DEPARTMENT OF THE AIR FORCE
Headquarters US Air Force
Washington, DC 20330-1030

CFETP 17X
Parts I and II
01 June 2015

AFSC 17X
CYBERSPACE OPERATIONS OFFICER


Basic


Senior


Master

CAREER FIELD EDUCATION AND TRAINING PLAN

ACCESSIBILITY: Publications and forms are available on the e-publishing web site at www.e-publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

AFSC 17X

CAREER FIELD EDUCATION AND TRAINING PLAN

TABLE OF CONTENTS

PART I

PART II

OPR: 333 TRS/TRR
Approved by: Lt Col Stephen Bailey, AFCFM SAF/A6SF
Supersedes CFETP 17X, dated 20 June 2014
Pages: 75

CYBERSPACE OPERATIONS

AFSC 17X
CAREER FIELD EDUCATION AND TRAINING PLAN

PART I

Preface

1. This Career Field Education and Training Plan (CFETP) is a comprehensive education and training document that identifies life-cycle education and training, training support resources and initial qualification requirements for the Cyberspace Operations officer career field. These initial and follow-on requirements were developed to educate and train the Cyberspace Operators, provide a career path to success and document all aspects of career field training.

2. The CFETP consists of two parts; both parts of the plan are used by officers, supervisors and commanders to plan, organize, lead, and control training within the Cyberspace Operations career field.

2.1. Part I provides information necessary for overall management of the specialty. Section A provides general information about the CFETP; Section B identifies duties and responsibilities, career field progression information, training decisions and career field path; Section C associates each Air Force Specialty (AFS) skill level with specialty qualifications (knowledge, education and training); and Section D addresses resource constraints.

2.2. Part II shows options available to meet an officer's education and training needs. Section A identifies the training students receive in a specific course. Section B identifies training courses including mandatory AF in-residence, field, exportable and online courses. Section C and Section D are reserved at this time.

3. This CFETP serves as the foundational document that will ensure individuals in the Cyberspace Operations Officer specialty receive effective and efficient training at the appropriate points in their career. This plan will enable those in the Cyberspace Operations career field to train today's 17X officers to a variety of opportunities across the spectrum of cyberspace operations.

NOTE: Civilians occupying equivalent positions may use the Specialty Training Standard in Part II Section B for their duty position qualification training.

Abbreviations/Terms Explained

Advanced Distributed Learning (ADL). Evolution of distributed learning (distance learning) that emphasizes collaboration on standards-based versions of reusable objects, networks, and learning management systems, yet may include some legacy methods and media. ADL leverages the full power of computers, information, and communication technologies through the use of common standards in order to provide synchronous or asynchronous learning that can be tailored to individual needs and delivered anywhere-anytime. ADL also includes establishing an interoperable "computer managed instruction" environment that supports the needs of developers, learners, instructors, administrators, managers, and family. ADL encompasses all the methodologies mentioned above, and in addition, includes ongoing and expected improvements in learning methods.

Air Force Career Field Manager (AFCFM). AF focal point for the Cyberspace Operations career field. Serves as the primary advocate for the career field, addressing issues and coordinating functional concerns across various staffs. Designated individual and office responsible for developing and sustaining career field resources and is also responsible for the career field policy and guidance. Must be appointed by the FM and hold the grade of Colonel/GS 15 (or equivalent) for officer and DAF civilian specialties.

Air Force Specialty (AFS). A basic grouping of positions requiring similar skills and qualifications.

Career Field Education and Training Plan (CFETP). A comprehensive core training document that identifies life-cycle education and training requirements, training support resources, and minimum core task requirements for a specialty. The CFETP aims to give personnel a clear path and instill a sense of industry in career field training.

Career Training Guide (CTG). Subsection of the CFETP used to identify tasks or capabilities expected of a career field. It is intended to serve as a guide of tasks, knowledge and concepts that applicable career field personnel should strive to develop throughout their careers.

Competencies. The observable or measurable knowledge, skills, abilities, behaviors, and other characteristics needed to perform a type or work or function.

Computer Based Training (CBT). A method for training whereby the student learns via a computer terminal. It is an especially effective training tool that allows students to practice applications while learning.

Continuum of Learning (CoL). Career-long process of individual development where challenging experiences are combined with education and training through a common taxonomy to produce Airmen who possess the tactical expertise, operational competence, and strategic vision to lead and execute the full spectrum of Air Force missions.

Core Tasks. Tasks the Air Force Career Field Managers identify as minimum qualification requirements for everyone within an AFSC, regardless of duty position. Core tasks may be specified for a particular skill level or in general across the AFSC.

Course Training Standard (CTS). Training standard that identifies the course material and the level of training members will receive in a specific course. The CTS serves as the career field's contract with the schoolhouse.

Cyberspace Operations (CO). The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0; JP 1-02)

Cyberspace Operations Functional Authority (FA). The Functional Authority appointed by the Secretary of the Air Force for the deliberate development, management and advancement of the Cyberspace operations Career field.

Development Team (DT). Provide oversight of officer and civilian personnel development to meet both functional and Air Force corporate leadership requirements.

Distributed Learning. Structured asynchronous learning mediated with technology that does not require the physical presence of the instructor. Distributed learning models can be used in combination with other forms of instruction or it can be used to create wholly virtual classrooms.

Education and Training Course Announcement (ETCA). Contains specific MAJCOM procedures, fund cite instructions, reporting instructions, and listings for those formal courses conducted or managed by the MAJCOMs or field operating agencies (FOAs). The ETCA contains courses conducted or administered by the AF and reserve forces and serves as a reference for the AF, DoD, other military services, government agencies, and security assistance programs.

Exportable Training. Training provided via computer-assisted, paper-text, interactive video, or other media.

Field Training. Technical, operator and other training that either a field training detachment or mobile training team conducts at operational locations on specific systems and associated direct-support equipment.

Force Development (FD). A deliberate process of preparing Airmen through the CoL with the required competencies to meet the challenges of current and future operating environments. Institutional development generally results in leadership, management, and warrior ethos proficiency.

Functional Competency. Occupational or functional competencies are the knowledge, skills, and abilities related to specific career field duties. Each career field identifies the desired occupational competencies for its members. These competencies are focused on building depth of functional experience.

