BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-1703, VOLUME 1

2 APRIL 2014

Incorporating Change 1, 6 May 2015

Operations

CYBERCREW TRAINING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

OPR: AF/A6SS

Certified by: AF/A3C/A6C
(Maj Gen Earl D. Matthews)

Pages: 18

This instruction implements Air Force Policy Directive (AFPD) 10-17, *Cyberspace Operations*. This instruction establishes the Cybercrew Training Program (CTP) that supports Air Force (AF) objectives and provides guidance on how to structure and monitor a cyber training program. This publication applies to all military and civilian AF personnel, members of the AF Reserve Command (AFRC), Air National Guard (ANG), third-party governmental employee and contractor support personnel in accordance with appropriate provisions contained in memoranda support agreements and AF contracts. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 (*5 U.S.C. 552a*). System of Records Notices F036 AF PC C, Military Personnel Records System, and OPM/GOVT-1, *General Personnel Records*, apply. Units may supplement this instruction. Coordinate supplements through HQ AFSPC/A3T prior to publication. Coordinate MAJCOM supplements with AF/A6SS. Guidance provided by the lead major command should contain specific training requirements unique to individual and crew positions. Send recommended changes or comments to HQ USAF/A6SS, 1480 Air Force Pentagon, Washington, DC 20330-1480, through appropriate channels, using AF Form 847, *Recommendation for Change of Publication*. When collecting and maintaining information protect it by the Privacy Act of 1974 authorized by 10 U.S.C. 8013. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the AF Records Disposition Schedule (RDS) located in the AF Records Management Information System (AFRIMS). See attachment 1 for a glossary of references and supporting information.

SUMMARY OF CHANGES

This interim change revises AFI 10-1703, Volume 1, by incorporating changes identified during the compliance statement review and updating office symbols and references. Several tiering codes have been updated and related language changed to improve readability and clarify responsibilities.

1. General. This instruction prescribes basic policy and guidance for training AF cybercrews according to AFPD 10-17.

1.1. **Program Goals**. The AF CTP ensures all cybercrew members obtain and maintain the certification/qualification and proficiency needed to effectively perform their unit's mission. The objective of the CTP is to develop and maintain a high state of mission readiness for immediate and effective employment across the full range of military operations, while structuring each training mission to achieve optimum training experience.

1.1.1. Cybercrews consist of individuals who conduct cyberspace operations and are assigned to a specific cyber weapon system. Personnel who perform cyberspace intelligence, surveillance, and reconnaissance (ISR) functions do not fall under the purview of this instruction; training for these personnel is addressed in the 14-2XX series of AF Instructions.

1.1.2. This AFI applies to cybercrew positions that are designated mission ready/combat mission ready (MR/CMR) in guidance provided by the lead major command. Personnel filling MR/CMR positions at the 624 OC and the 960 CyOG-Det 1 (854th Command Control Squadron (CSS) (AFRC)) will adhere to guidance in Paragraphs 1 through 1.3.5.6, and applicable Lead MAJCOM provided policy and guidance.

1.1.3. Individuals who perform cyberspace support functions but are not assigned to a MR/CMR crew position within a weapon system follow the Quality Assurance policy in AFI 33-150, *Management of Cyberspace Support Activities*, and/or AFI 36-2201, *Air Force Training Program*, as applicable.

1.2. **Waiver Authority**. 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 AFI 33-360, Publications and Forms Management, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers as described in this paragraph.

1.2.1. HQ USAF/A6SS is the waiver authority for this instruction. Unless otherwise noted, HQ USAF/A6SS delegates waiver authority to HQ AFSPC/A3T. Waiver authority may not be further delegated.

1.2.2. Forward all waiver requests via email through the applicable Group/CC, NAF/A3 or NAF/OV (as applicable), to HQ AFSPC/A3T. Describe the specific requirement, state the reason a waiver is required, and include proposed risk management steps, as needed. Specify an expiration date for the waiver, if applicable. Intermediate command levels should recommend approval or disapproval of the waiver request.

