profile to evaluate a member and ensure standardization and consistency of the evaluation process.

Table 2.2. Work role Specific Requirements - Performance Phase MSN Evaluations.

Area	Title	HA	NA
Conduct Defensive Cyberspace Operations			
201	Identify, enumerate, and characterize the AO	R	R
202	Identify the cyber related risks to the supported mission	R	R
203	Develop sensor employment plan to identify adversary presence	R	R
204	Conduct operational reporting to support HHQ decision making	R	R
205	Identify malicious activity based on reporting to determine response actions	R	R
206	Identify scope of adversary access to determine extent of intrusion	R	R
Clear Assigned Area			
211	Contain malicious activity to prevent adversary freedom of action	R	R
212	Contain malicious access to inhibit adversary entry into specified key terrain	R	R
213	Perform basic malware triage to advise response and hardening actions	R	R
214	Execute triage level case management to preserve adversarial artifacts	R	R

Area	Title	HA	NA
215	Eradicate dedicated malicious activity and access to remove adversarial presence	R	R
221	Analyze attack surface of the specified key terrain to enable hardening actions	R	R
222	Recommend and assist with threat mitigation actions to reduce operational risk	R	R
Conduct Operational Assessments			
231	Analyze information to determine root cause of intrusion	R	R
232	Conduct defensive monitoring on the specified key terrain to validate post mitigation actions	R	R
Emergency Procedures			
233	Emergency Procedures (**Critical**)	R	R

Work role	**Requirement Abbreviations**
NA – Network Analyst HA – Host Analyst	R – Required

2.5. Mission Evaluation (MSN) Criteria. 200-series areas are common to all work roles and will be used for all applicable evaluations. However, tasks required to complete areas may differ between work roles.

2.5.1. **Area 201. Identify, Enumerate, and Characterize the Area of Operations (AO)** .

2.5.1.1. Q. Effective and timely application of weapon systems to enumerate and identify endpoints within the assigned AO according to mission plans, directives, orders, or standards. Data is presented in the expected format to enable building and refining network maps or other means of maintaining situational awareness of endpoint presence within the terrain and informing follow-on actions.

2.5.1.2. Q-. Tasks were completed at a different time than the expected standard or format but only resulted in minor mission delays.

2.5.1.3. U. Tasks not completed in the allotted time or to the expected standard or format. Deficiencies resulted in significant delays or impacted the ability to meet mission objectives.

2.5.2. **Area 202. Identify the Cyber Related Risks to the Supported Mission** .

2.5.2.1. Q. Able to identify and explain Key Terrain-Cyber (KT-C) by analyzing provided intelligence and support documentation.

2.5.2.2. Q-. Able to identify some, but not all, KT-C by analyzing provided intelligence and/or support documentation. Unable to provide complete explanation of identified KT-C.

2.5.2.3. U. Failed to identify KT-C. Unable to provide explanation of any identified KT-C.

2.5.3. **Area 203. Develop Sensor Employment Plan to Identify Adversary Presence** .

2.5.3.1. Q. Able to analyze Mission Relevant Terrain-Cyber (MRT-C) and provided intelligence and/or support documentation to identify sensor placement to meet mission objectives and provides employment recommendation to MEL.

2.5.3.2. Q-. Developed sensor employment plan but failed to incorporate all relevant intelligence and/or support documentation. Delays impacted the ability to meet mission objectives.

2.5.3.3. U. Failed to develop adequate sensor employment plan and/or failed to incorporate intelligence and/or support documentation. Significant delays impacted the ability to complete mission.

2.5.4. **Area 204. Conduct Operational Reporting to Support HHQ Decision Making** .

2.5.4.1. Q. Reported all relevant observations and supporting information to MEL.

2.5.4.2. Q-. Reported most, but not all relevant observations and supporting information to MEL. Omitted information resulted in minor mission delays or resulted in inability to meet all mission objectives.

2.5.4.3. U. Failed to include appropriate observations and supporting information in reporting. Omissions in reporting caused significant mission delays and/or failure to complete mission objectives.

2.5.5. **Area 205. Identify Malicious Activity Based on Reporting to Determine Response Actions** .

