BY ORDER OF THE COMMANDER
AIR COMBAT COMMAND

AIR COMBAT COMMAND MANUAL
17-2CVAH, VOLUME 3

28 OCTOBER 2024

Cyberspace Operations

CYBER VULNERABILITY ASSESSMENT/HUNTER (CVA/H) - OPERATIONS AND PROCEDURES

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/A3/2/6K
Certified by: ACC/A3/2/6K
Supersedes: ACCMAN17-2CVAHV3, 19 January 2021
Pages: 29

This manual implements Department of the Air Force Policy Document (DAFPD) 17-2, *Cyber Warfare Operations,* and establishes the minimum AF standards for operating and performing cybercrew duties 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 memoranda, support agreements and AF contracts. This publication does not apply to AF units executing joint cyber missions under operational control (OPCON) to the Cyber National Mission Force (CNMF), as CNMF directs the use of a jointly procured weapons system that is PURPLE SAFARI (CNMF J6/8/9). Units executing missions under OPCON to the CNMF must comply with training, standardization and evaluation (Stan/Eval), and weapons and tactics requirements outlined in CNMF guidance; however, unit commanders (CCs) are encouraged to leverage guidance in this publication to the extent that it is consistent with joint guidance issued by proper authority. This publication requires the collection and or maintenance of information protected by the Privacy Act of 1974, as amended, authorized by Air Force Instruction (DAFI) 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://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/Air-Force-Article-List/**. Vigilance must be taken to protect Personally Identifiable Information when submitting or sending nominations, applications, or other documents to Department of Defense (DoD) agencies through government Internet, software applications, systems, e-mail, postal, faxing or scanning. Refer to the following directives for additional guidance: AFI 33-332, *Air Force Privacy and Civil Liberties Program*, DoD 5400.11-R,

Department of Defense Privacy Program. Forms containing Personally Identifiable Information require Privacy Act Statements. 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. Submit suggested improvements to this instruction on Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*, through command channels, to Air Combat Command (ACC) Information Warfare Division (ACC/A3/2/6K). ACC will conduct publication reviews and/or revisions as necessary with other agencies as the Cyberspace mission expands. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination 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 ACC Director of Operations (ACC/A3). Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority. 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 DAF.

SUMMARY OF CHANGES

This publication revises the previous version of ACC Manual (ACCMAN) 17-2CVAHV3 by updating CVA/H cybercrew member positions and by integrating guidance from United States Cyber Command (USCYBERCOM) requirements. The Cyber Crew Lead position and Mission Lead role have been replaced by Crew Lead (CL) and Mission Element Lead (MEL) positions, respectively, IAW updates made to Cyber Warfare Publication (CWP) 3-33.4 *Cyber Protection Team, Organization, Function & Employment*, 18 May 2022. The term "sortie" has been replaced by "event".

Chapter 1

GENERAL GUIDANCE

1.1. General. In conjunction with other governing directives, this volume prescribes procedures for operating the CVA/H weapon system. This manual applies to all ACC-assigned/attached organizations, airmen, and crewmembers who employ the CVA/H weapon system to achieve tasked mission objectives and designated crew position or work role responsibilities. This manual further applies to members in ACC-led formal training for immediate assignment to a CVA/H weapon system position.

1.1.1. Keywords explained.

1.1.2. “Must” indicates

1.1.3. “Should” indicates a preferred, but not mandatory, method of accomplishment.

1.1.4. “May” indicates acceptable or suggested means of accomplishment.

1.2. Crew Responsibility. Under most circumstances, this manual prescribes operations procedures for the CVA/H Weapon System, but it is not a substitute for sound judgment or common sense. Generally, except as noted in guidance that states an action “must” be carried out, operations or procedures not explicitly addressed in this manual accomplished if they enhance safety and effective mission accomplishment and are approved for execution by appropriate command authorities.

1.3. Alignment. Alignment of ACC operational statuses to United States Cyber Command (USCYBERCOM)-defined terms. CVA/H is leveraged by USAF 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)). Basic Mission Capable (BMC) status does not have a USCYBERCOM equivalency and will, therefore, remain the same. 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

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Mission Planning. As prescribed in Air Combat Command Instruction (ACCI) 17-202, Volume 3, *Cybercrew Operations and Procedures*, detailed mission planning helps ensure all members and an effective plan to understand mission objectives is developed to achieve those objectives. In preparation for and before each mission, crews will use tactical objectives provided through tasking orders and create tactical tasks for execution in the next mission.

2.2. Responsibility.

2.2.1. Squadron (SQ) Commanders (SQ/CCs) allocate resources, time, and space for mission planning. CCs will establish unit-specific mission planning guidance addressing mission essential tasks and will ensure an appropriate level of mission planning, compliant with requirements outlined in USCYBERCOM Instruction (USCCI) 3300-06, *Crew Operations and Procedures,* is conducted before each mission.

2.2.2. SQ Directors of Operations (DOs) (SQ/DOs) will ensure that all operations adhere to the Plan, Brief, Execute, and Debrief (PBED) process in accordance with (IAW) Higher Headquarters (HHQ) and squadron standards.

2.2.3. The lead cyber crewmember, usually the MEL, is ultimately responsible for ensuring all aspects of mission planning are accomplished. The lead crewmember will also ensure that all necessary crewmembers are present throughout the planning process. Additionally, the lead cyber crewmember will ensure currency of all mission planning materials and compliance with applicable HHQ, Joint, USCYBERCOM, network owner, and local command guidance.

2.3. Procedures. Cybercrews will adhere to the USCCI 3300-06 to plan, brief, and debrief all tactical missions to ensure thorough mission planning in conjunction with every mission. Unit CCs may supplement mission planning requirements and will ensure a sufficient level of planning is conducted before each mission. USCCI 3300-06, Attachment 2 is the designated mission planning resource. Additional elements for mission planning are covered in Air Force Tactics, Techniques, and Procedures (AFTTP) 3-1, *Cyber Vulnerability Assessment/Hunter*, AFTTP 3-1, *Advanced Cyber Threat Guide*, Chapter 13, AFTTP 3-3, *Integrated Planning and Employment*, CWP 3-33.4, as well as Wing and Group standards and local crew aids. These publications serve as tactical doctrines that are authoritative in nature and help ensure adequate mission planning and operational employment.