1.2.3. If approved, waivers remain in effect for the life of the published guidance, unless HQ AFSPC/A3T specifies a shorter period of time, cancels in writing, or issues a change that alters the basis for the waiver.

1.2.4. AF Reserve Units. HQ AFRC/A3T is the waiver authority for this instruction for reserve units. AFSPC gained units process waivers IAW paragraph 1.2. The reserve group commander submits waiver requests through 10 AF/A3 to HQ AFRC/A3T. HQ AFRC/A3T provides a copy of the waiver request and HQ AFRC/A3T waiver decision to HQ AFSPC/A3T.

1.3. **Responsibilities**.

1.3.1. HQ USAF/A3C/A6C:

1.3.1.1. Formulates cybercrew training Concept of Operations (CONOPS).

1.3.1.2. Sets policy and guidance for the conduct and execution of the cybercrew training program, in coordination with the Lead MAJCOM.

1.3.1.3. Oversees development and management of cybercrew weapon system designations.

1.3.1.4. Oversees Lead MAJCOM development and management of all cyber policy and guidance documents.

1.3.1.5. Monitors and reviews MAJCOM programs to ensure MAJCOM policies, guidance and instruction supplements are adequate.

1.3.1.6. Hosts training conferences annually, or as required, to assist in maintaining appropriate commonality and identify shortfalls in cybercrew training programs. Base the attendee list on conference topics.

1.3.1.7. Coordinates cyber intelligence, surveillance and reconnaissance (ISR) requirements with HQ USAF/A2D.

1.3.2. HQ USAF/A2:

1.3.2.1. Formulates cyberspace ISR training requirements and manages ISR-related training issues.

1.3.2.2. Coordinates cyberspace ISR training requirements and issues with HQ USAF/A3C/A6C and HQ AFSPC/A3T as required.

1.3.3. HQ AFSPC (As Lead MAJCOM):

1.3.3.1. Develops and manages cybercrew weapon system designations.

1.3.3.2. Develops and manages, in coordination with user commands, the appropriate guidance documents to establish cybercrew training requirements and standards, regardless of mission designation and command of assignment. Refer to Attachment 2 for information on training development.

1.3.3.3. Hosts annual, or as required, weapon system-specific training conferences to review all programs for currency, applicability, compliance, and effectiveness, and address issues in lead command-provided guidance documents as appropriate. Attendees should include training representatives from career field managers, user commands, formal schools, Numbered Air Force (NAF) training and stan/eval offices (if applicable), and selected unit representatives. Submit formal training requirements to career field managers for incorporation in Utilization & Training Workshop process as defined in AFI 36-2201.

1.3.3.4. Determines total force cybercrew training requirements in coordination with National Guard Bureau (NGB)/AF Reserve Command (AFRC) across the FYDP. Forward requirements annually to HQ USAF/A3C/A6C, via the Program Requirements Document (PRD), for validation and inclusion in the Undergraduate and Graduate PGLs.

1.3.3.5. Follows AFPD 10-9, *Lead Command Designation and Responsibilities for Weapon Systems*, for additional responsibilities.

1.3.4. All MAJCOMs (with assigned cybercrews IAW para 1.1 and AFPD 10-17).

1.3.4.1. Establish a cybercrew training office responsible for the overall management of the command's cybercrew training program. (Air National Guard (ANG) is considered a MAJCOM for purposes of this instruction.)

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

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

1.3.4.4. Send proposals for amending existing formal school course prerequisites and syllabi or deleting obsolete courses to the training command for approval.

