

**BY ORDER OF THE COMMANDER
AIR COMBAT COMMAND**

**AIR COMBAT COMMAND MANUAL
17-2ACD, VOLUME 2**



30 MARCH 2023

Cyberspace

**AIR FORCE CYBERSPACE DEFENSE (ACD) -
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 releasability restrictions on this publication.

OPR: ACC/A60

Certified by: ACC/A3T
(John F. Costa)

Supersedes: ACCMAN17-2ACDV2, 30 November 2020

Pages: 30

This publication implements ACCI 17-202V2, *Cybercrew Standardization/Evaluation Program*. This publication applies to all Air Combat Command (ACC) military and civilian personnel, members of Air Force Reserve Command, Air National Guard, and contractor support personnel in accordance with appropriate provisions contained in memoranda support agreements and Air Force contracts. This publication requires the collection and/or maintenance of information protected by the Privacy Act of 1974 authorized by Title 10 United States Code, Section (§) 9013, *Secretary of the Air Force*. The applicable System of Records Notices F011 AF AFMC B, Patriot Excalibur (PEX) System Records membership programs is available at: <https://dpcl.d.defense.gov/privacy/SORNS.aspx>. Ensure all records generated as a result of processes prescribed adhere to AFI 33-322, *Records Management and Information Governance Program*, and disposed of IAW the AF Records Disposition Schedule located in the AF Records Information Management System. Refer recommended changes and questions about this publication to the OPR using the DAF Form 847, *Recommendation for Change of Publication*; 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 prior to 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. Waiver authority for non-tiered paragraphs remains with Air Combat Command Director of Operations (ACC/A3). See DAFMAN 90-161, *Publishing Processes and Procedures*, Table A10.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier

waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. 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.

SUMMARY OF CHANGES

This publication has been substantially revised and needs to be completely reviewed. Major changes include, but are not limited to: revising **paragraph 2.4**, which establishes a clear and distinct mission and evaluation standard for the CDO and IR crew positions for shared areas 9 and 12. Significantly updated **Table 1.2** to reflect the CDO crew position and added IR and Instructor upgrade position requirements. Changes also include document wide waiver authority revisions and publication reference updates.

Chapter 1—GENERAL GUIDANCE	4
1.1. General.....	4
1.2. Responsibilities.....	4
1.3. Standardization and Evaluation Examiners (SEEs).....	4
1.4. General Evaluation Requirements.....	5
Table 1.1. Crew Position Specific Requirements - Written Examinations.....	6
1.5. Grading Instructions.....	7
Table 1.2. Crew Position Specific Requirements – Performance Phase Evaluations.....	8
Chapter 2—CREW POSITION EVALUATIONS AND GRADING CRITERIA	10
2.1. General.....	10
2.2. Qualification Evaluations:.....	10
2.3. Mission Certifications.....	10
2.4. General Crew Position Evaluation Criteria.....	10
2.5. Detection Actions Evaluation Criteria.....	15
2.6. Tactical Employment Actions Evaluation Criteria.....	18
Table 2.1. Intrusion Detection Scores.....	18
Table 2.2. Scoping Scores.....	18
Table 2.3. Strike Scores.....	19
Table 2.4. Incident Response Scores.....	19
Table 2.5. Threat Hunt Scores.....	19
2.7. Upgrade Positions.....	20
Chapter 3—INSTRUCTOR EVALUATIONS AND GRADING CRITERIA	21
3.1. General.....	21

3.2.	Instructor Upgrade and Qualification Requisites.....	21
3.3.	Instructor (INSTR) Qualification Evaluations:.....	21
3.4.	INSTR Evaluation Grading Criteria.	21
3.5.	INSTR Evaluation Documentation.	22
3.6.	Recurring/Periodic INSTR Evaluation.	23
Chapter 4—	SEE OBJECTIVITY EVALUATIONS AND GRADING CRITERIA	24
4.1.	General.....	24
4.2.	Evaluator Upgrade and Qualification Requisites.....	24
4.3.	SEE Objectivity Evaluations.....	24
Attachment 1—	GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION	26

Chapter 1

GENERAL GUIDANCE

1.1. General. This manual provides cyberspace operations examiners and crew members with procedures and evaluation criteria used during performance evaluations on operational cyberspace weapon systems. For evaluation purposes, refer to this publication for evaluation standards. Adherence to these procedures and criteria will ensure an accurate assessment of the proficiency and capabilities of crewmembers. In addition to general criteria information and grading criteria, this publication provides specific information and grading criteria for each crew position, instructor upgrade qualification, and Standardization and Evaluation (Stan/Eval) Examiner (SEE) objectivity evaluations.

1.2. Responsibilities.

1.2.1. Refer to ACCI 17-202V2 for all MAJCOM and Number Air Force (NAF) Stan/Eval roles, responsibilities and programs. For the purposes of this manual, "MAJCOM" includes direct reporting units and the National Guard Bureau.

1.2.2. Refer to ACCI 17-202V2 for all unit-level Stan/Eval roles, responsibilities and programs. For purposes of this manual, "unit" includes levels of organization under Higher Headquarters (HHQ) required to establish a Stan/Eval function.

1.3. Standardization and Evaluation Examiners (SEEs). SEEs will use the grading policies contained in ACCI 17-202V2, and the evaluation criteria in this manual for conducting all ACC and ACC-oversight units' weapon system performance, and Cybercrew Training Devices (CTDs). All evaluations assume a stable platform and normal operating conditions.

1.3.1. Each squadron (SQ) will design and maintain evaluation profiles for each mission that includes information on each crew position. **(T-2)** These profiles, approved by the Cyberspace Operations Group (COG) Stan/Eval office (OGV) (COG/OGV), will outline the minimum number and type of events to be performed/observed in order to satisfy a complete evaluation. Evaluation profiles will incorporate requirements established in the applicable grading criteria and reflect the primary unit tasking. **(T-2)**

1.3.2. All evaluations fall under the Qualification (QUAL), Mission (MSN), Spot (SPOT), or Instructor (INSTR) categories listed in ACCI 17-202V2. For dual/multiple qualification or difference evaluations (an evaluation that covers major changes in an existing capability, e.g., a major upgrade to sensor suite that adds or alters capabilities) that do not update an eligibility period, list as "SPOT" on the front of the ACC Form 4418, *Certificate of Cybercrew Qualification*, and explain that it was a difference evaluation under "Mission Description". **(T-2)**

1.3.2.1. Schedule all evaluation activity on one mission/sortie to the greatest extent possible. All performance phase requirements should be accomplished during a training (or operational if training not available) mission/sortie. If a required event is not accomplished during a mission/sortie, COG Commander (COG/CC) is the waiver authority for the event to be completed in the CTD. This may be delegated no lower than the SQ Commander (CC) (SQ/CC) unless otherwise authorized in position-specific chapters of this manual.

1.3.2.2. During all evaluations, any grading areas observed by the evaluator may be evaluated. If additional training is required for areas outside of the scheduled evaluation, document the training required under the appropriate area on the ACC Form 4418.