2.3.1. Units will accomplish sufficient planning to ensure successful mission accomplishment for all phases of an operation. At a minimum, mission planning will include an intelligence assessment (expected threats identification and counter-tactics); mission objectives and tactical tasks; capability and effects delivery; constraints; restraints; Rules of Engagement (ROE); applicable Special Instructions (SPINS); Blue Force deconfliction; cancel, abort, and rollback criteria; contingency plans; preplanned mission execution communications (also known as “contracts”); lessons learned; and a detailed incident response plan. Rehearsal of Concept (ROC) drills should be conducted before any execution employing the weapon system. At a minimum, the MEL should conduct a tabletop ROC drill before mission departure or execution. The Crew Information File (CIF) will be reviewed during the planning phase and validated during the ROC drill. **(T-3)**

2.3.2. Unit leadership will provide cybercrews with sufficient time and resources to accomplish mission planning and briefing. Units will ensure other activities, such as recurring academic training device periods, additional duties, and service administrative (e.g., ancillary training, awards packages) refrain from interfering with time allotted for mission planning and crew mission briefing. The lead crewmember is ultimately responsible for the proper conduct of mission planning, as mission planning must be accomplished by members who understand the capabilities and limitations of their infrastructure, tools, and terrain. Cyber crewmembers leading planning sessions must be, at minimum, BMC on the CVA/H weapons system. **(T-3)**

2.3.3. Subject Matter Experts (SMEs) external to the cybercrew may be used in the mission planning process. The lead crewmember should consider involving representation from other weapons systems or partner forces (e.g., local defender/cybersecurity services provider) if their capabilities are to be leveraged as part of the operation. **(T-2)**

2.3.4. All crewmembers will receive a mission briefing.

2.4. Debriefs. Post-mission debriefs will be conducted by the lead crewmember, and all crewmembers will be present. Debriefs will include, at minimum, an evaluation of task and objective fulfillment, any deviations from the mission plan, insights gleaned from lessons learned, acknowledgment of successes, introduction of new Tactics, Techniques, and Procedures (TTP), documentation of encountered anomalies, updates on task completion, and identification of manning or weapon system deficiencies. **(T-2)**

2.5. Intelligence Support. The lead crewmember will request support from unit-level intelligence or wing intelligence on current intelligence about mission tasking (as applicable). The lead crewmember will ensure all crewmembers receive a current intelligence briefing detailing current adversary activity, threat type, and adversary capabilities. Crews will review applicable TTP and implement approved TTP IAW mission requirements. Intelligence personnel will assess the intelligence value of information gathered during the mission and submit intelligence reports IAW **Attachment 4**, and update Requests for Information (RFI) as . **(T-2)**

Chapter 3

GUIDANCE AND PROCEDURES

3.1. Crew Logs. Crew logs are the official record of events during a crew shift or mission, whether live or simulated. IAW USCCI 3300-06, crew logs comprise various sources and documents such as the Master Station Log (MSL), Operator Notes (OpNotes), etc. Crew logs maintain an accurate and detailed accounting of all significant events, including any deviations from guidance in this manual or other HHQ guidance about operations occurring during each crew shift. A new log will be maintained for each event. The crew log may be kept in electronic format for accessibility purposes. At a minimum, crew logs will include identification of on-duty personnel, major operational activities, significant communications, major system degradations, other abnormal system responses, Standard Operating Procedures (SOPs), and TTP deviations. Units will maintain crew logs for one year.

3.2. Crew Information File (CIF). The CIF provides essential information to conduct mission operations and enable responses to emergency conditions. The CIF is a centralized solution to disseminate significant, time-sensitive issues and ensures standardized procedures reach all necessary operations personnel. All crewmembers must review any required CIF items and acknowledge them by signature before beginning cybercrew duties. **(T-3)**

3.3. Go/No-Go Procedures. IAW ACC17-202, Volume 2, *Cybercrew standardization/ Evaluation Program*, and ACCI 17-202V3 units will establish a positive control system ensuring cyber crewmembers have adequately completed all training and Stan/Eval items required for missions. The SQ/CC will provide written guidance on this system. Crewmembers will only operate on the weapon system once Go/No-Go procedures have been accomplished and verified. **(T-3)**

3.3.1. The SQ/CC will designate a crewmember, usually the MEL or CL, to conduct Go/No-Go verifications for a given event. **(T-3)**

3.3.2. Designated individuals will verify, document, and sign off on the Go/No-Go status before releasing crewmembers for scheduled missions. Go/No-Go accomplishment will be in the mission pre-brief as an essential briefing item. The unit will maintain records of the Go/No-Go accomplishment and verification for one year. **(T-3)**

3.3.3. At a minimum, the Go/No-Go program will monitor the following for each cyber crewmember:

3.3.3.1. Currency and proficiency of each scheduled crewmember IAW ACCMAN 17-2CVAHV1, *Cyber Vulnerability Assessment/Hunter (CVA/H) - Cybercrew Training,* and the CVA/H Ready Cybercrew Program Tasking Memorandum (RTM) for the crew position, mission, and duties they are scheduled to perform.

3.3.3.1.1. A non-fully mission-qualified (N-FMQ) cyber crewmember may occupy a crew position provided they are under instructor supervision and meet the currency requirements to regain FMQ status. The SQ/CC or designee will approve using an N-FMQ cyber crewmember on an event or mission.

3.3.3.1.2. The lead crewmember will coordinate with their respective unit scheduling function to replace cyber crewmembers who do not meet all required criteria. Suppose

the cyber crewmember cannot be replaced. In that case, the Mission Commander (MC) or designee will determine whether the mission can continue with the reduced cybercrew and either abort or continue with the execution. **(T-3)**

3.3.3.2. Currency and acknowledgement of all CIF (Volume 1, Part B) items.

3.4. Policy and Guidance.

3.4.1. Crewmembers will adhere to all HHQ-directed procedures (e.g., Technical Orders (TOs)). **(T-2)**

3.4.2. IAW ACCI 17-202V3 units will develop local procedures specific to their mission when operations fall outside existing Operating Instructions (OIs) and HHQ guidance. Local procedures will not be used to re-create or consolidate existing directives or HHQ guidance.