Functional Manager (FM). Senior leaders, designated by the appropriate FAs, who provide day-to-day management responsibility over specific functional communities. While they should maintain an institutional focus with regard to resource development and distribution, FMs are responsible for ensuring their specialties are equipped, developed, and sustained to provide AF capabilities.

Initial Skills Education and Training. A formal school course that is required for award of the qualified Air Force specialty code. The Undergraduate Cyberspace Training Course functions as the IST for the 17D and 17S AFSCs.

Initial Qualification Training (IQT). IQT is "training performed by the field training unit (FTU) in order to teach safe operation of a specific mission system in an assigned crew position. The culmination of IQT is a declaration of BMC for a specific mission system and position."

Institutional Competencies (ICs). Common taxonomy used to implement the CoL. These leadership competencies are expected of all Airmen, throughout their careers, and will be the competencies needed to operate successfully in the constantly changing environment in which they function.

MAJCOM Functional Manager (MFM). Representative appointed by the MAJCOM who directs the development and coordination of courses and standards for training and educating personnel in a specific career field at the MAJCOM level.

Mission Qualification Training (MQT). MQT follows IQT and is the final qualification training course. It is performed at the assigned operational unit to teach that unit's mission specific training requirements. The culmination of MQT is a declaration of MR/CMR for that unit's mission.

Occupational Competencies. A set of competencies required of all Airmen within a specific workforce category (a group of functions requiring similar work, i.e. Engineering). They describe technical/functional skills, knowledge, abilities, behaviors, and other characteristics needed to perform that function's mission successfully.

Occupational Series (OCSRS). The Office of Personnel Management (OPM) publishes occupational series descriptions and classification guides, used by Civilian Personnel Flights (CPFs) to classify individual position descriptions.

Occupational Analysis Report (OAR). A detailed report showing the results of an occupational survey of tasks performed within a particular AFSC.

On-the-Job Training (OJT). Hands-on, "over-the-shoulder" training conducted to certify personnel in both upgrade (skill level award) and job qualification (position certification training).

Resource Constraints. Resource deficiencies (such as money, facilities, time, manpower and equipment) that preclude desired training from being delivered.

Special Duty Assignment (SDA). A duty assignment outside an individual's primary career field, such as Squadron Officer School instructor.

Special Experience Identifiers (SEI). SEIs complement other classification tools to provide the means to record and retrieve specific experience and training to satisfy management needs.

Specialty Training Requirements Team (STRT). STRTs forums determine Education and Training requirements by bringing together the expertise to establish the most effective mix of formal and on-the-job training for each AFS. STRTs are also used to create or revise training standards and set responsibilities for providing training.

Subject Matter Expertise (SME). Competencies required for employees in one or more occupations within a mission category, depending on a particular specialty or assignment.

Utilization and Training Workshop (U&TW). A forum of the AFCFM, MFMs, subject matter experts (SME), and AETC training personnel that evaluates career field training requirements.

Weapon Systems: The Air Force has seven weapon systems in our inventory. Six of the seven have unclassified descriptions and are briefly described below. For additional information, see the following: http://www.afspc.af.mil/library/factsheets/index.asp

1) Cyberspace Defense Analysis (CDA): The Air Force Cyberspace Defense Analysis (CDA) weapon system conducts Defensive Cyberspace Operations by monitoring, collecting, analyzing, and reporting on sensitive information released from friendly unclassified systems, such as computer networks, telephones, email, and USAF websites. CDA is vital to identifying Operations Security (OPSEC) disclosures. The CDA weapon system is operated by three Active Duty units [68 Network Warfare Squadron (NWS), 352 NWS, 352 NWS Det 1] and two Reserve units [860 Network Warfare Flight (NWF) and 960 NWF] located at Joint Base San Antonio Lackland TX, Joint Base Pearl Harbor Hickam Field HI, Ramstein AB GE, Joint Base San Antonio Lackland TX, and Offutt AFB NE, respectively.

2) Cyber Security and Control System (CSCS): The Air Force Cyber Security and Control System (CSCS) weapon system is designed to provide 24/7 network operations and management functions and enable key enterprise services within Air Force unclassified and classified networks. This system also supports defensive operations within those Air Force networks. CSCS is operated by two Active Duty (AD) Network Operations Squadrons (NOS), one Air National Guard (ANG) Network Operations Security Squadron (NOSS) and two Air Force Reserve Command (AFRC) Associate NOSs aligned with the AD squadrons. The 83 NOS (AD) and 860 NOS (Reserve) are located at Langley AFB VA; the 561 NOS (AD) and 960 NOS (Reserve) are located at Peterson AFB CO; and the 299 NOSS (ANG) is located at McConnell AFB KS.

3) Air Force Intranet Control (AFINC): The Air Force Intranet Control (AFINC) weapon system is the top level boundary and entry point into the Air Force Information Network (AFIN), and controls the flow of all external and interbase traffic through standard, centrally managed gateways. The AFINC weapon system consists of 16 Gateway Suites and two Integrated Management Suites, and is operated by the 26 Network Operations Squadron (26 NOS) located at Gunter Annex, Montgomery, AL.

4) Cyberspace Vulnerability Assessment/Hunter (CVA/Hunt): The Air Force Cyberspace Vulnerability Assessment/Hunter (CVA/Hunter) weapon system executes vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and Hunter missions on AF and DoD networks & systems. Hunter operations characterize and

then eliminate threats for the purpose of mission assurance. The weapon system can perform defensive sorties world-wide via remote or on-site access. The CVA/Hunter weapon system is operated by one Active Duty unit, the 92d Information Operations Squadron (IOS), located at Joint Base San Antonio Lackland TX, and one Guard unit, the 262d Network Warfare Squadron (NWS), located at Joint Base LM McChord WA. There are two Guard units in the process of converting to this mission, the 143d IOS and the 261st NWS, located at Camp Murray WA, and Sepulveda ANGS CA, respectively.