1.3.5. All NAFs (with assigned cybercrews IAW para 1.1).

1.3.5.1. Establish a cybercrew training office responsible for the overall management of the cybercrew training program.

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

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

1.3.6. Training Command.

1.3.6.1. Is a command which operates a cyber weapon system and provides operational training for cybercrews.

1.3.6.2. Maintains quota allocation and management responsibilities.

1.3.6.3. Captures inputs from Air Staff, AFPC, lead and user MAJCOMs, and other users in the allocation of training quotas in order to fulfill maximum total force training requirements within programmed capacity.

1.3.6.4. Approves formal school courses and syllabi in coordination with lead commands and program managers.

1.3.6.5. Develops, updates, and maintains courseware and training syllabi to support Mission Essential Tasks (METs). Performs task and media analysis associated with cybercrew qualification training per AFI 36-2201; AFI 36-2251, *Management of Air Force Training Systems*; and function as the approving authority for these courses (coordinates with the lead command if different than the training command).

1.3.6.6. Outlines procedures for a Progress Review (PR) to be accomplished when a student fails to progress according to syllabus requirements.

2. Qualification Training. This section defines cybercrew operational status and specifies minimum training requirements for Initial Qualification Training (IQT) and Mission Qualification Training (MQT).

2.1. **Cybercrew Operational Status.** A cybercrew member may be assigned Basic Cyber Qualified (BCQ), Basic Mission Capable (BMC), or Mission Ready/Combat Mission Ready (MR/CMR) status.

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

2.1.2. Basic Mission Capable (BMC). A cybercrew member who has satisfactorily completed IQT and MQT, but is not in fully-certified MR/CMR status. The cybercrew member must be able to attain MR/CMR status to meet operational taskings as specified in the applicable lead MAJCOM-provided guidance **(T-1)**. Identify BMC requirements in the applicable lead MAJCOM-provided guidance.

2.1.3. Mission Ready (MR)/Combat Mission Ready (CMR). A cybercrew member who has satisfactorily completed IQT and MQT, and maintains certification, currency and proficiency in the command or unit operational mission is MR. A cybercrew member who has satisfactorily completed IQT and MQT, and maintains certification, currency and proficiency in the command or unit combat mission is CMR. Minimum requirements include:

2.1.3.1. Completion of IQT, MQT, and a formal Stan/Eval evaluation.

2.1.3.2. Certifying Official's (first operational commander in the member's chain of command, or his/her designee) certification as well as certification of completion of unit-designated crew force management requirements.

2.1.3.3. Once a certifying official (or his/her designee) certifies an individual as MR/CMR, the individual maintains MR/CMR status based on Continuation Training (CT) requirements identified in paragraph 3.

2.2. **Initial Qualification Training (IQT).** One or more courses covering system specific and/or positional specific training as a prerequisite to Mission Qualification Training (MQT).

2.2.1. Method. Unless otherwise specified in applicable lead MAJCOM guidance, the primary method of IQT is to attend and complete the appropriate formal training course(s) listed in the Education and Training Course Announcement (ETCA) found at **https://etca.randolph.af.mil**, USAF Formal Schools. Completing the appropriate formal course(s) satisfies all IQT requirements.

2.2.2. In-Unit IQT. When formal course attendance is not practical or quotas are not available, units will request waivers to conduct in-unit IQT, using formal school courseware, as specified in the applicable lead MAJCOM- provided guidance **(T-2)**. Accomplish in-unit training IAW applicable formal school courseware and the following guidance: **(T-2)**:

2.2.2.1. Training lessons should be completed in order; however, if mission scheduling or student progress dictates otherwise, the unit commander or designee may change the order.

2.2.2.2. Training syllabi establish a maximum time period between training events. Failure to accomplish training as scheduled requires documentation and corrective action.

2.2.2.3. With operations group commander (OG/CC) (or equivalent) approval, IQT requirements may be completed during operational missions under the supervision of an instructor certified on the task of like specialty. Comply with restrictions in appropriate lead MAJCOM-provided guidance, MAJCOM directives, and applicable operation orders (OPORD).