3.4.2.1. As stated in ACCI 17-202V3, units will adhere to directions published in TO 00-5-1, *Air Force Technical Order System,* or any directed templates from HHQ when developing local work cards, checklists, and Job Guides.

3.4.3. Crew Aids. Crewmembers are encouraged to develop local crew aids such as charts, question banks, guides, or other visual aids and processes to bolster proficiency and enhance mission briefings and effectiveness. Per ACCI 17-202V3, the SQ/DO will review and approve or reject all locally developed crew aids. Local crew aids will be coordinated through Group-level Stan/Eval or their designee. Any locally developed checklists, procedures, and crew aids may be more restrictive but not less restrictive than USCCI 3300-06.

3.4.4. Briefing Guides. Units will develop local briefing guides to ensure all necessary items are covered as required for each mission. Per ACCI 17-202V3, Group-level Stan/Eval, or designee, will determine minimum requirements for these guides and ensure standardization. **(T-3).** Examples in **Attachment 2**, and Attachment 2 of USCCI 3300-06.

3.5. Operational Procedures and Deviations. Without established SOPs, the MEL will coordinate with OPCON channels and the mission network owner to develop authoritative and directive operating guidance containing ROEs, constraints, and restraints at a minimum. In the case of an urgent requirement or emergency where the loss of life or disability or damage to equipment or infrastructure is more than likely, the MEL may deviate from established operational guidance to ensure crew safety, operational security, and mission accomplishment.

3.5.1. All equipment related to CVA/H, including Mobile Interceptor Platforms (MIPs), Deployed Interceptor Platforms (DIPs), Garrison Interceptor Platforms (GIP), routers, switches, and any other support equipment funded or provided by the Program Management Office (PMO), as well as licensed or unlicensed software and sensors, are considered integral components of the CVA/H Weapon System. It's important to note that scripts are not monitored as part of the CVA/H baseline.

3.5.1.1. CVA/H equipment and software are subject to strict configuration management control by the CVA/H PMO and will only be utilized for official government purposes.

3.5.1.2. CVA/H equipment will not be taken to non-government facilities or connected to unauthorized networks unless the activity is part of an approved mission, training, exercise, test, evaluation activity, official experiment, or weapon system or tactics development initiative. Upon conclusion of the activity, the equipment will be sanitized and re-baselined.

3.5.1.3. Unit CCs will hold individuals accountable for all violations of the CVA/H acceptable use policy and may decertify crewmembers from their crew position(s) pending completion of all unit commander-prescribed retraining and recertification requirements.

3.6. Normal Operations.

3.6.1. Vulnerability Window. For cybercrews, the vulnerability window is the task window for executing specific missions, tasks, and/or effects on the mission partner network (MPNET). The MEL will ensure all Go/No-Go actions, operations check, and planning actions are complete prior to the start of the vulnerability window (see **paragraph 3.6.4** for pre-mission responsibilities). The MEL will ensure all tasked actions are complete on the MPNET prior to end of the vulnerability window IAW tasking, established ROEs, and applicable guidance. If actions are not complete the MEL will request a vulnerability window extension or recommend rolling incomplete tasks to the next vulnerability window IAW HHQ guidance, tasking guidance, and ROEs.

3.6.2. Communications. During mission execution, conversations will occur through official communication channels and will consist of essential conversations necessary for cybercrew coordination and mission accomplishment. Crews should be aware that their communications are deemed "official communications" and may be recorded. Cyber crewmembers have no expectation of privacy on official communication channels.

3.6.2.1. The minimum requirement for mission execution is a primary and an alternate method of communication with all mission participants. The MEL will develop a communications plan to specify who should talk, when, and via which medium. A cyber crewmember will be designated to monitor the primary method of communication throughout the operation. The MEL will ensure all cyber crewmembers understand the communications plan. Check orders, tasking instructions, and ROE for applicable communication standards, check-in procedures, code words and brevity terms, etc. The communication plan should be practiced during a ROC drill.

3.6.2.2. Advisory Calls. Operators performing approved, but unexpected actions outside planned and/or main battle rhythm, will announce their intentions during the critical phases of operations IAW the established communications plan. These actions should be annotated in their crew log.

3.6.3. Operations Check (Ops Check). All oncoming cybercrews will accomplish sufficient Ops Checks to ensure safe and effective mission accomplishment. Each unit will ensure local procedures are established for performing Ops Checks that meet the minimum requirements listed below. If a cybercrew assumes responsibility during an ongoing mission, delay Ops Checks until mission tempo allows. The lead crewmember is responsible for ensuring Ops Checks are accomplished appropriately. Cybercrews will perform Ops Checks at initial check-in, as required during the event period, based on mission triggers, and as directed by HHQ guidance. **(T-3)**

3.6.3.1. Cybercrews will check the following items, at minimum, during an Ops Check:

3.6.3.1.1. Functionality of all communication channels (primary, secondary, etc.). **(T-3)**

3.6.3.1.2. Access (weapon system, MPNET, etc.). **(T-3)**

3.6.3.1.3. Firewall and security settings. **(T-3)**

3.6.3.1.4. Functionality of sensors, collectors, and/or weapon system components. **(T-3)**

3.6.3.1.5. Functionality of primary mission capabilities. **(T-3)**

3.6.4. Pre-mission Duties. Crews will complete required activities prior to each event or mission execution. **(T-3)**

3.6.4.1. Risk Management. Units will use Operational Risk Management (ORM) worksheets to address event risk factors. Risk management worksheets will address mission planning for the event, cybercrew experience, cybercrew personal risk factors, event complexity, event duration, risk to MPNET, and weapon system status. Weapon system status will include an impact assessment on all weapon system deviations employed without completing the formal weapon system modification process, as described in AFI 10-601, *Operational Capability Requirements Documentation and Validation*. The impact assessment must include the deviation's impact on the MPNET, authority to operate (ATO), and authority to connect. The MEL will ensure ORM worksheet completion prior to each event. **(T-3)**

3.6.4.1.1. Each operator is responsible for completing a personal ORM worksheet to identify individual risk factors and will provide the worksheet to the Crew Lead (CL) prior to the pre-mission brief. **(T-3)**