1.3.2.3. This manual contains a table of requirements for the written requisites, **Table 1.1**, and a table for the grading criteria for various evaluations, **Table 1.2**. Each table may include a "Note" which refers to a general note found in the individual grading criteria, and/or a number which refers to a note shown below the table. To complete an evaluation, all areas annotated with an "R" are required and must be successfully completed. **(T-3)**

1.3.2.4. Unit examiners may administer evaluations, within the same crew position, outside of their organization to include administering evaluations between ACC, Air Force Reserve Command and Air National Guard provided written agreements/understandings between the affected organizations are in-place. Written agreements/understandings shall be reviewed and updated annually. **(T-3)**

1.3.3. Momentary deviations from standards will not be considered in the grading, provided the examinee applies prompt corrective action and such deviations do not jeopardize safety or the mission. Cumulative deviations will be considered when determining the overall grade. The SEE will state the examinee's overall rating, review with the examinee the area grades assigned, thoroughly critique specific deviations, and recommend/assign any required additional training. **(T-2)**

1.3.4. SEEs will not evaluate students with whom they have instructed more than 50% of the qualification/upgrade training performance events without SQ/CC approval. SEEs will not evaluate students they recommended for end of training qualification/upgrade evaluation unless approved by the SQ/CC. **(T-3)**

1.3.5. All crewmembers for the mission/sortie (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. All crewmembers must be current on Crewmember Information Folders (CIF) and meet all Go/No-Go requirements IAW ACCI 17-202 series publications, and all applicable supplemental guidance prior to operating, instructing, or evaluating on the weapon system. **(T-2)**

1.4. General Evaluation Requirements.

1.4.1. Publications Check. Unless using publications from their direct source, a publication check will be accomplished IAW applicable publication guidance (e.g., ACCIs, approved checklists and crew aids). The publications check will be annotated in the Comments block of the ACC Form 4418 during initial issue of items to student crewmembers, after inspections of crewmember's issued items when called to do so by cadre, and during turn-in of issued items at the end of training. Publication and checklist currency will be annotated in accordance with Unit Stan/Eval guidance. Unit Stan/Eval will list the required operating publications each cyber crewmember is responsible for in the local CIF Library and/or local supplement to ACCI 17-202V2. **Note:** In units where such resources are not individually issued but made available/accessible for common use, the SQ Stan/Eval office will list those items (version and date) and ensure the accuracy and currency of the information contained in those resources for common use.

1.4.2. Written Examinations. The requisites in **Table 1.1**, are common to all ACD crew positions and will be accomplished IAW ACCI 17-202V2, all applicable supplemental guidance, and unit directives. These will be accomplished prior to the mission/sortie performance phase unless in conjunction with a No-Notice (N/N) QUAL. **Note:** A N/N evaluation conducted in the examinee's eligibility period and meeting all required QUAL profile requirements allows the examinee to opt for the N/N evaluation to satisfy a periodic QUAL, in which the examinee may complete written requisites after the performance phase. However, the written examination(s) must be completed prior to the examinee's expiration date. **(T-2)**

Table 1.1. Crew Position Specific Requirements - Written Examinations.

Examination Type	CDO	IR	TH	TVA	CCC	CITA
OPEN BOOK	R	R	R	R	R	R
CLOSED BOOK	O	O	O	O	O	O

R – Required and must be successfully completed // O – Optional
Notes:
 SQs will administer OPEN BOOK exams. CLOSED BOOK exams are not required but when utilized they will consist of questions derived from applicable operations manuals and governing directives. SQ Stan/Eval Office will determine the necessary number of questions to be included for each weapon system and crew position. **(T-3)**

1.4.3. QUAL Evaluations. These evaluations measure a crewmember's ability to meet grading areas listed on **Table 1.2**, additional standards from the profile document, and defined in **Chapter 2** of this manual. IAW ACCI 17-202V2 and weapon system-specific guidance, QUAL evaluations may be accomplished with MSN evaluations. When practical, QUAL evaluations should be combined with INSTR evaluations, as applicable for the crew position. **(T-2)**

1.4.4. MSN Evaluations. The various procedures and techniques used throughout the different weapon system variants are managed through a training program which results in a mission certification. Mission certifications will be IAW ACCI 17-202V1, *Cybercrew Training*, ACCMAN 17-2ACDV1, *Air Force Cyberspace Defense (ACD) - Cybercrew Training*, and all applicable supplements and will be documented in the appropriate training folder. MSN evaluation grading areas are also listed on **Table 1.2**, at the end of this chapter and defined in **Chapter 2** of this manual. **(T-2)**

1.4.4.1. For cyber crewmembers who maintain multiple mission certifications (see ACCMAN 17-2V1, Attachment 2), recurring evaluations need only evaluate the primary mission events as long as currency is maintained in all other required training events. **(T-2)**

1.4.5. INSTR Evaluations. Grading areas for these evaluations are listed on **Table 1.2**. See **Chapter 3** of this manual for amplified information and grading area definitions. **(T-2)**

1.4.6. SEE Objectivity Evaluations. Grading areas for these evaluations are listed in ACCI 17-202V2, Attachment 5. See **Chapter 4** of this manual for amplified information and grading area definitions. **(T-2)**

1.4.7. No-Notice (N/N) Evaluations. The intent is to preclude extraordinary preparation for the evaluation. A minimum of 10 percent of QUAL evaluations given on an annual basis (Calendar year from 1 January-31 December) will be N/N. **(T-3)**

1.4.8. DOD 8570.01-M, *Information Assurance Workforce Improvement Program*, Compliance: All operators will be compliant with DoD/Defense Information Systems Agency (DISA) and operator certification requirements as outlined by operator billet coding before taking their evaluation. (As of writing this document all ACD Operator billets are coded for Cyber Network Defense (CND)-Incident Response (IR))

1.5. Grading Instructions. Q, Q- and U ratings are used for specific evaluation areas. Q1, Q2, and Q3 are used for the overall evaluation rating. While the three-level grading system (Q, Q-, U) is used for most areas, a Q- grade will not be used for critical evaluation areas.

1.5.1. Critical Area/Subarea. Critical areas are events that require adequate accomplishment by the examinee in order to successfully and safely achieve the mission/sortie objectives and complete the evaluation. These events, if not adequately accomplished, could result in mission failure, endanger human life, or cause serious injury or death. Additionally, critical areas/subareas apply to time-sensitive tasks or tasks that must be accomplished as expeditiously as possible without any intervening lower priority actions that would, in the normal sequence of events, adversely affect task performance/outcome. If an examinee receives a "U" grade in any critical area, the overall grade for the evaluation will be "Q3." Critical areas are identified by "(C)" following the applicable area title. **(T-2)**

1.5.2. Major Area/Subarea. Major areas are events or tasks deemed integral to the performance of other tasks and required to sustain acceptable weapon system operations and mission execution. If an examinee receives a "U" grade in a non-critical area then the overall grade awarded will be no higher than "Q2." An examinee receiving a "Q-" grade in a non-critical area or areas may still receive a "Q1" overall grade at evaluator discretion. An overall "Q3" can be awarded if, in the judgment of the SEE, there is justification based on performance in one or several areas/sub areas. Major areas are identified by "(M)" following the applicable area title. **(T-2)**

1.5.3. If an examinee receives a "U" grade in a non-critical area then the overall grade awarded will be no higher than "Q2." An examinee receiving a "Q-" grade in a non-critical area or areas may still receive a "Q1" overall grade at evaluator discretion. An overall "Q3" can be awarded if, in the judgment of the SEE, there is justification based on performance in one or several areas/sub areas. **(T-2)**

1.5.4. The SEE must exercise judgment when the wording of areas is subjective and when specific situations are not covered. **(T-2)**

1.5.5. Evaluation judgment will be the final determining factor in deciding the overall qualification level. **(T-2)**

Table 1.2. Crew Position Specific Requirements – Performance Phase Evaluations.