2.5.5.1. Q. Able to effectively investigate Indicators of Compromise (IOCs) or identify anomalous or suspicious activity to determine with confidence if an incident is malicious. Able to document and classify findings within common threat/frameworks and provide relevant and appropriate response actions.

2.5.5.2. Q-. Concepts not applied efficiently, leading to minor mission delays or slightly reduced confidence in analyzing scoping and investigating suspected intrusion. There was a slight loss of situational awareness of adversary actions, but it still enabled effective targeting and engagement actions.

2.5.5.3. U. Concepts not applied effectively or thoroughly, causing mission delays or insufficient understanding of an intrusion, leading to ineffective remediation actions and increasing risk to the supported mission. Loss of situational awareness of the adversary due to the inability to identify and monitor adversary activity led or might have led to ineffective targeting and engagement actions.

2.5.6. **Area 206. Identify Scope of Adversary Access to Determine Extent of Intrusion** .

2.5.6.1. Q. Able to scope the depth and breadth of a suspected intrusion across the tasked AO. Able to document and classify findings within common threat frameworks and able

to provide relevant and appropriate response actions. Used appropriate resources to re-create attack chain and actions on objectives.

2.5.6.2. Q-. Failed to scope adversary access, leading to the incomplete reconstruction of intrusion and impact on the supported mission. Significant delays impacted the ability to meet mission objectives.

2.5.6.3. U. Failed to identify adversary access or scope of intrusion beyond initial observation. Delays led to inability to meet mission objectives.

2.5.7. **Area 211. Contain Malicious Activity to Prevent Adversary Freedom of Action** .

2.5.7.1. Q. Successfully applied appropriate rules and/or policies on devices to prevent adversary freedom of action as specified in the scenario. Errors in the process were self-corrected and caused a minimal delay in the completion of mission objectives.

2.5.7.2. Q-. Incorrect or errors in rules and/or policies failed to prevent adversary actions on key terrain or caused moderate delay in completion of mission objectives.

2.5.7.3. U. Inability to create rules and/or policies failed to prevent adversary actions on key terrain. Rules and/or policies inhibited mission execution or negatively impacted supported mission operations.

2.5.8. **Area 212. Contain Malicious Access to Inhibit Adversary Entry into Specified Key Terrain** .

2.5.8.1. Q. Successfully applied appropriate rules and/or policies on devices to impede adversary access into terrain as specified in the scenario. Errors in the process were self-corrected and caused a minimal delay in the completion of mission objectives.

2.5.8.2. Q-. Incorrect or errors in rules and/or policies failed to impede adversary access into key terrain or caused a moderate delay in completing mission objectives.

2.5.8.3. U. Inability to create rules and/or policies failed to impede adversary access into key terrain. Rules and/or policies inhibited mission execution or negatively impacted supported mission operations.

2.5.9. **Area 213. Perform Basic Malware Triage to Advise Response and Hardening Actions** .

2.5.9.1. Q. Able to accurately characterize observed malware. Performed triage safely and provided appropriate response and hardening action advice. Conducted reporting actions IAW unit Standard Operating Procedures (SOPs).

2.5.9.2. Q-. Partially characterized observed malware or performed did not complete triage. Provided partial response and hardening action advice. Actions caused minimal delay in completion of mission objectives but had minimal impact supported mission operations.

2.5.9.3. U. Failed to properly characterize observed malware or performed triage in an unsafe manner. Was unable to provide appropriate response and hardening action advice. Actions taken or not taken had a severe impact on the completion of mission objectives and supported mission operations.

2.5.10. **Area 214. Execute Triage Level Case Management to Preserve Adversarial Artifacts** .

2.5.10.1. Q. Triage case management was conducted. Identified key artifacts that allow for follow-on actions by other cybercrew. All artifacts are included with documentation for preservation.

2.5.10.2. Q-. Triage case management did not include all artifacts found or did not provide the appropriate level of detail. Lack of information had minimal delay in the completion of mission objectives.

2.5.10.3. U. Failed to properly document triage or provide artifacts. Lack of information had significant delay in completion of mission objectives or degraded supported mission operations.

2.5.11. **Area 215. Eradicate Dedicated Malicious Activity and Access to Remove Adversarial Presence** .