3.6.4.2. Go/No-Go. Crewmembers will not operate on the weapon system until the Go/No-Go has been accomplished and verified. **(T-3)**

3.6.4.3. Pre-Mission Briefing. Refer to USCCI 3300-06 for briefing templates and requirements.

3.6.4.4. Cybercrew Changeover. All cyber crewmembers will participate in a cybercrew changeover briefing when performing 24/7 or back-to-back events. If not performing 24/7 or back-to-back events, accomplish crew changeover requirements during the next day's pre-event briefing. At a minimum, the changeover will include all items previously identified for the pre-mission and pre-event briefings. **(T-3)**

3.6.5. Post-Mission Duties. Following mission completion, crews will complete required activities prior to being released to perform other duties or for crew rest. **(T-3)**

3.6.5.1. Mission Data Storage. The MEL will ensure all cyber crewmembers save all relevant mission data following mission completion. **(T-3)**

3.6.5.2. Cyber crewmembers will prepare their work areas for the following mission, when necessary.

3.6.5.3. Debriefing. All cyber crewmembers will participate in an official mission debrief. **(T-3)** The MEL is responsible for the overall mission debrief. Each CL is responsible for debriefing their individual crews. **(T-3)** Refer to **Attachment 3** and USCCI 3300-06 for briefing templates.

3.6.6. End of Event Duties. Units will develop and follow local procedures regarding End of Event activities.

3.6.6.1. The MEL maintains full control authority over the weapon system components from the start of the event through mission completion. MELs will declare event completion. Maintenance activities must not occur without MEL authorization.

3.6.6.2. Weapon System Maintenance and Re-Baselining. MELs will direct the disposition of weapon system equipment and data upon return to the home station; equipment must not be immediately turned in for Maintenance and re-baselining. Upon mission completion, the MEL will release the weapon system to Maintenance for re-baselining and sanitization. All maintenance and support actions involving the weapon system must be documented on an AFTO Form 95, *Significant Historical Data*, or automated equivalent.

3.6.6.3. Data Retention. The SQ/CC or designee will establish local data retention policies and procedures to satisfy operational requirements. The MEL will consult with mission partners on data retention concerns for data not owned by the CVA/H crew. All maintenance and support actions performed on the equipment must be documented IAW with Methods Procedures and Technical Orders (TO) 00-33A-1001, *Methods and Procedures General Cyber Defense Operations Activities Management Procedures and Practice requirements*, Chapter 7.

3.6.6.4. Crews will retain OpNotes, case management data (e.g., crew Command and Control (C2), analyst notes), mission plans, mission briefings, deviation information, learning points, finalized external reports (e.g., After Action Review (AAR), Situation Report (SITREP)), and supporting evidence (e.g., carved metadata, carved packet captures, selected files, hashes) for one year.

3.6.6.5. Full packet capture from the mission may be maintained at the discretion of the MEL in coordination with the mission partners for follow-on reporting and analysis as required. Upon completion of the mission, full packet captures may be deleted within 15 days or compressed for long-term storage for at most 90 days.

3.6.6.6. Data Destruction. The SQ/CC or designee will establish and execute local data destruction procedures. The MEL will consult with mission partners on destruction procedures for mission partner-owned data. Where there is conflict, the data owner’s destruction procedures take precedence. Units must account for classified destruction requirements and procedures as applicable. Data destruction should occur for all data not required to be retained within 15 days of mission termination.

3.6.6.7. Operational needs that necessitate a longer data retention period take precedence over the timelines established in this instruction.

Chapter 4

CREW FORCE MANAGEMENT

4.1. Crew Rest, Fatigue Management, and Duty Limitations. This section prescribes mandatory crew rest and maximum Duty Periods (DP) for all personnel who operate AF cyberspace weapon systems. Basic guidance for fatigue management strategies and waiver authority procedures are also addressed.

4.1.1. DP begins when a crewmember reports for an event, briefing, or other official duty and ends with the event completion.

4.1.2. The normal crew DP will not exceed 12 hours. **(T-3)**

4.1.3. The SQ/CC or designee may extend the maximum DP to two hours to compensate for unplanned event delays, provided the event requirements justify the increased risk. All extended DPs must be annotated in the appropriate log, at a minimum, detailing authorizing officials and crewmembers affected. Event or environmental needs that exceed a 14-hour DP require GP/CC approval.

4.1.4. Unless authorized DP, safety or an event is compromised by fatigue. In that case, the lead crewmember will restrict duty time, extend crew rest periods, and notify SQ leadership to generate an alternate crew or terminate the event.

4.1.5. The crew rest period is a 10-hour non-duty period before the DP begins.

4.1.5.1. The purpose of the crew rest period is to ensure crewmembers adequately rest before performing cyber warfare operations or event-related duties. Crew rest is free time and includes time for meals, transportation, and the opportunity for eight hours of uninterrupted sleep.

4.1.5.2. Any reduction from the 10-hour crew rest period requires pre-coordination for transportation, meals, and quarters so crewmembers are provided an opportunity for at least eight hours of uninterrupted sleep.

4.1.6. Crew rest is compulsory for any crewmember prior to performing any crew duty on any cyber weapon system.

4.1.7. Each crewmember is individually responsible for obtaining sufficient rest during crew rest periods.

4.1.8. Any official business or duty that requires the active participation of a crewmember outside of the DP interrupts the crew rest period. This official business or duty includes official business conducted via telephone or other electronic means. Intentional crew rest interruptions must only be made under the most exceptional circumstances. When crew rest is interrupted, the affected individual will inform a supervisor, and the lead crewmember will decide whether to remove the individual from the scheduled Event.

4.2. Operations Scheduling.

4.2.1. Units will publish, post, and monitor schedules for the crew force and initiate schedule changes based on tracking of qualifications, certifications, restrictions, crew rest, and other factors as required to meet mission objectives.

4.2.2. Schedulers should notify crewmembers of changes to scheduled operations no later than (NLT) 12 hours before the scheduled show time. Schedulers will notify the lead crewmember or affected members of the change as soon as possible.