AREA/TITLE	Cat	Crew Position	Upgrade Position		Special Mission Qualification			
		CDO	IR	INSTR	TH	TVA	CCC	CTIA
General								
1. Triage and Incident Response Plan	C		R					
2. Threat Hunt Plan	C				R			R
3. Tactical Emulation Plan	C					R		
4. CTO & Dynamic Targeting	C						R	
5. Acknowledge Mission Assignment	C	R	R					
6. Operational Risk Management (ORM)	C	R	R					
7. Go/No-Go	C	R	R					
8. Weapon System Account Check	C	R	R					
9. Brief	M	R	R					
10. Crew Leadership	M		R					
11. After Action Report	M	R	R					
12. Debrief/Self Critique	M	R	R					
13. Submit Training Activity Report (TAR)	M	R	R		R	R	R	R
14. Mission Report	M		R		R	R	R	R
15. Safety	C	R	R					
16. Crew Discipline	C	R	R					
Detection Actions								
17. Endpoint Alert List	M	R	R					
18. Process Start Time	M	R	R					
19. Process Privileges	M	R	R					
20. Process Path	M	R	R					
21. Process Parent/Child Relationships	M	R	R					
22. Process Dynamic-Link Libraries (DLL)	M	R	R					
23. Process Port	M	R	R					
24. Process Memory Collection	M	R	R					
25. File Collection	M	R	R					
26. File Behavior	M	R	R					
27. File Reputation	M	R	R					
28. Domain Name Reputation	M	R	R					
29. IP Address Reputation	M	R	R					
30. Packet Inspection	M	R	R					
31. Endpoint Port Use	M	R	R					
32. Endpoint Connection Statistics	M	R	R					
33. Endpoint Scheduled Tasks	M	R	R					
34. Endpoint Start Up Folder	M	R	R					
35. Endpoint Run Keys	M	R	R					
36. Endpoint Log Collection	M	R	R					
37. Endpoint Log Inspection	M	R	R					
38. Enterprise Comparison	M	R	R					
39. Detect Intrusions	C	R	R					
40. Scope Indicator of Compromise	C	R	R					
41. Strike Target	C	R	R					
42. Incident Response	C		R					
43. Threat Hunt	C				R			
44. Vulnerability Scanning	C					R		
45. Tactical Validation	C					R		
46. Instructional Ability	M			R				
47. Instructional Briefings/Critiques	M			R				
48. Demonstration and Performance	M			R				

Notes: Crew members who hold an Special Mission Qualification (SMQ) are also responsible for all areas related to their base crew position or upgrade position (CDO or IR).

The category for the evaluation area is as follows:

C—Critical

M—Major

R—Required

Chapter 2

CREW POSITION EVALUATIONS AND GRADING CRITERIA

2.1. General. The grading criteria in this chapter apply to evaluations for all ACD crew positions (as specified) and were established by experience, policies, and procedures set forth in weapon system manuals and other directives. Evaluators must realize the grading criteria contained herein cannot accommodate every situation. Written parameters must be tempered with mission objectives and, more importantly, mission/task accomplishment in the determination of overall crew performance.

2.1.1. The category for the evaluation area is listed in parentheses as follows:

2.1.1.1. [C]—Critical

2.1.1.2. [M]—Major

2.1.1.3. [R]—Required

2.2. Qualification Evaluations:

2.2.1. Written Examination Requisites: See [Table 1.1](#). (T-3)

2.2.2. Performance Phase. (T-3)

2.2.3. Special Mission Qualifications allows crewmembers to accomplish additional mission related duties and will consist of special mission training and evaluation requirements. SMQs are held in conjunction with the CDO or IR crew positions. Individuals who hold a SMQ are expected to perform periodic evaluations covering all evaluation areas for both their base qualification (CDO or IR) as well as their SMQ. Failure to maintain requirements for a base qualification results in immediate revocation of SMQ. Failure to accomplish missions/events required for RCP and SMQ will result in loss of that qualification. (T-3)

2.3. Mission Certifications. Mission Certifications ensure individuals are capable of performing duties essential to the effective employment of the weapon system. Mission Certifications are accomplished IAW local training requirements and/or SQ/CC directions. Mission certification events are normally performed during QUAL evaluations but may be performed on any mission/sortie with an instructor certified in that mission. (T-3)

2.4. General Crew Position Evaluation Criteria. The following evaluation criteria will be used to evaluate an operator's ability perform administrative tasks directly related to mission completion for ACD.

2.4.1. AREA 1, Incident Response Plan (C).

2.4.1.1. Q. Analyzes details of Crew Commander (CCC) assigned mission and prepares a plan that:

2.4.1.1.1. Summarizes suspicious activity and impacted blue space hosts/Internet Providers (IPs) (location)

2.4.1.1.2. Establishes an initial list of blue space hosts/IPs to engage

2.4.1.1.3. Sets minimum detection actions to execute against blue space hosts/IPs

- 2.4.1.1.4. Establishes an initial list of indicators of Compromise (IOCs) for scoping actions.
- 2.4.1.1.5. Sets mission phases/timing and assigns crew tasks/actions/responsibilities
- 2.4.1.1.6. Sets manning based on expected detection, scoping, and strike action task load
- 2.4.1.1.7. Sets detection, scoping, strike, and command, control and communications (C3) measures of effectiveness and performance (MOEs/MOPs)
- 2.4.1.1.8. Sets mission Check In, Brief, Execution, and Debrief times **(T-3)**
- 2.4.1.2. U. Fails to prepare an adequate plan. Misrepresents or omits too many details from assigned mission. Fails to determine initial detection/scoping actions, assign crew tasks/actions/responsibilities, or set phases/timing for execution plan. Does not request CDO manning based on expected detection, scoping, and strike action task load. Fails to establish MOE/MOPs for detection, scoping, strike and C3. Fails to organize Check In, Brief, Execution, and Debrief cycle for mission. **(T-3)**
- 2.4.2. AREA 2, Threat Hunt Plan (C)
 - 2.4.2.1. Q. Operator will develop a plan to proactively search for threats on the Air Force Information Network (AFIN) based on open source intelligence and provided intelligence that may have evaded current defense in depth measures. Plan is adequate for threat hunt mission and well documented. **(T-3)**
 - 2.4.2.2. U. Plan did not clearly outline mission objectives, crew roles, or tactical tasks to get after overall objective. Crew members unsure of the path to completion when reading/reviewing plan. Operator is unable to explain plan in depth. **(T-3)**
- 2.4.3. AREA 3, Tactical Emulation Plan (TEP) (C)
 - 2.4.3.1. Q. Adequately outlined TEP to include: overview, purpose, objectives, scenario validation, reporting procedures, mission requirements, documentation of successful simulation actions outside of AFIN, the tactical plan and source code. **(T-3)**
 - 2.4.3.2. U. Errors or omissions from TEP would cause delays or damage to mission, mission systems or mission environment that would adversely affect the weapons system or the AFIN. **(T-3)**
- 2.4.4. AREA 4, Cyber Tasking Order (CTO) & Dynamic Targeting (C)
 - 2.4.4.1. Q. Assured mission success by accurately identifying, effectively prioritizing, and efficiently managing CTOs and dynamic taskings based on planned and updated information. Identified contingencies, gathered data, and formulated decisions. Clearly communicated task priorities and updates to crew members. Used available resources necessary to manage workload, monitor crew activity, and aid in decision making. **(T-3)**
 - 2.4.4.2. U. Did not assure mission success. Failed to effectively prioritize and managed CTOs and dynamic taskings. Failed to identify contingencies, gather data or formulate decisions. Did not clearly communicate tasks and updates **(T-3)**
- 2.4.5. AREA 5, Acknowledge Mission Assignment (C)