2.2.2.4. Cybercrew members participating in in-unit IQT are dedicated to that training, which takes priority over non-training related duties. ***EXCEPTION:*** Supervisory personnel may continue their normal duties as time permits.

2.2.3. IQT Prerequisites. The Cyber Unit's Training OIC must ensure each cybercrew member complies with the appropriate formal course training prerequisites prescribed in the applicable syllabus, before entering qualification training **(T-2)**.

2.3. **Mission Qualification Training (MQT).** MQT prepares an individual for a successful formal evaluation. It focuses on filling training requirements not met at IQT, mastering local procedures, and increasing proficiency as needed. MQT ensures a smooth transition from IQT to MR/CMR status.

2.3.1. Method. MQT is comprised of training at a Formal Training Unit (FTU), if applicable, and local training at the unit. Units determine MQT requirements IAW lead MAJCOM policy and guidance. Cybercrew members participating in in-unit MQT are dedicated to that training, which takes priority over non-training related duties. ***EXCEPTION:*** Supervisory personnel may continue their normal duties as time permits.

2.3.2. MQT Prerequisites. Each cybercrew member must complete all applicable IQT requirements IAW para 2.2 before entering MQT **(T-2)**.

2.3.3. Time Limits. Training time limitations for MQT completion are contained in applicable lead MAJCOM-provided guidance. The AF member will begin In-unit MQT no later than 45 days (90 days for the Active Reserve Component) after reporting to a new duty station or unit, unless waived by the MAJCOM cybercrew training function **(T-2)**.

2.4. **Requalification Training.** A cybercrew member is considered unqualified upon loss of currency exceeding 6 months, expiration of his or her qualification evaluation, or completion of a qualification evaluation in a different weapon system (unless multiple qualification has been approved prior to the evaluation), whichever occurs first. The duration of unqualified time is measured from the date the cybercrew member became unqualified until the specific retraining start date. An unqualified cybercrew member can requalify IAW the following:

2.4.1. Loss of currency 6-12 months: Completion of training in all delinquent items (as applicable), additional training as directed by the certifying official and a requalification evaluation IAW AFI 10-1703 Volume 2.

2.4.2. Loss of currency exceeding 12 months: Recompletion of MQT and a requalification evaluation IAW AFI 10-1703 Volume 2.

2.4.3. Expiration of qualification evaluation not exceeding 6 months: Completion of training in all delinquent items (as applicable), additional training as directed by the certifying official, and a requalification evaluation AFI 10-1703 Volume 2.

2.4.4. Expiration of qualification evaluation exceeding 6 months: Recompletion of MQT and a requalification evaluation IAW AFI 10-1703 Volume 2.

3. Continuation Training (CT). Training that provides crew members with the volume, frequency, and mix of training necessary to maintain proficiency in the assigned position and at the designated certification/qualification level. This training is identified within the respective lead MAJCOM-provided guidance.

3.1. **Currency.** Currency requirements for cybercrew members are identified within the respective lead MAJCOM-provided guidance.

3.2. **Recurrency Training**. A cybercrew member is considered not current upon loss of currency as specified in the applicable lead MAJCOM-provided guidance. If currency is lost for up to six months, the cybercrew member must demonstrate proficiency with an instructor in all delinquent items **(T-2)**.

3.3. **Responsibilities.**

3.3.1. Squadron Commander. The squadron commander or designated representative will ensure individuals receive training to successfully attain/maintain required certifications/qualifications, complete unit missions and maintain individual proficiency **(T-2)**.

3.3.2. Cybercrew Members. Each cybercrew member is responsible for monitoring and completing all training requirements.

3.4. Failure to Complete Continuation Training Requirements.

3.4.1. Report individuals in Status of Resources and Training System (SORTS) IAW AFI 10-201, *Status of Resources and Training System (SORTS)*, and/or IAW lead MAJCOM-provided guidance.