Chapter 5

TECHNICAL RISK MANAGEMENT AND WEAPON SYSTEM DEVIATIONS

5.1. General.

5.1.1. The CVA/H is purpose-built and designed to detect, collect, contain, analyze, process, and store malicious code. It is designed to operate in compromised or potentially compromised environments. The CVA/H is also intended to perform threat replication and security assessment actions utilizing malicious code or code that replicates and/or emulates malicious activity.

5.1.2. Standard risks to enterprise systems are mitigated or eliminated within CVA/H weapon systems due to various technical and non-technical controls. These include but are not limited to, physical separation, logical separation, self-contained authentication mechanisms (for internal CVA/H weapon system resources), virtualization, containers, sandboxes, and mission-ready CVA/H crewmembers.

5.2. Technical Risk Management and Policies.

5.2.1. Cybercrew discipline is necessary for safe and effective CVA/H employment. The MEL or the CL should ensure all crewmembers maintain good cybercrew discipline and address misconduct appropriately. Cybercrew discipline includes but is not limited to conducting mission planning, maintaining OpNotes and crew logs, case management, weapon system security settings, respecting all components of the weapon system, reporting to duty as directed, keeping food and drinks away from components of the weapon system, following Operations Security (OPSEC) procedures, and safeguarding classified and sensitive information.

5.2.2. Safeguarding the Weapon System. The weapon system will be maintained within the units', or an approved Major Command (MAJCOM) facility approved for secure storage. Each cyber crewmember must safeguard weapon system components under their control. Positive control of the weapon system will be maintained when possible (e.g., by placing applicable components in carry-on luggage). When positive control is not possible, the weapon system will be secured with a reasonable expectation that it cannot be tampered with or manipulated, IAW applicable tamper detection guidance. Units will develop local procedures to supplement weapon system safeguarding guidance when necessary.

5.2.2.1. Weapon System Authentication. Crews will follow all published guidance and technical orders concerning system passwords. (e.g., AFI 17-130, *Cybersecurity Program Management*).

5.2.2.2. Units will establish local procedures for unique processes related to weapon system password management. Local procedures must be approved by the SQ/CC or designee before implementation.

5.2.3. Weapon System Handling. Units will follow the CVA/H Configuration Management Plan (CMP) and ensure local policy is established to enforce proper handling of the weapon system.

5.2.4. Weapon System Transport. When crewmembers travel with the weapon system on commercial transportation, the MEL or lead crewmember will ensure all precautions are taken to safeguard it from damage and theft.

5.2.4.1. Units will provide specific guidance on transporting or shipping weapon system components.

5.2.4.2. Methods of conveyance will not allow unauthorized personal custody or control of the system's components while in transit.

5.2.5. Weapon System Classification. CVA/H missions may occur on classified networks. CVA/H personnel will ensure the weapon system is labeled and handled appropriately based on classification. Crews will comply with all published security classification guidance and weapon system classification procedures IAW the TO, CVA/H CMP, and local SOPs to ensure operation IAW appropriate classification level.

5.2.6. External Devices and Media. All external devices and media added or attached to the weapon system to improve functionality must be approved through the configuration management process before use (e.g., hard drives, Wi-Fi antennas). External devices and media required for the mission (e.g., for forensics) will be assessed for risk by the DO before being attached to the weapon system.

5.2.7. Data Transfer. CVA/H crewmembers are authorized to transfer data to CVA/H via local procedures. Transfers from trusted sources (e.g., United States Government (USG) systems or services) are authorized, and members will follow local procedures for data transfers. Transfers from public sources (e.g., open-source scripts, data, visualizations) on missions will be accomplished through a designated "dirty" file transfer MIP. Members will scan the file for viruses and transfer it to operational CVA/H components IAW local procedures.

5.2.8. In-Garrison Training, Innovation, Experimentation, Research, and Tactics Development. CVA/H components and builds may be used in garrison isolated or with designated CVA/H components (e.g., designated CVA/H garrison systems) for training, innovation, research, experimentation, and tactics development. Operators are authorized to reconfigure and/or otherwise introduce software changes to CVA/H without written approval, subject to SQ/DO oversight. Before deploying on a mission, CVA/H assets in a non-standard/non-baseline configuration will be fully reimaged.

5.2.9. Software Upgrades (Minor release and bug fixes). Between formal PMO-provided updates, units may upgrade software resident on or provided with CVA/H to the latest minor release or bug fix builds for software on the CVA/H ATO. Operators will obtain the software from the appropriate trusted repository and validate the authenticity (e.g., compute a hash for the upgrade and compare it with the vendor-provided hash). This does not constitute a deviation. Units will work with their Information System Security Officer (ISSO) to submit a No Security Impact (NSI) memo to the CVA/H PMO for annotation within the CVA/H ATO.

5.2.10. Major releases of software components that create no significant adverse impact on other CVA/H components or capabilities may be used if operationally necessary. Follow the same process outlined in **paragraph 5.2.9** to employ the newer version.

5.2.11. Weapon System Deviations. A weapon system deviation is defined as "the introduction of stand-alone third-party compiled code, firmware, or hardware not on the

CVA/H ATO package, and/or compiled code, firmware, or hardware on the ATO package that is a significantly newer version (e.g., a major release with substantial code changes 7.1.2 to 7.1.3 is minor, 7.1.2 to 7.2 is major).

5.2.11.1. Deviations will only be used when:

5.2.11.1.1. The modification is critical to mission success, with mission failure occurring if not implemented.

5.2.11.1.2. Adhering to the standard configuration change and weapon system modification process would result in mission failure.

5.2.11.2. Deviation Approval and Procedures. CVA/H crews must follow implementation guidance for deviations set forth within the CMP for CVA/H. MELs will handle deviation request submission, coordination, and risk assessment. Approval authority for deviations is set at the following levels:

5.2.11.2.1. SQ/DO: Deviations that do not interact with an MPNET (e.g., no bi-directional communications) and are isolated CVA/H components.

5.2.11.2.2. SQ/DO (with the consent of the training range/simulator owner): Deviations that interact with/are deployed to a training range/simulator in a bi-directional manner.

5.2.11.2.3. SQ/CC (with the consent of MPNET system owner): Deviations that interact with, or are deployed to, an MPNET in a bi-directional manner.

5.2.11.3. Deviation Duration. A single deviation is authorized for the entire duration of a named operation, or six months, whichever is longer. The deviation may only be approved up to two times for other operations before an AF Form 1067, *Modification Proposal,* must be submitted.