2.5.11.1. Q. Able to target and engage threats on the defended terrain, if authorized and directed, to the extent that the adversary is unable to sustain unauthorized access to the environment through identified Tactics, Techniques, and Procedures (TTPs) or create, Deny, Degrade, Disrupt, Deceive and Manipulate effects.

2.5.11.2. Q-. Concepts not applied efficiently and coordinated, leading to minor mission delays or reduced confidence in the thorough completion of threat response actions. Lack of thorough engagement plans requires minor re-engagements but does not allow the adversary to impact the supported mission or gain freedom of maneuver or advantage in the environment.

2.5.11.3. U. Concepts not applied effectively allow an adversary to gain an advantage in the environment and will enable the adversary freedom of maneuver or action.

2.5.12. **Area 221. Analyze Attack Surface of the Specified Key Terrain to Enable Hardening Actions** .

2.5.12.1. Q. Able to provide appropriate recommendations for hardening of KT-C using observations identified during mission execution and relevant mission documentation/Intelligence.

2.5.12.2. Q-. Several minor details overlooked or incorrectly analyzed, leading to incomplete hardening action recommendations. Actions caused minimal delay in completion of mission objectives but had minimal impact supported mission operations.

2.5.12.3. U. Failed to appropriately characterize KT-C attack surface or failed to provide appropriate hardening action recommendations.

2.5.13. **Area 222. Recommend and Assist with Threat Mitigation Actions to Reduce Operational Risk** .

2.5.13.1. Q. Able to provide recommendations for threat mitigation using observations identified during mission execution and relevant mission documentation/intelligence. Minor errors, deviations, and omissions did not negatively affect mission accomplishment.

2.5.13.2. Q-. Provided incomplete recommendations for threat mitigation actions or was unable to fully assist with implementing recommendations.

2.5.13.3. U. Unable to provide appropriate recommendations for threat mitigation or not able to assist with implementing recommendations.

2.5.14. **Area 231. Analyze Information to Determine Root Cause of Intrusion** .

2.5.14.1. Q. Able to effectively assess the root cause of intrusion, including such details as date/time, method(s), and relevant account(s).

2.5.14.2. Q-. Able to correctly assess key parts of the intrusion but lacks some details.

2.5.14.3. U. Unable to assess root cause of intrusion or lacks significant key details.

2.5.15. **Area 232. Conduct Defensive Monitoring on the Specified Key Terrain to Validate Post-Mitigation Actions** .

2.5.15.1. Q. Able to assess the effectiveness of engagement activities executed internally to the crew or by other forces based on identified and scoped intrusions into friendly cyberspace and planned engagement actions.

2.5.15.2. Q-. Inefficient use of weapon system capabilities or identified IOCs results in a minor increase in the timeline of delivery or a reduction in assessment confidence, but overall assessment is sufficient to inform the common operational picture.

2.5.15.3. U. Ineffective use of weapon system capabilities or identified IOCs results in incorrect, incomplete, or unnecessarily low confidence assessment of adversary engagement.

2.5.16. **Area 233. Emergency Procedures (Critical)**.

2.5.16.1. Q. Recognized emergencies or malfunctions promptly and demonstrated and/or explained appropriate response actions. If applicable, demonstrated/explained effective coordinated emergency actions with other crewmembers without delay or confusion. Followed appropriate checklists as required. Minor errors did not exacerbate the emergency. (this area may be evaluated orally).

2.5.16.2. U. Failed to recognize emergency situations or malfunctions. Failed to demonstrate or explain proper response actions. Failed to demonstrate and/or explain knowledge of location or proper use of emergency equipment or checklists. If applicable, failed to demonstrate/explain coordinated emergency actions with other crewmembers. Checklist errors/omissions/deviations contributed to ineffective actions or exacerbated an emergency and/or malfunction.

Chapter 3

INSTRUCTOR EVALUATIONS AND GRADING CRITERIA

3.1. General. The instructor grading criteria apply to initial, Requalification (RQ), and all periodic INSTR evaluations. The examinee must demonstrate the ability to safely and effectively instruct. Instructors must demonstrate instructional ability on all periodic evaluations to maintain instructor qualification.