5) Cyber Command and Control Mission System (C3MS): The U.S. Air Force has mastered the ability to apply global reach, power and vigilance across the domains of air and space. The AF applies these same precepts in the cyberspace domain as part of its mission to fly, fight, and win in air, space and cyberspace. The Cyber Command and Control Mission System (C3MS) weapon system enables this mission by synchronizing other AF cyber weapon systems to produce operational level effects in support of Combatant Commanders worldwide. C3MS provides operational level Command and Control (C2) and Situational Awareness (SA) of AF cyber forces, networks and mission systems. C3MS enables the 24th Air Force Commander (24 AF/CC) to develop and disseminate cyber strategies and plans, then execute and assess these plans in support of AF and Joint warfighters. The C3MS weapon system is operated by the 854th Combat Operations Squadron for the 624th Operations Center (624 OC) at Joint Base San Antonio Lackland TX.

6) Air Force Cyberspace Defense (ACD): The Air Force Cyberspace Defense (ACD) weapon system is designed to prevent, detect, respond to, and provide forensics of intrusions into unclassified and classified networks. This weapon system supports the AF Computer Emergency Response Team in fulfilling their responsibilities. ACD is operated by the 33d Network Warfare Squadron (NWS) located at Joint Base San Antonio Lackland TX, the Air Force Reserve's 426th NWS located at Joint Base San Antonio Lackland TX and the Air National Guard's (ANG) 102d NWS located at Quonset ANGB RI.

Section A - General Information

1. Purpose of the CFETP. The CFETP provides the information necessary for AFCFM, MFMs, commanders, directors, training managers, supervisors and trainers to plan, develop, manage and conduct an effective and efficient career field training program. The plan outlines the training individuals in this AFS should receive to support their professional development and defines the competencies necessary to progress throughout their careers. For purposes of this plan, training is divided into initial and advanced skills training; supplemental training; and continuing education. Initial skills training is mandatory for award of the AFSC. Continuing education is acquired through advanced degrees, commercially procured training, on-the-job training and specialized training as required by MAJCOM or units.

2. Use of the CFETP. The plan will be used by MFMs and supervisors at all levels to ensure comprehensive and cohesive training programs are available for each individual in the specialty.

2.1. AETC training personnel will develop and revise formal resident, non-resident, field and exportable training based upon requirements established by the users and documented in Part II of the CFETP. They will also work with the AFCFM to develop acquisition strategies for obtaining resources needed to provide the identified training.

2.2. MFMs will ensure their training programs complement the CFETP. Identified requirements can be satisfied by OJT, resident training, and contracted training or exportable courses.

2.3. Each new 17X officer will complete the mandatory training requirements specified in the Career Training Guide (Part II, Section C) prior to awarding of the 17X1X AFSC. The list of courses in Part II, Section C will be used as a reference to support training.

3. Coordination and Approval. The Functional Authority for Cyberspace Operations, is the approval authority for the CFETP and will initiate a review of this document annually to ensure currency and accuracy. The Functional Authority will assess whether the AFS has undergone any mission or role related changes, and as a result, if a U&TW is necessary. The Cyberspace Operations Career Field Manager, MAJCOM Functional Managers and AETC training personnel will identify, develop and coordinate on the career field training requirements submitted to the Functional Authority.

Section B - Career Progression and Information

1. Cyberspace Operations Specialty Description. Executes cyberspace operations and information operations functions and activities. Plans, organizes, directs and executes cyberspace and information operations such as, Defensive Cyber Operations (DCO), Offensive Cyber Operations (OCO), Department of Defense (DoD) Information Network (DoDIN) Operations and Mission Assurance for Air Force weapons systems and platforms. Such operations cover the spectrum of mission areas within the cyberspace domain.

1.1. Duties and Responsibilities:

1.1.1. Plans and prepares for mission. Reviews mission tasking and intelligence information. Supervises mission planning, preparation and crew briefing/debriefing. Ensures equipment and crew are mission ready prior to execution/deployment.

1.1.2. Operates weapons system(s) and commands crew. Performs, supervises, or directs weapons system employment and associated crew activities.

1.1.3. Conducts or supervises training of crewmembers. Ensures operational readiness of crew by conducting or supervising mission specific training.

1.1.4. Develops plans and policies, monitors operations, and advises commanders. Assists commanders and performs staff functions related to this specialty.

1.1.5. Translates operational requirements into architectural and technical solutions. Works with commanders to deliver complete capabilities that include technical and procedural components. Researches or oversees research of technologies and advises commanders on associated risks and mitigation factors in conjunction with meeting requirements.

1.1.6. Directs extension, employment, reconfiguration, adaptation and creation of portions of cyberspace to assure mission success for combatant commanders. This includes both deliberate and crisis action scenarios.

2. Skill and Career Progression.

2.1. Adequate training and timely progression from the entry to the qualified level play an important role in the AF's ability to accomplish its mission. It is essential that everyone involved in training does his or her part to plan, manage, and conduct an effective training program. Section C of this CFETP expands upon the following overview.

2.1.1. Entry (17D1 and 17S1) Level. For entry into this specialty, an officer must meet the mandatory requirements listed in the specialty description in the 17D or 17S AFSC Air Force Officer Classification Directory (AFOCD).

2.1.2. Initial (17D2 and 17S2) Level. Upon completion of UCT member will be awarded AFSC 17D2 or 17S2 as applicable. Graduation from UCT meets career field Initial Qualification Training (IQT) standard.

2.1.3. Qualified (17D3 and 17S3) Level. For award of AFSC 17D3 and 17S3, officers must meet mission specific Mission Qualification Training (MQT) standards as identified by their Commander, MAJCOM and Desired Operational Capability Statements. Commanders will develop and document MQT requirements in On-The-Job and Job Qualification Standards. Commanders will certify MQT attainment.

2.1.4. Staff Level (17X4). Education and training requirements for this level are the same as the Qualified Level (17X3). Officer must be appointed to a staff position at the MAJCOM, Numbered Air Force, Field Operating Agency, Headquarters Air Staff, or Combatant Command to achieve the Staff Level.

2.2. Education. For Education requirements reference Part I, Section C or the AFOCD.

2.3. Training. For Training requirements reference Part I, Section C or the AFOCD.

2.4. Professional Development. To experience the full breadth of opportunities in sufficient depth normally requires a variety of assignments. Successful professional development is essential for those who will eventually hold top leadership positions in the Air Force. A balanced approach to professional development will produce officers with relevant technical expertise, diverse command experience, an ability to apply the tenets of air, space, and cyberspace doctrine and a record of performance and assignments that validates these credentials. Professional development requires the following:

2.4.1. Maintaining a balanced approach in tours of duty (i.e., CONUS, overseas, joint, unit-level, agencies and headquarters), positions (i.e., instructor, commander, crew, and action officer), specialization (i.e., network operations, fixed communications, deployable communications, space operations, information operations, and cyber operations) and disciplines (i.e., logistics, operations, intelligence, and acquisitions) as well as diversity of experience across the spectrum of cyber operations.