3.4.2. The training supervisors must ensure Individuals who fail to accomplish minimum CT requirements and subsequently lose currency are in a supervised status as specified in lead MAJCOM-provided guidance **(T-2)**.

3.4.3. The training supervisor will document decisions to suspend, retain, or downgrade a cybercrew member's status if the individual fails to meet the standards established by this AFI, AFI 10-1703, Volume 2, or lead MAJCOM-provided guidance, citing all which apply **(T-2)**.

4. Upgrade Training. Training needed to qualify to a cybercrew position of additional responsibility for a specific weapon system (e.g., from a crew member to a crew commander). See applicable lead MAJCOM-provided guidance for applicable positions, instructions, and additional requirements.

5. Multiple Qualification.

5.1. MAJCOMs may authorize qualification in more than one weapon system for crewmembers only when such action is directed by command mission requirements and is economically justifiable. This authority cannot be delegated below the MAJCOM level, except for the Lead MAJCOM, which may further delegate within its command, but not lower than wing commander.

5.2. Restriction on multiple qualification in para 5.1 does not apply to cybercrew members selected for reassignment to another weapon system who attend training prior to PCS.

6. Instructor Training and Certification. Instructors will complete appropriate training program and certification requirements, as specified in the appropriate lead MAJCOM-provided guidance **(T-2)**. Instructor trainees will be observed and supervised by the Chief of Training (or equivalent or their designee) **(T-2)**. Instructors will be current and certified in any task they instruct **(T-2)**. Supervisors will ensure that Instructor training consists of, at a minimum:

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

6.2. Instructional System Development (ISD) process and procedures **(T-2)**.

6.3. Construction, conduct, and administration of classroom training as appropriate for the weapon system **(T-2)**.

6.4. Construction, conduct, and administration of simulator, ops floor, and field training as appropriate for the weapon system **(T-2)**.

6.5. Observance, at a minimum, of one certified instructor conducting training in the classroom, in the simulator, on the ops floor, and in the field, as appropriate for the weapon system **(T-2)**.

7. Cybercrews Operating on Non-US Air Force Weapon Systems and/or with Non-US Air Force Units. Air Force cybercrews performing appropriate duties on non-US Air Force systems, or on duty with or attached to non-US Air Force units for cyber operations, are only required to maintain their training records.

8. Documentation.

8.1. Cybercrew member training events are documented on the Air Force Form 4419, *Record of Training* **(T-2)**. Software applications capturing the same information are authorized provided they comply with lead MAJCOM-provided policy and guidance **(T-2)**.

8.2. Cybercrew member CT and additional training events are maintained in an Individual Qualification Folder (IQF). Electronic format IQFs are authorized provided proper security measures, backup capability, and sustainment plans are in place.

8.3. Dispose of IQFs and other related material according to the AF Records Disposition Schedule (RDS), and AF guidance concerning the protection of Personally Identifiable Information.

BURTON M. FIELD, Lt Gen, USAF
DCS Operations, Plans & Requirements

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFDD 3-12, *Cyber Operations*, 15 July 2010, with change 1, 30 November 2011

AF Doctrine Annex 3-12, Cyberspace Operations, 15 July 2010, with change 1, 30 November 2011

AFPD 10-17, *Cyberspace Operations*, 31 July 2012

AFPD 10-9, Lead Command Designation and Responsibilities for Weapon Systems, 8 May 2007

AFI 10-201, *Status of Resources and Training System (SORTS)*, 13 April 2006

AFI 10-201, Status of Resources and Training System (SORTS), 19 April 2013

AFI 14-2, *Intelligence Rules and Procedures*, 29 November 2007

AFI 33-150, *Management of Cyberspace Support Activities,* 30 November 2011.