3.2. Requirements. Instructors must maintain qualification in all areas they will instruct. INSTR evaluations should be accomplished with periodic assessment but may be in an operational or classroom setting so long as all evaluation criteria have been met. If able, conduct initial INSTR evaluations with candidates instructing actual students. Otherwise, the SEE may act as the student. An RQ INSTR evaluation is required anytime an instructor loses qualification for any reason, including CC-directed downgrades.

3.3. Instructor Upgrade and Qualification Requisites. Before an initial INSTR, Instructor examinees must have completed all requisites for Instructor upgrade consideration, nomination, and training IAW ACCI 17-202V1; ACCMAN 17-2CVAH, Volume 1, *Cyber Vulnerability Assessment/Hunter (CVA/H) – Cybercrew Training*; and all applicable supplemental guidance.

3.4. Instructor Qualification Evaluations (INSTR). Units should strive to combine instructor evaluations (initial and periodic) with periodic QUAL or MSN evaluations. INSTR evaluations can only be combined with QUAL or MSN evaluations when the examinee is in their periodic eligibility period.

3.4.1. Initial INSTR evaluations should be conducted with a student occupying the applicable CVA/H work role whenever possible. Periodic INSTR evaluations may be conducted with the SEE role-playing as the student.

3.4.2. The instructor examinee will monitor all mission phases from an advantageous position and be prepared to demonstrate or explain any area or procedure. The SEE will note the instructor's ability to recognize student difficulties and provide effective, timely instruction and/or corrective action. The SEE will also evaluate the grade assigned and the completed grade sheet or event training form for the student on all initial instructor checks.

3.4.3. The student will perform those duties prescribed by the instructor for the mission/event being accomplished. If an actual student is not available, the SEE will identify to the examinee (before the mission) the level of performance to be expected from the SEE acting as the student. If this option is utilized, at least one event or briefing must be instructed. **(T-3)**

3.4.4. If performed with periodic QUAL or MSN evaluations, the examinee must occupy the primary duty position for an adequate period to demonstrate proficiency in the work role with required QUAL evaluations. All INSTR evaluations will include a pre-mission and post-mission briefing. **(T-3)**

3.4.5. Awarding a "U" in any Instructor Grading Criteria areas will result in a Q3 for the overall instructor grade. The overall grade for the instructor portion of the evaluation will be no higher than the lowest overall grade awarded under QUAL.

Table 3.1. Instructor (INSTR) Specific Requirements - Performance Phase Evaluations.

Area	Title	INSTR
INSTR Criteria		
301	Instructional Ability	R
302	Instructional Briefings / Critique	R
303	Knowledge, Demonstration and Performance	R
Upgrade Position INSTR – Instructor		**Requirement Abbreviations** R – Required

3.5. Instructor Evaluation (INSTR) Criteria. All INSTR Criteria must be observed and graded to ensure a complete evaluation. The following general evaluation grading criteria are common to all work roles and will be used for all applicable instructor evaluations:

3.5.1. **Area 301. Instructional Ability.**

3.5.1.1. Q. Demonstrated ability to develop and assess effective learning objectives, dynamically evaluate student progress, and effectively adapt instruction to the student's needs. Provided appropriate and timely corrective guidance when necessary and communicated clearly. Correctly analyzed student errors and offered constructive feedback.

3.5.1.2. Q-. Instructional inputs were too soon or overly abundant in such a way that instruction could have been more focused, or other minor discrepancies in the above criteria that did not adversely impact student progress.

3.5.1.3. U. Unable to effectively communicate with the student. Did not provide corrective action where necessary. Did not plan or anticipate student problems. They incorrectly analyzed student errors or appropriate levels of instruction. Actions and techniques adversely impacted student progress.

3.5.2. **Area 302. Instructional briefings/critique** .

3.5.2.1. Q. Briefings were well organized, accurate, and thorough. Reviewed student's present level of training and defined mission events to be performed. Demonstrated ability during critique to reconstruct the mission/event, offer mission analysis, and provide corrective guidance where appropriate. Completed all training documents according to prescribed directives. Appropriate grades awarded. Correctly followed and implemented student's training syllabus.

3.5.2.2. Q-. As above but with minor errors or omissions in briefings, critique, or training documents that did not adversely impact student progress.