2.4.2. Completing professional military education, relevant advanced academic degree and supplemental and continuing technical training and education to include Professional Continuing Education in Cyber 200, 300 and 400 courses.

2.4.3. Role of the Commander, Supervisor and Senior 17X officers in Professional Development.

2.4.3.1. Commanders, supervisors and senior cyberspace operations officers must take an active role in officer professional development. The 17X career pyramid shown in Figure 1 is available to facilitate this discussion. Officers should review career goals with their commander, supervisor, and/or senior cyberspace operations officer at least annually. Junior officers should use the results of these discussions to formulate input to their Airman Development Plans (ADP). ADPs should be reviewed and updated annually in order to ensure the Air Force Personnel Center is aware of an officer's professional development goals and opportunities sought.

2.4.3.2. Cyberspace Operations officers whose supervisors are not in their career field, have the option of seeking out a senior Cyberspace Operations officer for mentoring.

3. Training Decisions.

3.1. The following decision was made at the Cyberspace Operations U&TW in April 2013.

3.1.1. Complete a major course revision of the Undergraduate Cyber Training (Phase 1 and 2). The reason for the change is to reduce the amount of wash backs and eliminations. The realigned course flow places the heavy technical blocks of instruction together eliminating the pendulum swing between non-technical and technical blocks.

3.1.2. The career field identified the need for increased cyberspace training for all cyberspace operations officers. The training needed is currently being taught by the 39th IOS in INWT, but is not currently a part of IQT. As a result, a decision was made to investigate incorporating the pre IQT training from INWT into UCT Phase 3.

3.1.3. A strategic decision was made to change the focus of Scope Eagle to a more strategic based training course and align it with the current Cyber 200 and Cyber 300 continuum. As a result, SAF A6 staff working with the 333rd TRS staff developed Cyber 400.

4. Career Development

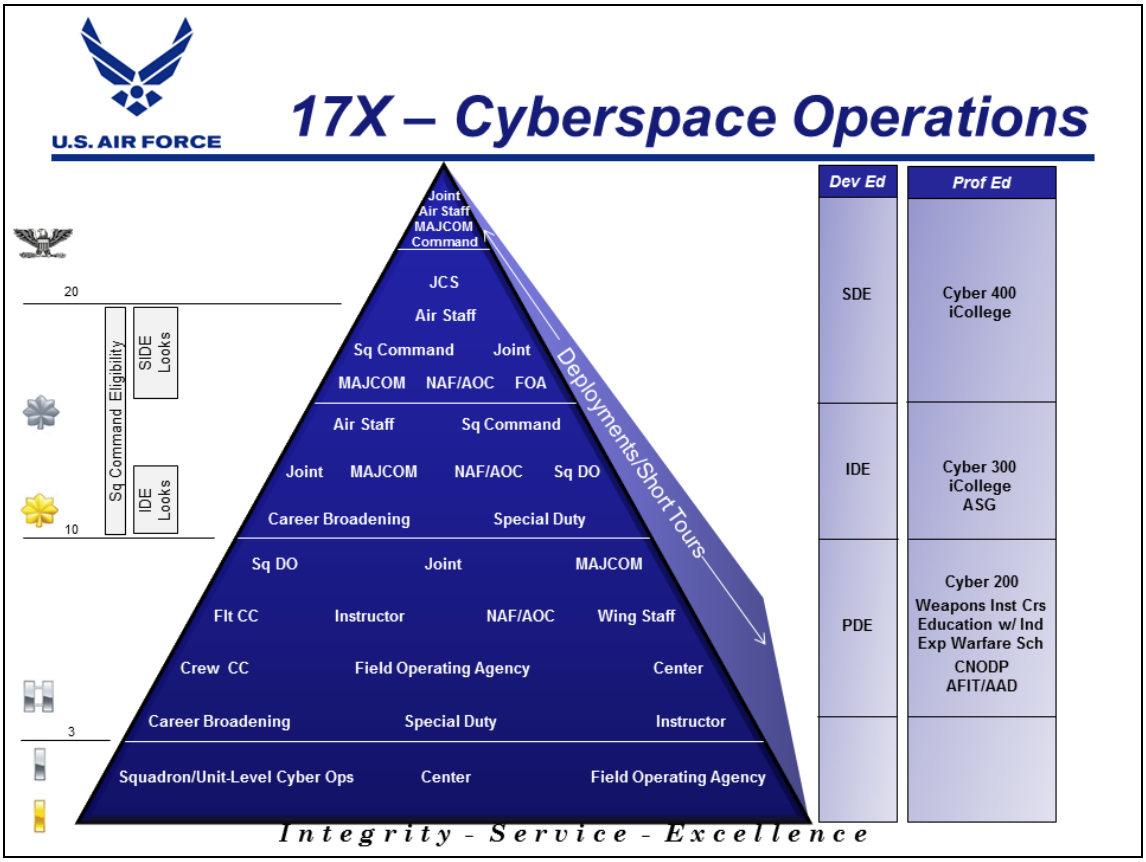

Figure 1. 17X Career Field Pyramid

4.1. Career Field Pyramid. The Cyberspace Operations Officer Career Path Pyramid shows progression through a variety of jobs. This pyramid should be used as a planning guide by commanders, supervisors, and individuals in conjunction with other planning tools, to include AFI 36-2110, and senior cyberspace operations officer advice. Early on, officers should develop a solid technical and operational experience base and continually focus on gaining depth and breadth as their careers progress. We must build a force of competent, agile, and aggressive cyberspace operators able to apply their skills in an operational environment and articulate the effects cyberspace capabilities have on the AF mission in operational (vs technical) terms. Cyber 200 and Cyber 300 are required professional military courses that are career specific.

4.2. Every assignment and all assignment advice given must reflect this philosophy. 17X officers must know and fully understand all of our cyberspace capabilities and limitations. They must be able to operate in any environment, perform a variety of cyberspace-related jobs, and understand all aspects of operations.