5.2.11.4. Deviations for the same capability, software, or hardware may be authorized twice for the same CVA/H crew. If the capability is required beyond two deviations, follow the appropriate process to add the capability to the CVA/H baseline. When a situation arises during a mission that requires action outside the normal scope of the mission or tools that are not approved and validated and were submitted for approval awaiting process completion, the MEL will notify the SQ/DO for immediate approval. Under rare circumstances, if the MEL cannot contact the SQ/DO, the MEL has the delegated authority to make a decision concerning the deviation, ensure proper documentation, and notify the SQ/DO and the Weapons and Tactics flight at the first opportunity.

5.2.11.5. Deviation Notification. Teams will submit copies of approved deviation requests to their Squadron Weapons and Tactics (DOK) shop, Wing Weapons and Tactics Shop, and CVA/H PMO at minimum.

5.2.11.6. Deviation Debriefs. Teams will debrief the effectiveness of the deviation and provide a written deviation debrief report to their SQ/DO, SQ Weapons and Tactics shop, Wing Weapons and Tactics shop, and CVA/H PMO.

5.2.12. Sandbox, Reverse Engineering, Forensic Analysis, Malware Detonation. CVA/H provides capabilities to sandbox, reverse engineer, execute, and analyze code, including malware. When employing these capabilities against known or suspected malware,

crewmembers should exercise due diligence and, where possible, separate systems performing this function from other operational CVA/H components and MPNET. Physical separation (e.g., dedicated hardware without network connection) is preferred, but where not possible, logical separation should be utilized (e.g., virtual local area network segmentation, firewall access control lists, sandbox, isolated virtual machines).

5.2.13. All deficiencies must be reported IAW TO 00-35D-54, *USAF Deficiency Reporting, Investigation, and Resolution*. Alternative deficiency reporting systems such as "Bug Reports" are prohibited. Deficiencies are defined in Chapter 1 of TO 00-35D-54.

Chapter 6

CVA/H CYBERCREW POSITIONS

6.1. General. CVA/H cyber crewmembers include a Host Analyst (HA), Network Analyst (NA), Mission Element Lead (MEL), and CL. Support personnel (i.e., Network Technician and Source Analyst) utilizing CVA/H will follow certification requirements outlined in ACCMAN 17-2CVAHV1, *Cyber Vulnerability Assessment/Hunter (CVA/H) - Cybercrew Training*. Utilization covers the actions of configuring, imaging, installing, sanitizing between classification levels, maintenance or replacement of components, use of MIP software for research, analyzing information retrieved from the DIP, and office automation applications for supporting operations and crew reporting. Non-qualified support personnel cannot utilize the CVA/H weapon system to employ effects on the MPNETs or systems.

6.1.1. The MEL and CL are not work roles and can be drawn from HA or NA work roles. They are not considered leadership positions that require leadership certification. Please see CWP 3-33.4, *CPT Organization, Function, and Employment,* for further guidance on the CVA/H Leadership work roles.

6.2. Host Analyst (HA). A CVA/H HA specializes in advanced vulnerabilities and threats in host system hardware and software. HAs possess the skills and knowledge to assess a targeted host system's configuration, settings, and activity to identify weak security, vulnerabilities, or maliciously configured systems. HAs are the experts utilized for incident investigations and counter-threat actions on their specific host system type. HAs can create scripts for a targeted host system to assess the health and gather information that other operators can analyze or use to determine actions.

6.3. Network Analyst (NA). A CVA/H NA specializes in advanced vulnerabilities and threats to network architectures, technologies, and associated systems. NAs possess the knowledge and skills to reconstruct a network to analyze the data collected from captures and flow data. NAs can identify misconfiguration and malicious activity based on observable network traffic. NAs assess configurations, settings, and network activity to identify security gaps, vulnerabilities, and maliciously configured network infrastructure. NAs are utilized for incident investigations and counter-threat actions on network infrastructure.

6.4. Mission Element Lead (MEL). A MEL leads a cybercrew during mission planning, briefing, mission execution, and debriefing. They are responsible for task management, communications management, mission execution, and equipment management for their ME. The MEL generates the overall mission plan and daily execution plan for their element. They are the focal point for coordination between the ME and leadership and will consolidate RFIs, SITREPs, and other reports.

6.5. Crew Lead (CL). The CL is responsible for their crew and events. CLs are responsible for managing the direct tasks of the HAs and NAs within their cybercrew and managing the communications between them and the MEL. When only one crew exists, the CL for that crew is also the Mission Element Lead (MEL).

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

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION.

References

5 USC § 552a, *Records Maintained on Individuals*

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) - Cybercrew Training,* 28 October 2024

AFI 10-601, *Operational Capability Requirements Documentation and Validation*, 27 April 2021

AFI 17-130, *Cybersecurity Program Management*, 13 February 2020

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

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

AFTTP 3-1. *Cyber Vulnerability Assessment/Hunter*, 12 June 2018 (S//US/AUS/GBR)

AFTTP 3-1. *Threat Guide Chapter 13,* 10 December 2018 (Contents are S//NF)

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

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

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

CVA/H Configuration Management Plan (CMP)Annex Version 2.4, 31 October 2023

DAFI 36-2608, *Military Personnel Records System*, 16 April 2021

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

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

DoD 5400.11-R, *Department of Defense Privacy Program*, 14 May 2007

TO 00-33A-1001, *Methods and Procedures General Cyber Defense Operations Activities Management Procedures and Practice requirements*, 11 December 2023

TO 00-5-1, *Air Force Technical Orders System*, 13 September 2023

TO 00-35D-54, *USAF Deficiency Reporting, Investigation, and Resolution, 15 August* 2023
USCCI 3300-06, *Crew Operations and Procedures, 9 March 2018*