AFI 36-2201, *Air Force Training Program*, 15 September 2010

AFI 36-2235, Volume 1, *Information for Designers of Instructional Systems - ISD Executive Summary for Commanders and Managers*, 2 September 2002

AFMAN 33-363, *Management of Records*, 1 March 2008

AFMAN 36-2234, Instructional Systems Development, 1 November 1993

Privacy Act of 1974 (5 United States Code [U.S.C.] 552a)

Privacy Act of 1974 (5 United States Code [U.S.C.] 552a)

Prescribed Forms

AF Form 4419, *Record of Training*.

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFSC—Air Force Specialty Code

ANG—Air National Guard

ARC—Air Reserve Component (AFRC and ANG)

BCQ—Basic Cyber Qualified

BMC—Basic Mission Capable

CMR—Combat Mission Ready

CONOPS—Concept of Operations

CT—Continuation Training

CTP—Cybercrew Training Program

ETCA—Education and Training Course Announcement

FCR—Formal Course Review

FTU—Formal Training Unit

FYDP—Future Years Defense Program

IQF—Individual Qualification Folder

IQT—Initial Qualification Training

ISR—Intelligence, Surveillance, and Reconnaissance

MAJCOM—Major Command

MET—Mission Essential Tasks

MQT—Mission Qualification Training

MR—Mission Ready

NAF—Numbered Air Force

PGL—Program Guidance Letter

PR—Progress Review

PRD—Program Requirements Document

SORTS—Status of Resources and Training System

Terms

(UPDATED) Instructional System Development (ISD)— Instructional system development is a deliberate and orderly, but flexible process for planning, developing, implementing, and managing instructional systems. It ensures that personnel are taught in a cost-efficient way the knowledge, skills, and attitudes essential for successful job performance. (AFMAN 36-2234)

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

Basic Mission Capable— A cybercrew member who has satisfactorily completed IQT and MQT, but is not in fully-certified MR/CMR status. The cybercrew member must be able to attain MR/CMR status to meet operational taskings as specified in the applicable instructional supplements. This status is primarily for individuals in units that perform weapon system-specific operational support functions (i.e., formal training units, operational test and tactics development). BMC requirements will be identified in the appropriate lead MAJCOM-provided guidance.

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

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

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

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

Cybercrew Members— Cybercrew members consist of individuals who conduct cyberspace operations or computer network exploitation and are typically assigned to a specific weapon system.

Cyber (adj.)— Of or pertaining to the cyberspace environment, capabilities, plans, or operations.

Cyberspace— A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02)

Cyberspace Operations— The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (Joint Pub 3-12)

Cyberspace Support— Foundational, continuous or responsive operations in order to ensure information integrity and availability in, through, or from Air Force-controlled infrastructure and its interconnected analog and digital portion of the battlespace. (AFPD 10-17)

Initial Qualification Training (IQT)— One or more courses covering system specific and/or positional specific training as a prerequisite to Mission Qualification Training (MQT).

Instructional System Development (ISD)— A systematic, flexible, proven process for determining whether instruction is necessary in a given situation, for defining what instruction is needed, and for ensuring development of effective, cost-efficient instruction. (AFI 36-2235, Volume 1)

Instructor— An experienced individual qualified to instruct other individuals in mission area academics and positional duties. Instructors will be qualified appropriately to the level of the training they provide.

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

Mission Qualification Training (MQT)— Training needed to qualify for cybercrew duties in an assigned crew position for a specific weapon system.

Requalification Training— Academic and positional training required to requalify to MR/CMR status.

Time Periods— The following definitions are provided for interpretation of timing requirements specified in this instruction:

Day— Unless otherwise specified, "day" means calendar days. When “work days” are specified, count only duty days. Do not count scheduled unit "down" days against this time limit.

Month— The term "month" means calendar months, not 30-day periods.

Unqualified— Previously CMR crewmembers whose CMR status has lapsed due to any of the reasons contained in paragraph 2.4.