4.3. Depth and Breadth. A company grade officer should develop depth early in his/her career with appropriate level assignments. Officers need to understand the technical application of the mission systems they man, how they fit into the Air Force, Joint, National and Combatant Commander Missions and how they interoperate or exchange information/data with Sister Service Mission Systems to achieve a Combatant Commander task. Subsequently, officers will

gradually broaden their baseline both within and outside of the cyberspace operations career field through career breadth and career broadening tours.

4.4. Ultimately, an individual's career path will be influenced by his/her personal aspirations and the needs of the Air Force. Ideally, officers will gain depth in the first 10 years of their career and assume more strategic positions as they mature through field grade ranks.

4.5. Assignments should prepare cyberspace operations officers for command and leadership positions within the Air Force, Joint Commands and the cyber community. The keys to success are breadth of experience, depth of knowledge, and high quality performance at every job level.

4.6. Experience Tracking Through Career Path Tool (CPT). In order to more effectively identify key experiences to fill AF and Joint requirements as well as better management of the AF career force, AF/A1 developed an experience coding and tracking system to more readily employ forces called CPT. CPT pulls individual duty histories from MILPDS. CPT is based upon a six digit Airmen Capability Management (ACM) code, where the first three digits consist of the career field AFS (17D or 17S) and the last three are used to categorize roles and experience. The Career Field Manager (CFM) is charged to develop a methodology for the last three digits of the ACMs. Once fully populated, CPT allows AF functional and CFMs the data necessary to monitor and develop the force to the appropriate breadth and depth of experience required for the health of the career field. Additionally, CPT allows the AFPC assignment team and the Cyberspace Operations Development Team (DT) to quickly identify candidates for positions requiring specific experiences and certifications, replacing the time intensive process of delving into hundreds of individual documents (such as performance reports).

4.6.1. Career Path Tool is online and fully functional. If they haven't already, officers must go to the CPT website (https://afvec.langley.af.mil/af-cpt) and register. Once registered, members should view and validate the coding of their duty histories. Officers may correct discrepancies by either updating their duty histories in MILPDS (through the vMPF) or by using the "Report ACM Error" function from the "My Duty History" screen (if the error is related to the coding in CPT).

4.7. Duty Titles. In order to facilitate implementation of the Air Force standardized experience tracking system (Career Path Tool) and mentoring tool (My Vector), a standardized set of duty titles is required. The information will be used in all aspects of an Airmen's career. All cyberspace officers will have standardized duty titles. These duty titles will include a standardized job role followed by a brief descriptor of the position: Job Role, Descriptor. Examples of such are: "Flt/CC, Operations"; "Branch Chief, Cyber Defense"; "Division Chief, C4 Capabilities"

Duty Title	LT	CAPT	MAJ	LTCOL	COL
Action Officer	X	X	X	X	X
Analyst	X	X	X*		
Branch Chief			X	X	
Chief	X	X	X	X*	
CND Manager	X	X	X		
Commander		X	X	X	
CoS				X	X
Crew Commander	X	X	X*		
Cyberspace Operator	X	X	X		
Dep Director				X	X
Dep Div Chief			X	X	
Deputy Branch Chief		X	X	X*	
Deputy Group CC				X	
Director				X	X
Director of Operations		X	X	X	
Division Chief				X	X
DoS				X	X
Element Lead	X	X	X		
Engineer	X	X	X		
Evaluator		X	X	X*	
Exec Officer	X	X	X	X	
Flight/CC	X	X	X		
IMA	X*	X*	X*	X*	X*
Instructor	X	X	X	X	
Lead	X	X	X		
Mission CC		X	X	X*	
OIC	X	X	X	X*	
Programmer	X	X	X*		
Project Manager	X	X	X		
Section Chief	X	X	X		
Student	X	X	X	X	X
Team Lead	X	X	X		
Vice Commander					X
Watch Officer	X	X	X		

* Denotes AFRC and ANG personnel

Table 1. Standardized Duty Titles

Section C - Proficiency Training Requirements

1. Purpose. Proficiency training requirements in this career field are defined in terms of tasks and knowledge requirements. This section outlines the specialty qualification requirements for entry, award and retention of each AFS level. The specific task and knowledge training requirements are identified in the Course Training Standard (CTS), Career Training Guide (CTG), and Training Course Index at Part II, Sections A, B, and C of this CFETP. They are stated in broad, general terms and establish the standards of performance. These training requirements reflect the criteria documented in the Officer Classification Directory (AFOCD).

2. Specialty Qualifications

2.1. Entry Level (17X1)

KNOWLEDGE	Fundamentals of Computer Systems, Operating Systems, Software Applications and Architecture, Protocols, Addressing and Hardware. In addition, an Understanding of Networking Fundamentals, Network Infrastructure, to include Telecommunications Theory, Industrial Control Systems, and Data Communications/Links is needed. Officers must also be Proficient on Wireless Networking, as well as, Data Delivery to Personal Wireless Devices and understand Cryptography; to include Utilization and Exploitation Techniques. Cyberspace Operations and Information Operations Organization, Policies, Directives and Doctrine; Cyberspace Operations Systems and Fundamentals; Requirements, Acquisition, and Logistics; Cyberspace Operations Management, Utilization and Planning Principles.
EDUCATION	For entry into this Specialty, most 17X Officers will possess Computer, Science, Technical, Engineering or Mathematic degrees. See the AFOCD for a complete list of degree programs.
TRAINING	Officers will attend Undergraduate Cyberspace Training (Phase 1 and 2) as soon as possible after being accessed as a 17X1.
EXPERIENCE	No experience requirement.

2.2. Intermediate (17D2)*

KNOWLEDGE	Mission specific and work role requirements.
EDUCATION	No additional education required.
TRAINING	OJT/JQS IQT requirements or graduation from IQT awarding FTU.

2.3. Intermediate (17S2)*

KNOWLEDGE	Mission specific and work role requirements.
EDUCATION	No additional education required.
TRAINING	OJT/JQS IQT requirements or graduation from IQT awarding FTU.