Prescribed Forms

None

Adopted Forms

ACC Form 4418, *Certificate of Cybercrew Qualification*

AF Form 1067, *Modification Proposal*

AFTO Form 95, *Significant Historical Data*

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AAR—After Action Review

ACC—Air Combat Command

ACCI—Air Combat Command Instruction

ACCMAN—Air Combat Command Manual

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFR—Air Force Reserve

AFRIMS—Air Force Records Information Management System

AFTTP—Air Force Tactics, Techniques, and Procedures

ANG—Air National Guard

AO—Area of Operations

AOR—Area of Responsibility

ATO—Authority to Operate

BCQ—Basic Cyber Qualified

BMC—Basic Mission Capable

C2—Command and Control

CC—Commander

CL—Crew Lead

CIF—Crew Information File

CMP—Configuration Management Plan

CMR—Combat Mission Ready

CNMF—Cyber National Mission Force

CPT—Cyber Protection Teams

CTO—Cyber Tasking Order

CVA/H—Cyber Vulnerability Assessment/Hunter

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DAFMAN—Department of the Air Force Manual

DAFPD—Department of the Air Force Directive
DCO—Defensive Cyberspace Operations
DFP—Debrief Focal Points
DIP—Deployed Interceptor Platform
DP—Duty Periods
DO—Director of Operations (Unit Level)
DOC—Designed Operational Capability
DoD—Department of Defense
DODI—Department of Defense Instruction
DTG—Date Time Group
FT—Fully Trained
GIP—Garrison Interceptor Platform
HHQ—Higher Headquarters
HA—Host Analyst
IAW—In Accordance With
INTREP—Intelligence Report
IP—Internet Protocol
IQT—Initial Qualification Training
ISSO—Information System Security Officer
IST—Initial Skills Training
MAJCOM—Major Command
MC—Mission Commander
MDS—Mission Design Series
MISREP—Mission Report
MIP—Mobile Interceptor Platform
MEL—Mission Element Lead
MPNET—Mission Partner Network
MQT—Mission Qualification Training
MSL—Master Station Log
MSGID—Message Identification
MX—Maintenance
N-CMR—Non-Combat Mission Ready

N-FMQ—Non-Fully Mission-Qualified

NA—Network Analyst

NLT—No Later Than

NSI—No Security Impact

OI—Operating Instruction

OPCON—Operational Control

OpNotes—Operator Notes

Ops Check—Operations Check

OPORD—Operations Order

OPR—Office of Primary Responsibility

OPSEC—Operations Security

ORM—Operational Risk Management

PBED—Planning, Briefing, Execution, and Debriefing

PEX—Patriot Excalibur

PMO—Program Management Office

POC—Point of Contact

RCP—Ready Cybercrew Program

RDS—Records Disposition Schedule

RFI—Request for Information

ROC—Rehearsal of Concept

ROE—Rules of Engagement

RTM—Ready Cybercrew Program Tasking Memorandum

SITREP—Situation Report

SPINS—Special Instructions

SME—Subject Matter Expert

SMQ—Special Mission Qualification

SOP—Standard Operating Procedures

SORN—System of Records Notice

SQ—Squadron

Stan/Eval—Standardization and Evaluation

TO—Technical Order

TTP—Tactic, Technique and Procedures

US—United States

USAF—United States Air Force

USCCI—United State Cyber Command Instruction

USCYBERCOM—United States Cyber Command

USG—United States Government

Office Symbols

ACC/A3—ACC Director of Operations

ACC/A3/2/6K—Air Combat Command (ACC) Information Warfare Division

CNMF J6/8/9—CNMF

Terms

All-Source Analysts—Each CVA/H is assigned all-source analysts to support CVA/H intelligence requirements and serve as the CVA/H's inject point into the intelligence community. CVA/H all-source analysts request intelligence information in support of operations and report operational data and other information into the intelligence system for further processing and analysis.

Basic Mission Capable (BMC)—A cybercrew member who has satisfactorily completed IQT and MQT but does not conduct operations as their primary organizational mission. This status is normally assigned to crew members with staff functions directly supporting cyber operations (e.g., wing staff, OSS personnel). CVA/H cybercrew members in BMC status must be able to attain FMQ (i.e., CMR) status within 30 days (90 days for ARC).

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, *Certificate of Cybercrew Qualification*, and documentation.

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

Combat Mission Ready (CMR)—A cybercrew member who has satisfactorily completed IQT and MQT, and maintains certification, currency, and proficiency in the command or unit's operational mission. CMR has been changed to FMQ to align with USCYBERCOM terminology.

Crew Information File (CIF)—The CIF is required to ensure that information essential to the conduct of operations or emergency conditions is available. The CIF centralizes significant and/or time-sensitive issues and ensures procedures are disseminated to operations personnel. Standardization and Evaluation personnel use the CIF to make critical operational information available to crewmembers.

Crew Lead (CL)—The CL is responsible for their crew and events. When only one crew exists, the CL for that crew may also function as the MEL.

Currency—A measure of how frequently and/or recently a task is completed. Currency requirements should ensure that the average cyber crewmember maintains a minimum level of proficiency in a specific event.

Cybercrew—Also referred to as crewmembers; consists of individuals who conduct cyberspace operations and are typically assigned to a specific weapon system.

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

Cyber Crew Operations Deviation—Performing action(s) not in sequence with current procedures, directives, or regulations. Performing action(s) out of sequence due to unusual or extenuating circumstances is not considered a deviation.

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

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

Host Analyst (HA)—A CVA/H crew position. A CVA/H HA specializes in advanced vulnerabilities and threats in the hardware and software of host systems. They have the skills and 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 counterthreat actions on their specific host system type. They can create scripts for a targeted host system which can assess the health and gather information that other operators can analyze or use to determine actions.

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

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

Mission Element Lead (MEL)—The MEL has ultimate authority for a CVA/H event and is responsible for the overall execution of the mission.

Mission Report (MISREP)—Report ensuring tasking authority awareness of completed mission and/or mission phase results to provide information necessary to direct future operational tasks.

Network Analyst (NA)—A CVA/H crew position. 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 and malicious activity based on the observable traffic of the network. They would assess the configuration, settings, and activity of a network 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.

Network Technician—Providing technical assistance to the mission element by ensuring the team CVA/H Systems or equivalent kits are ready and available. Provides planning and conduct training

for the mission elements. Assisting mission elements to develop and establish collection and reporting performance and effectiveness measures.

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

Rules of Engagement (ROE)—Directives issued by competent military authority delineate the circumstances and limitations under which US forces will initiate and continue engagement with other forces encountered.