Attachment 2

TRAINING DEVELOPMENT

A2.1. Training development: Will define the special set of skills required for mission accomplishment **(T-2)**. Applicable published training standards establish the minimum training task performance standards required and provide constraints for all performance scenarios. These will include all tasks/subtasks, along with associated performance standards, conditions, proficiency codes and applicable timing requirements **(T-2)**. For standardization levels see AFI 10-1703v2, *Cyberspace Operations Standardization and Evaluation (Stan/Eval) Program*.

A2.1.1. Tasks Standard Level Descriptions. Three task standard levels will be used for each task: A, B, and C **(T-2)**. All tasks/subtasks will be documented in a comprehensive task/sub-task list developed by the units, approved by the NAF, and coordinated through Lead MAJCOM/A3T **(T-2)**.

A2.1.2. Level A/Critical task/sub-task. Critical tasks are tasks that could result in mission failure, endangerment of human life, serious injury or death. Critical tasks have the greatest potential for extreme mission or personnel impacts and drive the most stringent training and evaluation program requirements. Critical tasks 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.

A2.1.3. Level B/Essential task/sub-task. Essential tasks are tasks deemed integral to the performance of other tasks and required to sustain acceptable weapon system operations and mission execution. Essential tasks drive significant training requirements.

A2.1.4. Level C/Non-Essential task/sub-task. Non-Essential tasks are rudimentary or simple tasks related to weapons system operations that by themselves have little or no impact on mission execution. Non-Essential tasks require the least stringent training requirements.

A2.1.5. Ensure the requirements contain detailed givens/constraints, performance, and standards for all critical tasks/subtasks (T-2).

A2.2. Use the sample Task/Subtask List: and task requirements tables on the next pages as examples only.

A2.3. Table A. 2.1 is an example only. CCC is cyber crew commander, CA is Cyber Analyst, and CO is Cyber Operator.

Table A2.1. (Sample) Task/Subtask List

		33NWS						92IOS		
AREA & TASK ***SUB-TASK***	DESCRIPTION	**Level**	**CCC**	**COC**	**CO**	**CA**	**COT**	**Level**	**CCC**	**CA**
	MISSION SUPPORT OPERATIONS									
A01	**Perform Crew Actions**									
A01A	Perform Crew Changeover/Shift Actions	C	3c	3c	3b	1b	1b			
A01B	Perform Status of Manning Actions	B	3c	3c						
A01C	Log Operational Activities	B	3c	3c	3c	3c	3c			
A02	**Pre Mission Activities**									
A02A	Perform Tasking Coordination Activities							B	3c	
A02B	Perform Personnel Assignment Activities							B	3c	
A02C	Perform Equipment Preparation Activities							B	3c	3c
A02D	Perform Site Survey Activities							B	3c	3c
A02E	Perform Assessment Plan Activities							B	3c	3c
A02F	Perform Team Pre-Mission Activities							B	3c	3c
A03	**Post Mission Activities**									
A03A	Perform Reporting Activities							B	3c	3c
A03B	Perform Data Archival Activities							B	3c	3c
A03C	Perform Hot Wash Activities							B	3c	3c
A03D	Perform Equipment Return Activities							B	3c	3c
	STATUS MONITORING									
B01	**Perform Fault/Anomaly Resolution Procedures**									
B01A	Perform Mission System Outage Procedures	**A**	**3c**	**3c**	3c	3c	3c			
B01B	Perform Facility System Outage Procedures	A	3c	3c	3c	3c	3c			