2.4. Qualified (17D3)*

KNOWLEDGE	Mission specific and work role requirements.
EDUCATION	No additional education required.
TRAINING	OJT/JQS MQT requirements.
Initial Award	Initial award of 3 skill level will be NET 12 months from award of AFSC

2.5. Qualified (17S3)*

KNOWLEDGE	Mission specific and work role requirements.
EDUCATION	No additional education required.
TRAINING	OJT/JQS MQT requirements.
Initial Award	Initial award of 3 skill level will be NET 12 months from award of AFSC

2.6. Staff Level (17X4)*

KNOWLEDGE	See Paragraph 2.1. above.
EDUCATION	No additional education required.
TRAINING	Must be 17X3 qualified before filling a 17X4 billet.
Other	Designation of staff level relates only to the level of functional responsibility and is restricted to positions above wing level. It does not denote additional specialty qualifications.

* In accordance with AFI 36-2101, *Classifying Military Personnel (Officer and Enlisted),* Commanders use any of the following source documents to award, upgrade, downgrade, and withdraw Air Force Specialty Codes (AFSC), Special Duty Identifiers (SDI), Reporting Identifiers (RI) and Special Experience Identifiers (SEI): AF Form 2096, Classification/On-the-Job Training Action, Case Management System (CMS) or AFPC generated action, MilPDS generated Report on Individual Person (RIP) or AFPC-generated order. Source documentation is submitted through local MPS and forwarded to AFPC Automated Records Management System (ARMS) shop for scanning into the Airman's digital record.

2.7. Qualification Training.

2.7.1. Initial Qualification Training (IQT). IQT is comprised of one or more courses covering system specific and/or positional specific training as a prerequisite to Mission Qualification Training. Completion of UCT serves as the IQT for the Cyberspace Operations career field. Weapons systems will have their own unique IQT and subsequent MQT progression. Completion of UCT meets the requirement for award of the 17X2X – Qualified IAW AFOCD.

2.7.2. 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. MQT is comprised of training at a Formal Training Unit, if applicable, and

local training at the unit. Units will determine MQT requirements in accordance with Lead MAJCOM policy and guidance. Completion of MQT (unit or weapons system) meets the requirement for award of the 17X3X – Qualified IAW AFOCD.

2.8. DoD 8570 Compliance.

2.8.1. 17D/17S officers will maintain compliance with DoD 8570.01-M. All Cyber Operations Officers will attain and possess a current Information Assurance Management certification in accordance with DoD 8570.01-M. There is no single answer on which certification an officer will attain. Officers should stay abreast of changes in the Directive in order to maintain the appropriate certification. While changes in this effort are being codified in AFMAN 33-285, *Information Assurance (IA) Workforce Improvement Program*, the following guidelines are provided. Refer to AFMAN 33-285 for guidance on preferred certifications.

2.8.2. Company Grade Officers (CGOs). Most CGOs possess Security+ certification based on their attendance at Undergraduate Cyberspace Training. Some will attain additional certifications based on mission assignment or personal initiative. CGOs are tasked to maintain currency in their most advanced Information Assurance Management (IAM) certification.

2.8.3. Field Grade Officers (FGOs). As an officer matures in grade, they are required to lead junior officers who possess IAM certifications. As such, they will be required to attain and maintain currency on the applicable IAM certification. Refer to AFMAN 33-285 for guidance on applicable certifications.

2.8.4. Maintaining Currency. Officers attaining certification with Air Force funding are required to register their certification with the Defense Manpower Data Center (https://www.dmdc.osd.mil/appj/dwp/index.jsp). Once codified in AFMAN 33-285, the Air Force will use the information provide to: 1) verify an officers certification and 2) pay for certification maintenance fees. While an individual may attain multiple certifications over their career, the Air Force will pay maintenance fees for the most advanced certification.

Section D - Resource Constraints

1. Purpose. This section identifies known resource constraints that preclude optimal/desired training from being developed or conducted, including information such as part numbers, national stock numbers, number of units required, cost, manpower, etc. Included are narrative explanations of each resource constraint and an impact statement describing what effect each constraint has on training. Finally, this section includes actions required, OPR and target completion date. Resource constraints will be, at a minimum, reviewed and updated annually.

1.1. Constraints. Funding and budget constraints may influence class size, duration, and ability to meet AF training requirements.

PART II

Section A - Course Training Standard

1. Purpose.

1.1. The Air Force uses the CTS to identify the training students receive in a specific course. It serves as the foundational document which describes the course's content and standard of proficiency each student is expected to achieve in order to successfully complete the course. It's also used as the basis for the Course Resource Estimate (CRE) which describes the human, physical, and fiscal resources required to execute the course. In essence, the CTS is a contract between the Career Field Manager and the training provider, and can only be modified through the Specialty Training Requirements Team (STRT)/U&TW process and AFCFM policy directives. The training tasks are based on an analysis of duties in the AF Officer Classification Directory for 17D and 17S AFSCs as described in the Air Force Education and Training Course Announcements (ETCA) database.

1.1.1. Undergraduate Cyber Training Phase 1 (UCT) CTS. See Attachment 2.

1.1.2. Undergraduate Cyber Training Phase 2 (UCT) CTS. See Attachment 3.

Proficiency Designator	Title	Course Requirements
17X1	Entry Level	Attend Undergraduate Cyber Training
17D2/17S2	Initial	Completion of Initial Qualification Training
17D3/17S3	Qualified	Complete Mission Qualification Training
17X4	Staff Officer	Must be 17X3 (See *Note)

*Note: Designation of staff level relates only to the level of functional responsibility and is restricted to positions above wing level. It does not denote additional specialty qualification. Officer must be a 17X3 before being assigned to a 17X4 position.

Section B - Training Course Index

1. Purpose. This section of the CFETP identifies training courses including mandatory AF in-residence, field, exportable and online courses. For information on all formal courses, refer to the Air Force Education and Training Course Announcements (ETCA) database.