Situation Report (SITREP)—Report to mission partner and/or tasking authority providing situational awareness on events occurring during the current event that are outside of the expected parameters for the event.

Special Mission Qualification (SMQ)—An SMQ is an additional qualification added to a crew position 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.

Task—A clearly defined action or activity specifically assigned to an individual or organization by an appropriate authority.

Team Lead (TL)—The TL leads the CVA/H Support Element which directs and trains CVA/H personnel and provides synchronized mission planning, information sharing, and operational management of the mission and support elements to ensure cohesion and mutual support. The TL serves as the point of entry supporting tactical planning and C2 for higher headquarters, supported commanders, network owners, and mission partners.

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.

Vulnerability Window—A window of opportunity and direction for a tactical commander to conduct tactical operations. A vulnerability window is time- bounded (start by/finish by) to provide a tactical commander with the authorized and suspended timing available to plan and execute missions. Deviations from the assigned vulnerability window must be approved by HHQ.

Weapon System Deviation—Critical changes or modifications to the weapon system are required by an urgent mission-critical need that satisfies both mission and time critical criteria. 1) The modification must be critical to mission success, with mission failure occurring if not implemented, and 2) Following the normal configuration change and weapon system modification process would result in mission failure.

Attachment 2

BRIEFING GUIDE

A2.1. Briefing Guides. This attachment provides items for guidance and consideration when developing unit briefing guides. Additional guidance and information can be found in USCCI 3300-06 and other mission planning documents. These manuals are authoritative, not directive, and should be considered when developing unit specific guides. Units may augment these guides as necessary. Mission related items may be briefed in any sequence, provided all minimum requirements listed in this publication and other local directives and guidance are addressed.

A2.2. MISSION BRIEF.

A2.2.1. Situation - Environment, friendly forces, enemy forces, threat overview

A2.2.2. Mission - What you want to achieve, primary tasks and objectives

A2.2.3. Execution - Intended "how" to accomplish the mission

A2.2.4. Administration/Logistics - Abort criteria, transport, equipment, supplies, and coordination of resources

A2.2.5. Command & Control - Communication, succession of command

A2.3. PRE-EVENT BRIEF.

A2.3.1. Timehack / Roll Call / Classification

A2.3.2. Intel Threat Brief

A2.3.3. Open RFIs

A2.3.4. Weapon System Status / Open MX Tickets

A2.3.5. Mission Partner Activity / Status / Deconfliction

A2.3.6. Tasking Instructions/ROE

A2.3.7. Commander's Intent / Mission Objectives

A2.3.8. Outstanding events from previous event

A2.3.9. Tactical Objectives

A2.3.10. Tactical Tasks and MOPs

A2.3.11. Push Times / Execution Period

A2.3.12. Contingencies / Emergency Procedures / Abort Criteria

A2.3.13. Event Risk Assessment

A2.3.14. CIF / Go/No-Go / Supervision statuses

A2.3.15. Key Contact Information / Coordination or Communication Card

A2.3.16. Mission Websites / Links / Chat / Databases

A2.3.17. Contracts / Roles & Responsibilities

Attachment 3

DEBRIEFING GUIDE

A3.1. Debriefing Guides. This attachment provides items for guidance and consideration when developing unit debriefing guides. Additional guidance and information can be found in USCCI 3300-06 and other mission planning documents. These manuals are authoritative, not directive, and should be considered when developing unit specific guides. Units may augment these guides as necessary. Mission related items may be debriefed in any sequence, provided all minimum requirements listed in this publication and other local directives and guidance are addressed.

A3.2. DEBRIEF COMPONENTS.

A3.2.1. Classification

A3.2.2. ROE

A3.2.3. Admin/Alibis

A3.2.4. Objectives

A3.2.5. Debrief Planning (use debriefing process)

A3.2.6. Debrief Execution (use debriefing process)

A3.3. DEBRIEFING PROCESS.

A3.3.1. Gather data for mission reconstruction

A3.3.2. Reconstruct execution of mission

A3.3.3. Assess mission objective and task accomplishment

A3.3.4. Identify “Big Rocks”

A3.3.5. Generate Debrief Focal Points (DFPs)

A3.3.6. “Walk Down” from DFP

A3.3.7. Identify Contributing Factors to the Root Cause

A3.3.8. Identify Root Cause

A3.3.9. Create Instructional Fix to Root Cause

A3.3.10. Document Lessons Learned

Attachment 4

MISSION / SITUATION REPORT / INTELLIGENCE REPORT TEMPLATE

A4.1. Content.

A4.1.1. CLASSIFICATION/ <classification>/<classification source>/<Declassify on Date-Time-Group (DTG)>

A4.1.2. OPER/EXER/<OPORD/EXORD>/<OPORD TITLE>

A4.1.3. MSGID/<MISREP/SITREP/INTREP>/MIL-STD-6040(SERIES)/B.0.01.00/<Originating Unit>/<DTG>/<country>

A4.1.4. REF/<only used when referencing another mission, that mission MSGID input here>

A4.1.5. POC/<FULL NAME>/<RANK/GRADE>/<Unit>/<Base>/<Phone #>/<email>

A4.1.6. MSNINFO/<CTO date>/<Msn #>/<Did the mission execute? YES/NO>/<Abort reason>/<# of packages>/<Msn type>

A4.1.7. AMPN/<Abort explanation amplification>

A4.1.8. FLTDTAIL/<Callsign>/<Weapon system>/<unit>/A/<In Execution report? YES/NO>/<Post-Mission debrief DTG>/<departure DTG>/<Mission complete DTG>

A4.1.9. AMPN/<Mission Explanation>

A4.1.10. MSNLOC/<start DTG>/<stop DTG>/<Mission Location>/<Terrain (system name, network)>

A4.1.11. AMPN/<CAT event # (If Applicable)>;

A4.1.12. TGTPOS/<Network or System Type>/<Target ID>/<Target Description>/

A4.1.13. RESULT/<DTG>/<Achieved mission tasking YES/NO>/<Not Achieved reason>/<Mission Results>

A4.1.14. AMPN/<CAT event # (If Applicable)>

A4.1.15. NARR/<Overall Mission Explanation (i.e., short important point narrative)>