- 2.4.5.1. Q. Submits acknowledgement of assigned mission. **(T-3)**
- 2.4.5.2. U. Fails to acknowledge mission assignment. **(T-3)**
- 2.4.6. AREA 6, Operational Risk Management (ORM) (C)
 - 2.4.6.1. Q. Calculates ORM. Takes appropriate risk informed follow-on actions. **(T-3)**
 - 2.4.6.2. U. Fails to calculate ORM. Does not take appropriate risk informed follow-on actions. **(T-3)**
- 2.4.7. AREA 7, Go/No-Go (C)
 - 2.4.7.1. Q. Reports status. Takes appropriate follow-on actions to achieve “Go”. **(T-3)**
 - 2.4.7.2. U. Fails to report status. Fails to take appropriate follow-on actions to achieve “Go”. **(T-3)**
- 2.4.8. AREA 8, Weapon System Account Check (C)
 - 2.4.8.1. Q. Operator can log into all accounts necessary to performs operations. **(T-3)**
 - 2.4.8.2. U. Operator does not have all accounts necessary to perform operations. **(T-3)**
- 2.4.9. AREA 9, Brief (M)
 - 2.4.9.1. Q. CDO is able to brief details for one of the following as assigned:
 - 2.4.9.1.1. AFIN terrain status: List outages, degradations, Periods of Non-Disruption (POND), and Authorized Service Interruptions (ASI) across AFIN and describe tactical impacts.
 - 2.4.9.1.2. ACD status: List sensor/tool degradations and describe tactical impacts.
 - 2.4.9.1.3. Enemy tactics, techniques, and procedures (TTPs): Technical description of known adversary behaviors and at least one friendly method of detection. **(T-3)**
 - 2.4.9.2. Q-. Performance included errors that did not jeopardize mission accomplishment. **(T-3)**
 - 2.4.9.3. U. Failed to provide assigned information. Jeopardized mission accomplishment. **(T-3)**
 - 2.4.9.4. Q. IR ensures crew understands mission by briefing the following:
 - 2.4.9.4.1. Mission check-in, brief, execution, and debrief schedule
 - 2.4.9.4.2. Suspicious activity, impacted blue space hosts/IPs (locations), enemy profile, and CC’s intent
 - 2.4.9.4.3. Initial list of blue space hosts/IPs to engage
 - 2.4.9.4.4. Minimum detection actions to execute against list of blue space hosts/IPs
 - 2.4.9.4.5. Initial list of IOCs for scoping actions
 - 2.4.9.4.6. Execution plan timing/phasing and assigned crew tasks/actions/responsibilities
 - 2.4.9.4.7. MOEs/MOPs for detection, scoping, strike, and C3 actions

- 2.4.9.4.8. Tactical information briefs: AFIN status, ACD status, and Enemy TTP
- 2.4.9.4.9. Rules of Engagement (ROEs), contingencies, and emergency procedures
- 2.4.9.5. Q-. Performance included errors or omissions that did not jeopardize mission accomplishment.
- 2.4.9.6. U. Failed to provide adequate information. Jeopardized mission accomplishment.
- 2.4.10. AREA 10, Crew Leadership (M)
 - 2.4.10.1. Q. Accomplish the following throughout mission:
 - 2.4.10.1.1. Ensure assigned crew are on time to check-in, brief, execution, and debrief
 - 2.4.10.1.2. Assess assigned crew ORM, Go/No Go, and tool access prior to execution
 - 2.4.10.1.3. Track progress of detection actions against list of impacted blue space hosts/IPs
 - 2.4.10.1.4. Track progress of scoping actions against list of IOCs
 - 2.4.10.1.5. Ensure assigned crew is gainfully and equitably employed
 - 2.4.10.1.6. Adjust detection, scoping, and strike actions as needed to accomplish mission
 - 2.4.10.1.7. Adjust execution window as needed to accomplish mission
 - 2.4.10.1.8. Request additional operators based on action/task load and desired timeliness
 - 2.4.10.1.9. Request mission cancellation/re-scheduling due to unforeseen circumstances
 - 2.4.10.1.10. Enforce professionalism of assigned crew **(T-3)**
 - 2.4.10.2. Q-. Performance included errors or omissions that did not jeopardize mission accomplishment. **(T-3)**
 - 2.4.10.3. U. Failed to provide adequate technical/tactical leadership. Jeopardized mission accomplishment. **(T-3)**
- 2.4.11. AREA 11, After Action Report (AAR) (M)
 - 2.4.11.1. Q. Recorded all detection actions per blue space host/IP, scoping actions per IOC, and strike actions per target. **(T-3)**
 - 2.4.11.2. Q-. Notes included errors or omission that did not jeopardize accurate report of mission accomplishment. **(T-3)**
 - 2.4.11.3. U. Failed to provide adequate information. Jeopardize accurate mission reporting. **(T-3)**
- 2.4.12. AREA 12, Debrief/Self Critique (M)
 - 2.4.12.1. Q. CDO identifies opportunities for growth in tactical employment skills and suggests viable methods of improvement. **(T-3)**

2.4.12.2. Q- . CDO identifies opportunities for growth in tactical employment skills. **(T-3)**

2.4.12.3. U. CDO fails to identify growth opportunities in tactical employment skills. **(T-3)**

2.4.12.4. Q. IR leads assigned CDOs to review MOEs/MOPs and accurately self-assess execution. Able to assist in identification of growth areas and development of paths to improve tactical employment skills.

2.4.12.5. Q-. IR leads assigned CDOs to review MOEs/MOPs and accurately self-assess execution. Able to assist in identification of growth areas for tactical employment skills.

2.4.12.6. U. IR fails to lead assigned CDOs to review MOEs/MOPs. Not able to identify growth areas for tactical employment skills.

2.4.13. AREA 13, Submit TAR (M)

2.4.13.1. Q. Submits TAR with no errors or discrepancies **(T-3)**

2.4.13.2. Q-. Submits TAR with few errors or discrepancies **(T-3)**

2.4.13.3. U. TAR does not accurately reflect mission performance **(T-3)**

2.4.14. AREA 14, Mission Report (MISREP) (M)

2.4.14.1. Q. Submits mission report to CCC covering the following:

2.4.14.1.1. List of blue space hosts/IPs associated with intrusion

2.4.14.1.2. List of enemy initial access and follow-on actions per blue space host/IP

2.4.14.1.3. List of IOC associated with intrusion

2.4.14.1.4. List of strike actions executed to contain intrusion. **(T-3)**

2.4.14.2. Q-. Submits mission report to CCC with few errors, omissions, or discrepancies. **(T-3)**

2.4.14.3. U. Fails to submit mission report to CCC. Mission report is inaccurate, incomplete, or misleading. **(T-3)**

2.4.15. AREA 15, Safety (C)

2.4.15.1. Q. Aware of and complied with all factors required for safe operations and mission accomplishment. **(T-3)**

2.4.15.2. U. Was not aware of safety factors or disregarded procedures to safely operate and conduct the mission. Conducted unsafe actions that jeopardized mission accomplishment and/or put crewmembers at risk of injury or death. Operated in a manner that could or did result in damage to the weapon system/equipment. **(T-3)**

2.4.16. AREA 16, Crew Discipline (C)

2.4.16.1. Q. Demonstrated strict professional crew discipline throughout all phases of the mission. Planned, briefed, executed, and debriefed mission IAW applicable instructions and directives. **(T-3)**

2.4.16.2. U. Failed to demonstrate strict professional crew discipline throughout all phases of the mission. Violated or failed to comply with applicable instructions and directives which could have jeopardized safety of crewmembers or mission accomplishment. **(T-3)**

2.5. Detection Actions Evaluation Criteria. The following evaluation criteria will be used to test an operator's ability to perform detection actions.