2. Air Force Cyberspace Operations Officer Courses.

Course Number	Course Title
E3OQR17D1 0A1A	Undergraduate Cyber Training Phase 1 (UCT)
E3OBR17D1 OA1A	Undergraduate Cyber Training Phase 2 (UCT)
IOS-INWT 002	Intermediate Network Warfare Training (INWT)
IOS-NWBC 001	Network Warfare Bridge Course (NWBC)
WCYBER200	Cyber 200
WCYBER300	Cyber 300
E3OAR17D4 0A1B	Cyber 400 (formerly Scope Eagle)
E3OZR17D3 0A1A	Cyberspace Officer Engineering
E6OZW17D3 0A5A	Cyberspace Officer Deployable/Tactical Communications
E3OZR17D3 0A3A	Cyberspace Officer Network Training
E6OZW17D3 0A1A	Cyberspace Officer Warfighting Integration Course
E6OZW17D3 0A4A	Enterprise Network Operations
E5OZD82A0 00AA	Joint Command, Control, Communications, Computer (Cyber), and Intelligence Staff and Operations (JC4ISOC)

3. Exportable Courses.

A current list of the available CBT courses is available on the AF e-Learning site which is accessible only through the AF Portal. For example, there are several Program Management online courses available through e-Learning.

4. Additional Training Courses and Resources.

4.1. This section identifies training programs and resources currently available for cyberspace operations officers to further their knowledge of the career field. Professional Continuing Education (PCE) (Cyber 200 and Cyber 300) and technical refresher training are additional education and training options, either in residence, or through exportable courses and on-the-job training. This training is available to personnel to increase their skills and knowledge beyond the minimum required. For further information on available training check the 17D/17S professional development website.

4.2. The Air Force Institute of Technology (AFIT) Graduate School of Engineering and Management located at Wright-Patterson AFB, OH, offers numerous cyberspace related courses. Graduate programs include Cyber Operations, Computer Engineering, Computer Science, Electrical Engineering, and Software Engineering. These are in-residence courses requiring a PCS move. Additionally, AFIT offers graduate degrees in Systems Engineering and Engineering Management, through which students can specialize in Information Resource Management

(1AUY), Information Systems Management (OIYY), and Management Information Systems (1AME). The Systems Engineering graduate program offers both in-residence curriculum as well as distance learning opportunities.

4.2.1. The Center for Cyberspace Research (Air Force Cyberspace Technical Center of Excellence) conducts defense-focused research at the Master's and PhD levels. The CCR is forward-looking and responsive to the changing educational and research needs of the Air Force, Department of Defense, and the federal government. The CCR affiliated faculty teach and perform research focusing on understanding and developing advanced cyber-related theories and technologies.

4.3. The AFIT School of Systems and Logistics offers courses on acquisition, software and systems engineering, test and evaluation, logistics and financial management. These courses are offered through a mix of in residence, on-site and distance learning modes. The software engineering courses are collectively known as the Software Professional Development Program (SPDP). The objective of the program is to provide continuing education for USAF members involved in any aspect of software engineering, including acquisition, writing or modification of software. Specific topics include software project management, software requirements, software design, software implementation, software testing, and software maintenance. (Available to Active Duty, Reserve and Guard members).

4.4. The National Defense University offers leading-edge training in information resource management for lieutenant colonels (and civilian equivalent) and above. Applications for the course meet a selection board. Several courses, seminars, symposia and workshops are offered with differing lengths from 3 days to14 weeks.

4.5. The iCollege, Information Resources Management College at the National Defense University, prepares military and civilian leaders to optimize information technology management and secure information dominance within cyberspace. The iCollege offers seven unique, but connected, programs of study. They offer both classroom and online Distributed Learning formats.

4.6. The USAF Special Operations School (USAFSOS) sponsors a variety of courses furthering operational knowledge. USAFSOS is part of the Joint Special Operations University (JSOU) at Hurlburt Field, FL. JSOU educates Special Operations Forces (SOF) executive, senior and intermediate leaders and selected other national and international security decision-makers, both military and civilian, through teaching, research, and outreach in the science and art of Joint Special Operations.

4.7. Naval Postgraduate School (NPS). The Navy has developed a unique academic institution whose emphasis is on education and research programs that are relevant to the Navy, defense and national and international security interests. NPS provides a continuum of learning opportunities, including graduate degree programs, continuous learning opportunities, refresher, and transition education. The NPS offers an Operational and Information Sciences program which covers the wide range of Information Operations. (Program available to Active Duty members).

4.8. The Information Operations Fundamental Applications Course, formerly known as Information Warfare Applications Course (IWAC) at Maxwell AFB, AL, educates students in the fundamental principles of Information Operations in accordance with AF Doctrine Document 2-5. The objective is to provide students with a broad understanding of Information Operations Doctrine and insight into how Information Operations are applied across the full spectrum of conflict from peace to war. The course is taught at the college level through lectures, seminars, practical exercises, readings and computer based lessons.

4.9. The Engineering Installations Lightning Force Academy at Fort Indiantown Gap, PA, provides formal classroom training to acquaint communication systems project engineers and newly assigned engineers with the various intricacies and communications disciplines they will confront within their real world workload.

4.10. The Contingency Wartime Planning Course (CWPC) at Maxwell AFB, AL, provides a comprehensive macro view of the contingency and crisis action planning processes from both joint and Air Force perspectives. Supporting topics include unit readiness assessment, mobilization, expeditionary site planning, and command relationships. (Available to Air National Guard and Air Force Reserve personnel, but the quota is not funded by Air University).

4.11. The Defense Acquisition University (DAU) provides mandatory, assignment-specific, and continuing education courses for military and civilian acquisition personnel within the Department of Defense. Its mission is to provide the acquisition community with the right learning products and services to make smart business decisions. The DAU coordinates acquisition education and training programs to meet the training requirements of more than 140,000 DoD acquisition personnel. As the DoD corporate university for acquisition education, the DAU sponsors curriculum and instructor training to provide a full range of basic, intermediate, advanced, and assignment-specific courses to support the career goals and professional development of the Acquisition Workforce. In addition to providing curriculum-based training, both in the classroom and via the Internet, the DAU fosters professional development through publications, symposia, research, and consulting in areas related to the acquisition functions.

4.12. The National Intelligence University is a federal degree granting institution with a far-reaching mission - to educate and prepare intelligence officers to meet current and future challenges to the national security of the United States. The NIU is a unique and technologically advanced university that focuses on the profession of intelligence and is the only institution of higher education in the nation that allows its students to study and complete research in the Top Secret/Sensitive Compartmentalized Information (TS/SCI) arena. The University is committed to offering and continuously maintaining an in-depth curriculum intended to enhance the desired analytical skills and competencies of intelligence analysis to include critical thinking, communications, engagement and leadership. The staff and faculty at NIU work closely with a professionally diverse student population to provide a challenging and rewarding educational experience that culminates in a Bachelor of Science in Intelligence Degree, a Master of Science in Strategic Intelligence Degree, and graduate certificates in intelligence studies.