3.5.2.3. U. Pre-mission or post-mission briefings were marginal or nonexistent. Did not review student's training folder or past performance. Failed to critique students adequately or conducted an incomplete mission analysis compromised learning. Student strengths or weaknesses were not identified and adversely impacted student progress. Inappropriate grades awarded. Overlooked or omitted significant discrepancies. Did not follow or administer syllabus directives appropriately.

3.5.3. **Area 303. Knowledge, demonstration and performance** .

3.5.3.1. Q. Effectively demonstrated procedures and techniques. Demonstrated thorough knowledge of weapon system/components, procedures, and all applicable publications and regulations.

3.5.3.2. Q-. Minor discrepancies in the above criteria that did not adversely impact student progress.

3.5.3.3. U. Did not demonstrate correct procedure or technique. Insufficient depth of knowledge about weapon system/components, procedures, or proper source material. Adversely impacted student progress.

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

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION.

References

ACCI 17-202V1, *Cybercrew Training*, 12 January 2021

ACCI 17-202V2, *Cybercrew Standardization/Evaluation Program*, 12 January 2021

ACCI 17-202V3, *Cybercrew Operations and Procedures*, 12 January 2021

ACCMAN 17-2CVAHV1, *Cyber Vulnerability Assessment/Hunter (CVA/H) – Training*, 28 October 2024

ACCMAN 17-2CVAHV3, *Cyber Vulnerability Assessment/Hunter (CVA/H) – Operations and Procedures*, 28 October 2024

AFCYBER *Joint Qualification Record and Individual Qualification Program Guidance*

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

CTM 7-02, *Cyber Mission Force Training and Readiness Manual*, 22 February 2018

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

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

Prescribed Forms

None

Adopted Forms

ACC Form 4418, *Certificate of Cybercrew Qualification*

AF Form 8, *Certificate of Aircrew Qualification*

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

AF—Air Force

AFCYBER—Air Force Cyber

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFR—Air Force Reserve

ANG—Air National Guard

AO—Area of Operations

BCQ—Basic Cyber Qualified

BMC—Basic Mission Capable

CC—Commander

CL—Crew Lead

CMR—Combat Mission Ready

COG—Cyber Operations Group

CPT—Cyber Protection Teams

CVA/H—Cyber Vulnerability Assessment/Hunter

CTM—Cyber Technical Manual

DAF—Department of the Air Force

DAFMAN—Department of the Air Force Manual

DAFPD—Department of the Air Force Policy Directive

EPE—Emergency Procedures Evaluation

FMQ—Fully Mission Qualified

FT—Fully Trained

HHQ—Higher Headquarters

HA—Host Analyst

IAW—In Accordance With

INSTR—Instructor Evaluation

IOC—Indicator of Compromise

IQP—Individual Qualification Program

JQR—Job Qualification Record

JQS—Job Qualification Standard

KT-C—Key Terrain-Cyber

LOX—Letter of Certifications

MAJCOM—Major Command

MDS—Mission Design Series

MEL—Mission Element Lead

MQF—Master Qualification File

MSN—Mission Evaluation

MRT-C—Mission Relevant Terrain-Cyber

NA—Network Analyst

N/N—No-Notice Qualification

OGV—Group Stan/Eval

OI—Operating Instruction

OPCON—Operational Control

OPR—Office of Primary Responsibility

ORM—Operational Risk Management

QUAL—Qualification Evaluation

RQ—Requalification

SEB—Stan/Eval Board

SEE—Stan/Eval Examiner

SMQ—Special Mission Qualification

SOP—Standard Operating Procedure

SPOT—Spot Evaluation

SQ—Squadron

SQB—Secure Question Bank

Stan/Eval—Standardization and Evaluation

TTP—Tactics, Techniques and Procedures

US—United States

USAF—United States Air Force

USCYBERCOM—United States Cyber command

Office Symbols

ACC/A3—Air Combat Command Director of Operations

ACC/A3T—Air Combat Command Flight Operations Division

ACC/A3TV—Air Combat Command Standardization Branch

Terms

Basic—Basic proficiency level. An individual is considered qualified to be assigned to a work role. Basic qualification requires completion of all Air Force feeder training and outlined formal training; completion of all applicable basic level tasks outlined in the JQS (i.e., JQR Tab 4); and completion of all mission-specific training required to execute tasks for an assigned duty position.