2.5.1. AREA 17, Endpoint Alert List (M)

2.5.1.1. Q. Enumerated a list of alerts for a given endpoint. **(T-3)**

2.5.1.2. Q-. Enumerated a list of alerts for a given endpoint with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.1.3. U. Performance shortcomings jeopardized task accomplishment **(T-3)**

2.5.2. AREA 18, Process Start Time (M)

2.5.2.1. Q. Determined start time for a given process. **(T-3)**

2.5.2.2. Q-. Determined start time for a given process with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.2.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.3. AREA 19, Process Privileges (M)

2.5.3.1. Q. Determined privilege level for a given process. **(T-3)**

2.5.3.2. Q-. Determined privilege level for a given process with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.3.3. U. Performance shortcomings jeopardized task accomplishment **(T-3)**

2.5.4. AREA 20, Process Path (M)

2.5.4.1. Q. Determined path for a given process. **(T-3)**

2.5.4.2. Q-. Determined path for a given process with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.4.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.5. AREA 21, Process Parent/Child Relationships (M)

2.5.5.1. Q. Determined parent/child relationship for a given process. **(T-3)**

2.5.5.2. Q-. Determined parent/child relationship for a given process with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.5.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.6. AREA 22, Process Dynamic-Link Libraries (DLL) (M)

2.5.6.1. Q. Determined DLL usage for a given process. **(T-3)**

2.5.6.2. Q-. Determined DLL usage for a given process with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.6.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.7. AREA 23, Process Port (M)

2.5.7.1. Q. Determined port usage for a given process. **(T-3)**

2.5.7.2. Q-. Determined port usage for a given process with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.7.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.8. AREA 24, Process Memory Collection (M)

2.5.8.1. Q. Collected memory for a given process. **(T-3)**

2.5.8.2. Q-. Collected memory for a given process with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.8.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.9. AREA 25, File Collection (M)

2.5.9.1. Q. Collected file for a given endpoint. **(T-3)**

2.5.9.2. Q-. Collected file for a given endpoint with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.9.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.10. AREA 26, File Behavior (M)

2.5.10.1. Q. Determined behavior for a given file. **(T-3)**

2.5.10.2. Q-. Determined behavior for a given file with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.10.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.11. AREA 27, File Reputation (M)

2.5.11.1. Q. Determined reputation for a given file. **(T-3)**

2.5.11.2. Q-. Determined reputation for a given file with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.11.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.12. AREA 28, Domain Name Reputation (M)

2.5.12.1. Q. Determined reputation for a given domain. **(T-3)**

2.5.12.2. Q-. Determined reputation for a given domain with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.12.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.13. AREA 29, IP Address Reputation (M)

2.5.13.1. Q. Determined reputation for a given IP address. **(T-3)**

2.5.13.2. Q-. Determined reputation for a given IP address with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.13.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.14. AREA 30, Packet Inspection (M) 2.5.14.1. Q. Determined details for a given packet capture file. **(T-3)**

2.5.14.1. Q-. Determined details for a given packet capture file with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.14.2. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.15. AREA 31, Endpoint Port Use (M)

2.5.15.1. Q. Determined port usage for a given endpoint. **(T-3)**

2.5.15.2. Q-. Determined port usage for a given endpoint with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.15.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.16. AREA 32, Endpoint Connection Statistics (M)

2.5.16.1. Q. Determined connection statistics such as times, frequencies, and volumes for a given endpoint. **(T-3)**

2.5.16.2. Q-. Determined connection statistics such as time, frequencies, and volumes for a given endpoint with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.16.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.17. AREA 33, Endpoint Scheduled Tasks (M)

2.5.17.1. Q. Determined scheduled tasks for a given endpoint. **(T-3)**

2.5.17.2. Q-. Determined scheduled tasks for a given endpoint with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.17.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.18. AREA 34, Endpoint Start Up Folder (M)

2.5.18.1. Q. Determined start up folder programs for a given endpoint. **(T-3)**

2.5.18.2. Q-. Determined start up folder programs for a given endpoint with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.18.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.19. AREA 35, Endpoint Run Keys (M)

2.5.19.1. Q. Determined run keys for a given endpoint. **(T-3)**

2.5.19.2. Q-. Determined run keys for a given endpoint with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.19.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.20. AREA 36, Endpoint Log Collection (M)

2.5.20.1. Q. Collected log files for a given endpoint. **(T-3)**

2.5.20.2. Q-. Collected log files for a given endpoint with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.20.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.21. AREA 37, Endpoint Log Inspection (M)

2.5.21.1. Q. Determined details for a given log file. **(T-3)**

2.5.21.2. Q-. Determined details for a given log file with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.21.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.5.22. AREA 38, Enterprise Comparison (M)

2.5.22.1. Q. Determined enterprise frequency of given endpoint behavior. **(T-3)**

2.5.22.2. Q-. Determined enterprise frequency of given endpoint behavior with errors, omissions, or delays that did not jeopardize task accomplishment. **(T-3)**

2.5.22.3. U. Performance shortcomings jeopardized task accomplishment. **(T-3)**

2.6. Tactical Employment Actions Evaluation Criteria. The following tactical evaluation criteria will be used to test an operator's ability for tactical employment of tasks and skills. **(T-3)**

2.6.1. AREA 39, Detect Intrusions (C) (see **Table 2.1**)

Table 2.1. Intrusion Detection Scores.

SCORE	CRITERIA	PARAMETERS
Q	TIME	≤ 150 min
	ACCURACY	≤ 2 Errors; Operator analysis is Reliable .
U		Did not meet Q- effectiveness rating ; Operator analysis is Not Reliable .
Operator must conduct analysis to determine compromise state of 5 endpoints. Errors occur when operator mischaracterizes endpoints. For example, labelling an uncompromised endpoint as compromised (False Positive) or labelling a compromised endpoint as uncompromised (False Negative).		

2.6.2. AREA 40, Scope Indicator of Compromise (IoC) (C) (see **table 2.2**)

Table 2.2. Scoping Scores.

SCORE	CRITERIA	PARAMETERS
Q	TIME	≤ 8 min
	ACCURACY	≥ 70% of associated endpoints discovered
U		Did not meet Q- effectiveness rating
Operator will execute scoping actions to locate endpoints associated with one of the following IOCs: Domain Name, Port, IP address, User Account, Process, File, or Registry Key.		
Evaluator will use discretion with timing for Q, Q-, U criteria. (i.e., Don't grant a U for exceeding time limits when tools took abnormally long to load/perform as expected).		
Time thresholds are based on initial trials of operator performance.		

2.6.3. AREA 41, Strike Target (C) (see **Table 2.3**)**Table 2.3. Strike Scores.**

SCORE	CRITERIA	PARAMETERS
Q	TIME	≤ 8 min
	EFFECTIVENESS	Successful Hit
U		Strikes wrong target
Operator will execute strike actions to achieve directed denial effect against one of the following targets: Domain Name, IPv4 address, Process, File, or Endpoint.		
Evaluator will use discretion with timing for Q, Q-, U criteria. (i.e., Don't grant a U for exceeding time limits when tools took abnormally long to load/perform as expected.)		
Time thresholds are based on initial trials of operator performance.		