		33NWS						92IOS		
AREA & TASK ***SUB-TASK***	DESCRIPTION	**Level**	**CCC**	**COC**	**CO**	**CA**	**COT**	**Level**	**CCC**	**CA**
B01C	Perform Sensor Outage Reporting	B					3c			
B02	**Monitor Communication Channels**									
B02A	Manage Internal Communication	B	3c	3c	2c	1b	3c			
B02B	Manage External Communication	B	3c	3c	2c	1b	3c			
	MISSION PROCEDURES									
C01	**Perform INFOCON Procedures**	B	3c	3c						
C02	**Perform In-Brief Activities**							B	3c	
C03	**Perform Equipment Setup Activities**							B	2b	3c
C04	**Perform Collection Activities**							B	2b	3c
C05	**Perform Analysis and Validation Activities**							B	2b	3c
C06	**Perform Daily Reporting Activities**							B	3c	3c
C07	**Perform Non-Technical Assessment Activities**							B	2b	3c
C08	**Perform Equipment Breakdown Activities**							B	2b	3c
C09	**Perform Out-Brief Activities**							B	3c	
C10	**Perform Platform Operations (PO)**									
C10A	Perform ArcSight Console Operations	B	2c	2c	3c	3c				
C10B	Perform Sensor Operations	B	2c	2c	3c	3c				
C10C	Apply Sensor Signature Update	B					3c			
C11	**Perform Analyst Operations**									
C11A	Perform Channel Monitoring	A	1c	1c	3c	3c				
C11B	Perform Basic Event Analysis	A	1c	1c	3c	3c				

		33NWS						92IOS		
AREA & TASK ***SUB-TASK***	DESCRIPTION	**Level**	**CCC**	**COC**	**CO**	**CA**	**COT**	**Level**	**CCC**	**CA**
C11C	Perform Packet Retrieval	A	1c	1c	3c	3c				
C11D	Perform Packet Analysis	A	1c	1c	3c	3c				
C11E	Perform IP Blocking	B	2d	2d	3c	3c				
C11F	Perform Event Categorization	B	3d	3d	3c	3c				
C11G	Coordinate / Deconflict External Assessments	B	3c	3c	3c	2c				
C11H	Perform Advanced WireShark Operation	B	1c	1c	3c	3c				
C12	**Apply Network Security Principles (NS)**									
C12A	Identify Network Protocols	C	2c	2c	3c	3c				
C12B	Identify Network Security Threats	C	2c	2c	3c	3c				
C12C	Resolution Tools	C	2c	2c	3c	3c				
C13	**Execute Contingency Operations**									
C13A	Execute Continuity of Operations Plan (COOP)	B	3d	3d	3c	3c	3c			
C13B	Transition to Alternate Operating Location (AOL)	A	3d	3d	3c	3c	3c			
C14	**Utilize Reporting Tools / Procedures**									
C14A	Open and Edit ArcSight Cases	B	2c	2c	3c	3c				
C14B	Annotate Events	B	2c	2c	3c	3c				
C14C	Operate historical information database	B	3c	3c	3c	3c				
C14D	Event Investigation Handling	A	3c	3c	3c					
C14E	Incident Handling	A	3c	3c	3c					
C14F	Coordinate TCNO/C4NOTAM	B	3c	3c			3c			
C14G	Coordinate OPREP 3 Information Requirements	B	3c	3c				B		3c
C14H	Coordinate Reporting Products	B	3c	3c						
C14I	Conduct Online Collaborative Sessions	B	3c	3c						

		33NWS						92IOS		
AREA & TASK ***SUB-TASK***	DESCRIPTION	**Level**	**CCC**	**COC**	**CO**	**CA**	**COT**	**Level**	**CCC**	**CA**
	EMERGENCY PROCEDURES									
E01	Perform Emergency/Safety/Security/ Contingency Procedures									
E01A	Perform Fire Procedures	A	3c	3c	3c	3c	3c	C	3c	3c
E01B	Perform Bomb Threat Procedures	A	3c	3c	3c	3c	3c	C	3c	3c
E01C	Perform Accident/Injury/Illness Procedures	A	3c	3c	3c	3c	3c	C	3c	3c
E01D	Perform Severe Weather/Natural Disaster Procedures	A	3c	3c	3c	3c	3c	C	3c	3c
E01E	Perform Total Evacuation Procedures	A	3c	3c	3c	3c	3c	C	3c	3c
E01F	Perform Missing Crewmember Procedures	B	3c	3c	3c	3c	3c			