Certification—Procedure used to document competency in a particular task as determined by a Certifying Official. It is not interchangeable with "qualification," which requires ACC Form 4418 or AF Form 8 documentation.

Certifying Official—The first operational CC in the member's chain of command or a designated representative.

Cybercrew—Also referred to as crew members, they consist of individuals who conduct cyberspace operations and are typically assigned to a specific CVA/H system.

Cyberspace—A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Event—The leveraging of people, process, and technology resulting in the execution of cyber operations.

Go/No-Go—The "Go" stage is when a trainee has gained enough skill, knowledge, and experience to perform the tasks without supervision, meeting the task standard. The "No-Go" stage is when the trainee has not gained enough skill, knowledge, and experience to perform the task without supervision and does not meet the task standard.

Host Analyst (HA)—A CVA/H work role. A CVA/H HA specializes in advanced vulnerabilities and threats in the 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 are the expert to utilize for investigations into an incident or counter-threat actions on their specific host system type. They can create scripts for a targeted host system that can assess the health and gather information that other operators can analyze or use to determine actions.

Instructor—An operator who has completed Instructor Methodology Course and is qualified to instruct other individuals in mission area academics and positional duties. Instructors are appointed by the Certifying Official.

Master—Advanced proficiency level. The individual is fully trained and experienced in all aspects of the assigned unit mission. Individuals are required to complete the JQR to be qualified at the Master level proficiency. Certain work roles note additional minimal requirements to be met before qualifying as a Master. Individual can supervise the training and qualification of unit personnel on the execution of unit tactical and operational missions within their respective work roles. Master-level proficiency includes advising leadership on mission challenges, direction, and risk mitigation strategies; development, oversight, and implementation of training to address technical competence shortfalls; evaluation of mission effectiveness; and providing recommended solutions and implementing strategies to address gaps during mission execution.

May—Acceptable or suggested means of accomplishment.

Mission—The task, together with the purpose, that clearly indicates the actions taken and the reason, therefore. In common usage, a duty assigned to an individual or unit. The base mechanism used to achieve mission objectives is events. Missions may require multiple events from multiple units to accomplish the mission's objectives.

Mission Element Lead (MEL)—The MEL has ultimate authority for a CVA/H mission and is responsible for the overall execution of the mission. When only one crew exists, the CL for that crew may also function as the MEL.

Network Analyst (NA)—A CVA/H work role. A CVA/H NA specializes in advanced vulnerabilities and threats to network architectures, technologies, and associated systems. Their knowledge is to the level where they can reconstruct a network for analyzing the data collected

from captures and flow data. They can identify misconfiguration & malicious activity based on the observable traffic of the network. They would assess a network's configuration, settings, and activity to identify weak security, vulnerabilities, or maliciously configured network infrastructure. They are the expert to utilize for investigations into an incident or counter-threat actions on network infrastructure.

Qualification—A demonstrated knowledge, skill, and ability that, through evaluation, meets a passing threshold for a job, position, or system.

Qualification Evaluation (QUAL)—Qualifies a cybercrew member to perform the duties of a particular work role in the specified MDS. Requires ACC Form 4418 or AF Form 8 documentation.

Senior—Intermediate proficiency level. To achieve Senior qualification, an individual must complete all outlined senior-level formal training and applicable Senior-level tasks outlined in the JQS (JQR Tab 4) and complete all mission-specific training required to execute tasks for an assigned duty position. Individuals must also possess the experience and judgment to operate without direct technical oversight.

Should—A preferred, but not mandatory, method of accomplishment.

Special Mission Qualification (SMQ)—An SMQ is an additional qualification added to a work role MDS that accounts for specific aspects of unique missions or one-off tasks that are not widely performed. SMQ training is accomplished via on-the-job training and/or a course. See ACCMAN 17-2CVAHV1 for more details.

Terrain—The cyberspace AO where a force package is directed to conduct an event. Telecommunications networks, computer systems, embedded processors and controllers, Internet Protocol addresses, associated subnet, domain, or transport space with the tasked AO.

Will—A mandatory requirement.