2.6.4. AREA 42, Incident Response (C) (see **Table 2.4**)**Table 2.4. Incident Response Scores.**

SCORE	CRITERIA	PARAMETERS
Q	PHASE 1 TIME	≤ 240 min
	EFFECTIVENESS	≥ 70% of compromised endpoints discovered and contained
	PHASE 2 TIME	≤ 240 min
	ACCURACY	≥ 70% of enemy actions on compromised endpoints determined
U		Did not meet Q- effectiveness rating
Phase 1: Operator must execute and lead crew through detection, scoping, and strike actions to find and kill adversary control of 10 to 15 endpoints associated with an intrusion.		
Phase 2: Operator must execute and lead crew through root cause analysis of endpoints associated with an intrusion to determine initial access and enemy actions on objective.		

2.6.5. AREA 43, Threat Hunt (C) (see **table 2.5**)**Table 2.5. Threat Hunt Scores.**

SCORE	CRITERIA	PARAMETERS
Q	TIME	≤ 240 min
	EFFECTIVENESS	≥ 70% detection TTPs deployed against designated blue space hosts/IPs ≥ 70% of compromised endpoints discovered and contained
U		Did not meet Q- effectiveness rating
Operator must lead crew through deployment of detection TTPs associated with hunt package.		
Operator must execute and lead crew through detection, scoping, and strike actions to find and kill adversary control of 10 to 15 endpoints associated with an intrusion.		

2.6.6. AREA 44, Vulnerability Scanning (C)

2.6.6.1. Q. Properly planned and executed De-Militarized Zone automated and/or manual discovery and/or vulnerability scans, IAW tasking, directives, and applicable checklists. Demonstrated thorough knowledge in procedures and techniques for reviewing scan results and analyzing data. Correctly reported results requiring further analysis and investigation. Properly planned, executed and reported validation of ACD weapon system capabilities. **(T-3)**

2.6.6.2. U. Errors, omissions, or delays jeopardized overall mission accomplishment. **(T-3)**

2.6.7. AREA 45, Tactical Emulation (C)

2.6.7.1. Q. Demonstrated ability to log actions in a timely fashion, adhere to the tactical plan developed, request appropriate deviations, terminate mission as appropriate, and generate an after-action report. Employed appropriate TTPs and made adjustments as necessary throughout all phases of the mission. Followed all applicable system component operating directives, guides, manuals, checklists etc. **(T-3)**

2.6.7.2. U. Failed to identify, prioritize, or manage tasks leading to possible unsafe conditions or significant risk to mission accomplishment. Inability to identify contingencies, ineffective decision making, or errors/omissions placed mission accomplishment and/or safety of others at risk. **(T-3)**

2.7. Upgrade Positions. Instructor (INSTR), Evaluator (SEE), and Incident Responder (IR) are upgrade positions within the ACD weapon system. For instructor criteria and guidance see **Chapter 3** of this document. All evaluator grading criteria and instructions are located in ACCI 17-202V2. IR criteria are located within **Table 1.2** and detailed above. All crew positions may upgrade to INSTR or SEE, however, only the CDO crew position upgrades to IR. **(T-3)**

Chapter 3

INSTRUCTOR EVALUATIONS AND GRADING CRITERIA

3.1. General. Grading criteria (see [Table 1.2](#)) contained herein cannot accommodate every situation. Written parameters must be tempered with sortie objectives, evaluator judgment, and task accomplishment in the determination of overall crew performance. **(T-2)**

3.2. Instructor Upgrade and Qualification Requisites. Prior to an initial (INIT) Instructor Evaluation, Instructor examinees must complete all requisites for Instructor upgrade consideration, nomination and training IAW ACCI 17-202V1, ACCMAN 17-2ACDV1, and all applicable supplemental guidance. **(T-2)**

3.3. Instructor (INSTR) Qualification Evaluations: INSTR evaluations can only be combined with QUAL evaluations when the examinee is in their periodic QUAL eligibility period. There is no eligibility period associated with an INSTR QUAL, however, INSTR QUALs will expire after the 17th month from the previous INSTR QUAL Evaluation. See [paragraph 3.5](#), for documentation guidance. **(T-2)**

3.3.1. INIT INSTR evaluations should be conducted with a student occupying the applicable cybercrew position whenever possible. Recurring or periodic INSTR Evaluations may be conducted with the SEE role playing as the student. **(T-2)**

3.3.2. The instructor examinee will monitor all phases of the mission from an advantageous position and be prepared to demonstrate or explain any area or procedure within their qualified position. The SEE will particularly 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. **(T-2)**

3.3.3. The student will perform those duties prescribed by the instructor for the mission/sortie being accomplished. If an actual student is not available, the SEE will identify to the examinee (prior to the mission) the level of performance expected from the SEE acting as the student. If this option is utilized, at least one event or briefing must be instructed. **(T-2)**

3.3.4. Periodic INSTR evaluations will be administered in conjunction with required periodic qualification evaluations. The examinee must occupy the primary duty position for an adequate period of time to demonstrate proficiency in the crew position with required qualification evaluations. All instructor evaluations will include a pre-mission and post-mission briefing. **(T-2)**

3.3.5. Awarding a "U" in any of the 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. **(T-2)**

3.4. INSTR Evaluation Grading Criteria. All Instructor Evaluation Criteria must be observed and graded to ensure a complete evaluation. Specific requirements for each evaluation are as follows:

3.4.1. AREA 46, Instructional Ability (M)

3.4.1.1. Q. Demonstrated ability to effectively communicate weapon system capability, mission planning, briefing/debriefing, employment/TTP, and mission/events to the student. Provided appropriate corrective guidance when necessary. Planned ahead and made timely decisions. Correctly analyzed student errors. **(T-2)**

3.4.1.2. Q-. Demonstrated a limited ability to effectively communicate weapon system capability, mission planning, briefing/debriefing, employment/TTP, and tasked mission areas to the student. Provided corrective guidance with some errors. Demonstrated limited ability to plan ahead and made some timely decisions. Correctly analyzed some, but not all student errors. **(T-2)**

3.4.1.3. U. Unable to effectively communicate with the student. Did not provide corrective action where necessary. Did not plan ahead or anticipate student problems. Incorrectly analyzed student errors. Adversely impacted student progress. **(T-2)**

3.4.2. AREA 47, Instructional Briefings/Critique (M)

3.4.2.1. Q. Briefings were well organized, accurate, and thorough. Reviewed the student's present level of training and defined mission events to be performed. Demonstrated ability during critique to reconstruct the mission/sortie, offer mission analysis, and provide corrective guidance where appropriate. Completed all training documents according to prescribed directives. Appropriate grades awarded. **(T-2)**

3.4.2.2. Q-. As above but with minor errors or omissions in briefings, critique, or training documents that did not adversely impact student progress. **(T-2)**

3.4.2.3. U. Pre-mission or post-mission briefings were marginal or nonexistent. Did not review the student's training folder or past performance. Failed to adequately critique the student or conducted an incomplete mission analysis which compromised learning. Student strengths or weaknesses were not identified. Adversely impacted student progress. Inappropriate grades awarded. Overlooked or omitted major discrepancies **(T-2)**

3.4.3. AREA 48, Demonstration and Performance (M)

3.4.3.1. Q. Effectively demonstrated procedures and techniques. Demonstrated thorough knowledge of weapon system/components, procedures, and all applicable publications and regulations. **(T-2)**

3.4.3.2. Q-. Minor discrepancies in the above criteria that did not adversely impact student progress. **(T-2)**

3.4.3.3. 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. **(T-2)**

3.5. INSTR Evaluation Documentation.

3.5.1. Instructor Qualification Evaluations will be documented as an INSTR on the ACC Form 4418 and ACC Form 4420, *Individual's Record of Duties and Qualifications*, and maintained in the member's crew evaluation folder (CEF) IAW ACCI 17-202V2, applicable higher headquarters supplements, and local supplemental guidance. **(T-2)** Additional INSTR Evaluation documentation is as follows:

3.5.2. Initial Instructor Qualification Evaluation.

3.5.2.1. If conducted in conjunction with the Instructor Examinee's periodic QUAL evaluation, the INSTR Evaluation will be documented on the same ACC Form 4418, placing INIT INSTR on the same line as QUAL/MSN in the first "Evaluation Type" block of Section II Qualification. Place a statement in Section V Comments that the QUAL evaluation was in conjunction with an INIT INSTR Evaluation. Place any comments specific to the Instructor portion of the evaluation separately from the QUAL portion of the evaluation. **(T-2)**

3.5.2.2. If the INSTR Evaluation is not in conjunction with a periodic QUAL evaluation, document the evaluation as a INIT INSTR in the first "Evaluation Type" block of Section II Qualification and place a statement in Section V Comments that the evaluation was an INIT QUAL INSTR Evaluation. Place any comments regarding commendable performance and/or discrepancies for the instructor evaluation in Section V Comments. **(T-2)**

3.5.2.3. Upon completion of the ACC Form 4418, place the appropriate corresponding entry onto the ACC Form 4420.

3.6. Recurring/Periodic INSTR Evaluation.

3.6.1. If conducted in conjunction with the Instructor Examinee's periodic QUAL evaluation, the Instructor Examinee's Crew Position in Section I will include the instructor designation (e.g., IXX). Place a statement in Section V Comments that the evaluation was a periodic QUAL evaluation in conjunction with periodic or recurring INSTR Evaluation. Place any comments specific to the Instructor portion of the evaluation separately from the QUAL portion of the evaluation. **(T-2)**

3.6.2. When the INSTR Evaluation is not in conjunction with a periodic QUAL evaluation, document the evaluation as a RQ INSTR in the first "Evaluation Type" block of Section II RQ INSTR and place a statement in Section V Comments that the evaluation was recurring or periodic INSTR Evaluation. Place any comments regarding commendable performance and/or discrepancies for the instructor evaluation in Section V Comments. **(T-2)**

3.6.3. Upon completion of the ACC Form 4418, place the appropriate corresponding entry onto the ACC Form 4420. **(T-2)**

3.6.4. Letter of Certification (LOX).

3.6.4.1. The LOX is the list of all the certifications and qualifications for MR and BMC personnel within the unit. The LOX is maintained by the unit and is signed by the unit CC. **(T-2)**

3.6.4.2. Upon the successful completion of an INSTR Evaluation, units will ensure the crewmembers instructor status is reflected on the LOX. **(T-2)**

3.6.4.3. Upon the expiration of a qualification or failure of an INSTR Evaluation, units will ensure the crewmembers instructor status is reflected on the LOX. **(T-2)**

Chapter 4

SEE OBJECTIVITY EVALUATIONS AND GRADING CRITERIA

4.1. General. SEE Objectivity Evaluations are a vehicle for CCs to upgrade crewmembers for SEE certification and a tool to monitor the evaluator crew force's adherence to Stan/Eval directives. Grading criteria contained herein cannot accommodate every situation. Written parameters must be tempered with sortie objectives, evaluator judgment, and task accomplishment in the determination of overall examinee performance. The criteria contained in this chapter are to augment ACCI 17-202V2, Attachment 5, and are established by experience, policies, and procedures set forth in weapon system manuals and other directives and is applicable to all SEE Objectivity Evaluations for ACD crewmembers. **(T-2)**

4.2. Evaluator Upgrade and Qualification Requisites. Evaluator upgrade candidates will be selected from the most qualified and competent instructors. **(T-2)**

4.2.1. Candidates must complete all SEE training IAW ACCI 17-202V2, this manual, and all applicable supplemental guidance. **(T-2)** As a minimum, SEE training will consist of:

4.2.1.1. Group and local SEE academics/instruction covering all Stan/Eval programs and procedures. **(T-2)**

4.2.1.2. The candidate observes one entire evaluation performed by a qualified SEE. **Note:** To the maximum extent possible, SEE Upgrade candidates should observe evaluations conducted within the weapon system for which they are qualified. Training completion should be documented in the members CEF. **(T-2)**

4.3. SEE Objectivity Evaluations. There is no eligibility period or expiration date associated with a SEE Objectivity Evaluation. Once obtained, crewmembers maintain SEE certification unless they fail a QUAL evaluation, fail an INSTR evaluation, fail a SEE Objectivity Evaluation, their weapon system QUAL expires, or upon their SEE appointment being revoked/rescinded by the appointing official. **(T-2)**

4.3.1. SEE Objectivity Evaluations will not be combined with any other type of evaluation. **(T-2)**

4.3.2. SEE Objectivity Evaluations will ensure the SEE examinee (for example in the case of a SEE Objectivity conducted as part of a higher headquarters inspection) observes and grades the entire mission activity of the QUAL examinee. Mission activity is defined as all mission planning, briefing, execution, and debrief activities for the mission/sortie. **(T-2)**

4.3.3. The SEE Upgrade candidate or SEE Examinee will brief the qualified SEE Examiner on all observations, grades, commendable/discrepancies (if any), recommended additional training, and other mission related debrief topics prior to debriefing the QUAL examinee. **(T-2)**

4.3.4. The SEE Examinee will draft the ACC Form 4418 for the INIT or Periodic Examinee's evaluation. The SEE Examiner will review and sign the ACC Form 4418 for both the SEE Examinee and INIT or Periodic Examinee's. **(T-2)**

4.3.5. For SEE Upgrade candidates, SEE Objectivity evaluations will only be administered for observed INIT QUAL or periodic QUAL evaluations. SEE Objectivity evaluations will not be accomplished on SPOT, INIT INSTR, or periodic INSTR not accomplished in tandem with periodic Qual. **(T-2)**

DAVID B. LYONS, Maj Gen, USAF
Director of Operations

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

10 USC § 9013, *Secretary of the Air Force*, 10 August 1956
ACCI 17-202V1, *Cybercrew Training*, 12 January 2021
ACCI 17-202V2, *Cybercrew Standardization/Evaluation Program*, 12 January 2021
ACCMAN 17-2ACDV1, *Air Force Cyberspace Defense (ACD) - Cybercrew Training*, 30 March 2023
AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020
DAFMAN 90-161, *Publishing Processes and Procedures*, 15 April 2022
DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005
DoD Dictionary of Military and Associated Terms, 1 November 2022

Prescribed Forms

None

Adopted Forms

ACC Form 4418, *Certificate of Cybercrew Qualification*
ACC Form 4420, *Individual's Record of Duties and Qualifications*
DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AAR—After Action Report
ACC—Air Combat Command
ACD—Air Force Cyberspace Defense
AFIN—Air Force Network
ASI—Authorized Service Interruptions
BMC—Basic Mission Capable
C—Critical Area of Evaluation
C3—Command, Control, and Communications
CC—Commander
CCC—Crew Commander
CF—Composite Force
CEF—Crew evaluation Folder

CIF—Crew Information File
CND—Cyber Network Defense
COG—Cyberspace Operations Group
COG/CC—Cyber Operations Group Commander
CTD—Cybercrew Training Device
CTE—Cyber Threat Emulation
CTO—Cyber Tasking Order
DCC—Defensive Counter Cyber
DISA—Defense Information Systems Agency
DLL—Dynamic-Link Libraries
EPE—Emergency Procedure Evaluation
FMA—Forensic Malware Analysis
HSO—Host Sensor Operator
INIT—Initial
INSTR—Instructor
IOC—Indicator of Compromise
IP—Internet Provider
IR—Incident Responder
IRO—Incident Response Operator
LEP—list of Effective Pages
LOX—Letter of Certification
M—Major Area of Evaluation
MISREP—Mission Report
MOE—Measure of Effectiveness
MOP—Measure of Performance
MR—Mission Ready
MS—Mutual Support
MSN—Mission
NAF—Numbered Air Force
N/N—No-notice
OGV—Group Standardization and Evaluation
ORM—Operational Risk Management

PAA—Pre-Approved Actions

POND—Periods of Non-Disruption

Q&A—Question and Answer

QUAL—Qualification

R—Required Area of Evaluation

RCP/RTM—Ready Cybercrew Program (RCP) Tasking Memorandum (RTM)

ROE—Rules of Engagement

SEE—Standardization and Evaluation Examiner

SMQ—Special Mission Qualification

SPOT—Spot (Evaluation)

SQ—Squadron

SQ/CC—Squadron Commander

SROE—Standard Rules of Engagement

Stan/Eval—Standardization and Evaluation

TAR—Training Activity Report

TEP—Tactical Emulation Plan

TTP—Tactics, Techniques, and Procedures

Office Symbols

ACC/A3—Air Combat Command Director of Operations

ACC/A3T—Air Combat Command Flight Operation Division

Terms

Basic Mission Capable (BMC)—The status of a crewmember who satisfactorily completed IQT, MQT and a full Stan/Eval evaluation, and maintains certification, currency and proficiency in the command or unit operational mission, is BMC. The cybercrew member must be able to attain Mission Ready (MR) status to meet operational taskings as specified in the applicable weapon system volumes. Persons filling a BMC position must be able to meet MR currency requirements within 30 days (90 days for Air Reserve Component).

Certification—Designation of an individual by the certifying official as having completed required training and/or evaluation and being capable of performing a specific duty.

Commendable—An observed demonstration of exceptional skill and knowledge by a cybercrew member and/or noteworthy ability to perform by the examinee in a specific graded area/subarea, tactic, technique, procedure, and/or task.

Crew Commander (CCC)—Responsible for ACD crew operations and provides command oversight for operations floor personnel. Enforces compliance with policies and procedures to ensure successful mission accomplishment.

Crew Information File (CIF)—A collection of publications and material identified by the MAJCOM and unit as necessary for day-to-day operations.

Currency—A measure of how frequently and/or recently a task is completed. Currency requirements should ensure the average crew member maintains a minimum level of proficiency in a specific event. Currency is a RTM requirement and usually measured in days.

Cybercrew Training Device (CTD)—A training platform suitable to conduct evaluations.

Cyberspace Operations (CO)—The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

Deviation—Performing action(s) not in compliance with current procedures, directives, or regulations. Performing action(s) not in compliance due to unusual or extenuating circumstances is not considered a deviation. In some cases, momentary deviations may be acceptable; however, cumulative deviations will be considered in determining the overall qualification level.

Emergency Procedures Evaluation (EPE)—A performance, CTD, sim or verbal evaluation used to evaluate emergency procedures and systems knowledge.

Evaluation—1) Procedure to determine the effectiveness of the performance of an instructional product or process in order to ascertain specific causes for the effectiveness or lack of it, and to make decisions appropriate to the extent of the effectiveness. 2) The review and analysis of qualitative or quantitative data obtained from design review, hardware inspection, testing or operational use of equipment. See also *DoD Dictionary of Military and Associated Terms*.

Event—An item that occurs or is encountered that initiates a process requiring a set of tasks to be accomplished. Multiple events may be completed and logged during a sortie (be it operational sortie or a training sortie) unless specifically excluded elsewhere in this manual.

Host Sensor Operator (HSO)—Operates the ACD host-based cyberspace alert capability through enduring alert on NIPRNet and SIPRNet to nominate targets for further action.

Incident Response Operator (IRO)—Executes surveillance missions after the detection of an emerging target to characterize target(s); confirm or invalidate target(s) and provide amplifying targeting information for follow-on forces.

Initial Evaluation—The first evaluation of any type for a MDS (e.g., INIT QUAL, INIT MSN, INIT INSTR).

Instructor Evaluation—An evaluation that initially grants instructor qualification or reestablishes instructor qualification of the examinee in a MDS (e.g., INIT INSTR and RQ INSTR).

Mission—Missions are operations conducted with an intended purpose. Missions are conducted by a unit and/or units with relevant capability and preponderance of capacity. The base mechanism used to achieve mission objectives are sorties. Missions may require multiple sorties from multiple units to accomplish the mission objectives.

Mission (MSN) Evaluation—Qualifies a cybercrew member to employ the member's assigned weapon system in accomplishing the unit's operational or DOC statement mission. Requires ACC Form 4418 documentation.

Mission Ready (MR)—The status of a crewmember who satisfactorily completed IQT, MQT, and maintains certification, currency and proficiency in the command or unit operational mission.

No-Notice (N/N) Evaluation—An evaluation where the examinee is notified of the evaluation at or after the beginning of normal preparation for the mission.

Qualification (QUAL)—Designation of an individual by the SQ/CC as having completed required training and evaluation and being capable of performing a specific duty.

Stan/Eval Examiner (SEE)—A cybercrew member designated to perform evaluation duties as specified by this instruction. SEE must be qualified in the events they evaluate (**Exception:** SPOT evaluations). Unit SEEs include squadron SEE assigned to the operational cyber squadron, OGV SEE assigned to the OGV but attached to the operational cyber squadron and other Wing individuals tasked with examiner duties assigned above the squadron level. A HHQ SEE is an examiner assigned to a NAF or MAJCOM. Senior SEEs are senior CCCs – specifically, NAF/CCs and COG/CCs (and/or, their deputies) – that act in the capacity of SEEs.

Supervised Training Status—The status of a cybercrew member who must perform mission under the supervision of either an instructor or a designated supervisor (as specified in ACCMAN17-2ACDV1) qualified in that specific cybercrew position. The examiner determines when supervision is required. The type of supervisor, i.e., instructor or designated supervisor, is as specified in ACCMAN17-2ACDV1, or as determined by the SQ/CC.

Target—The adversary, purposeful malicious actor code, or processes residing in blue or gray terrain. Targets include, but are not limited to, processes, code, credentials, storage, and the countering of adversary tactics, techniques and procedures designed to establish persistent access and C2.

Terrain—The cyberspace area of operations where a force package is directed to conduct a sortie. Terrain is defined as Internet Protocol (IP) address, domain, or transport space within the DoDIN or AF enclave (commonly referred to as "blue" space), or commercial, contractor-owned mission partner-owned ("grey" space) host, server, and network devices that enable C2, communication, sensing, and access capabilities.

Weapon System—A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.