4.13. The Joint Command, Control, Communications, and Computers (C4) Planners Course
The Joint C4 Planners Course (JC4PC) mission is to educate C4 Planners in Doctrinal C4

concepts in the Joint, Interagency, and Coalition environments. While normal communications training programs focus on Service specific requirements, the Joint C4 Planners Course fills a capability gap by preparing mid-grade C4 Planners for the technical requirements of planning Joint net-centric operations in Joint, Coalition and Interagency environments. The course focuses on the technical aspects of Joint C4 planning associated with Strategic, Theater and Tactical level systems within the deliberate and crisis action planning (CAP) processes. The JC4PC is a four-week operational level course sponsored by the Joint Chief of Staff J6.

4.14. The AOC Initial Qualification Training, Communications Course (AOCIQCOM) at Hurlburt Field trains personnel assigned to an AN/USQ-163 AOC weapon system or a manpower forces unit to perform Communications duties in a Combined/Joint Air Operations Center (C/JAOC). The course provides students with education and training on JAOC communications organization, tasks and responsibilities, Communications doctrine, Internal AOC systems and services, Data Link and Flow Analysis, Crisis Action Planning, Communications Planning Tools and Factors, OPORD Formats, Annex K, ATO Communications and Distribution Planning, and alternate AOC site surveys. Personnel also receive education and training on joint and Service doctrine, Theater Air Ground System (TAGS), JAOC organization and processes, and applicable Theater Battle Management Core Systems (TBMCS) applications and other associated JAOC Command and Control (C2) systems tools.

4.15 The Information Operations Fundamental Course. The IOFC is a distance-learning course designed to be self-paced and is the pre-requisite to attend the Information Operations Integration Course (IOIC) at Hurlburt Field FL. This course is designed to provide the tools to understand the basics of IO, and provide a basic understanding of the need for IO in the Air Force and the concerns of senior leadership in the IO arena.

4.16. The Information Operations Integration Course. The IOIC trains selected officers and NCOs to provide gain, exploit, defend, and attack products and services to the Air Force Forces (AFFOR) and Joint Forces Air Component Commander (JFACC). The purpose of this course is to teach students the basics of Information Operations (IO), Air Force and Joint doctrine, concepts of operations, executing organizations, and operational functions of the USAF. Students will receive an initial familiarization of operations within the Air & Space Operations Center, focused on effects-based operations, and the importance of IO integration within operations planning.

4.17. The Joint C4I Staff and Operations Course educate and train Joint C4I decision makers in C4I concepts in the joint/coalition/interagency environments, the DoD's organization and how it supports the C4I process, and the management and operation of current Joint C4I systems and joint operational procedures associated with both strategic and theater/tactical systems. Students are required to demonstrate their learning by means of successfully completing an end of course examination and through participation in a C4I planning practical exercise.

4.18. Books 24x7. Books 24x7 is an online reference library containing over 4,000 unabridged IT publications. It is accessible via a member's AF IT E-Learning account on the AF Portal.

4.19. The Cyberspace Operations Officer Assignments Team web site also lists training opportunities. Access via the myPers and search using "Officer Assignments," then choose 17XX Cyber Operations.

Section C - Support Materials

There are currently no support material requirements. This area is reserved.

Section D - MAJCOM Unique Requirements

There are currently no MAJCOM unique requirements. This area is reserved.

2. Recommendations. Comments and recommendations are invited concerning the quality of AETC training. A Customer Service Information Line (CSIL) has been installed for the supervisors' convenience. For a quick response to concerns, call our CSIL at DSN 597-4566, or fax us at DSN 597-3790, or email us at 81trg-tget@us.af.mil. Reference this CTS/CTG and identify the specific area of concern (paragraph, training standard element, etc.).

BY ORDER OF THE SECRETARY OF THE AIR FORCE

OFFICIAL

WILLIAM J. BENDER, Lieutenant General, USAF
Chief, Information Dominance and
Chief Information Officer

Attachments:
1. Training Proficiency Code Key
2. Undergraduate Cyber Training (Phase 1-Tentative) CTS
3. Undergraduate Cyber Training (Phase 2-Tentative) CTS
4. Specialty Training Standard (STS) 17X

PROFICIENCY CODE KEY		
	SCALE VALUE	DEFINITION**: The individual**
Task Performance Levels	1	Can do simple parts of the task. Needs to be told or shown how to do most of the task. (EXTREMELY LIMITED)
	2	Can do most parts of the task. Needs help only on hardest parts. (PARTIALLY PROFICIENT)
	3	Can do all parts of the task. Needs only a spot check of completed work. (COMPETENT)
	4	Can do the complete task quickly and accurately. Can tell or show others how to do the task. (HIGHLY PROFICIENT)
***Task Knowledge Levels**	a	Can name parts, tools, and simple facts about the task. (NOMENCLATURE)
	b	Can determine step by step procedures for doing the task. (PROCEDURES)
	c	Can identify why and when the task must be done and why each step is needed. (OPERATING PRINCIPLES)
	d	Can predict, isolate, and resolve problems about the task. (ADVANCED THEORY)
****Subject Knowledge Levels**	A	Can identify basic facts and terms about the subject. (FACTS)
	B	Can identify relationship of basic facts and state general principles about the subject. (PRINCIPLES)
	C	Can analyze facts and principles and draw conclusions about the subject. (ANALYSIS)
	D	Can evaluate conditions and make proper decisions about the subject. (EVALUATION)

Explanations

* A task knowledge scale value may be used alone or with a task performance scale value to define a level of knowledge for a specific task. (Example: b and 1b)

** A subject knowledge scale value is used alone to define a level of knowledge for a subject not directly related to any specific task, or for a subject common to several tasks. This mark is used alone instead of a scale value to show that no proficiency training is provided in the course or CDC.

(-) This mark is used alone in Proficiency Codes Course columns to show that training is required but not given due to limitations in resources.

NOTE: All tasks and knowledge items shown with a proficiency code are trained during wartime.

(-) When this code is used in the Core & Wartime Tasks Column it indicates that the qualification is a local determination.

(5) When this code is used in the Core & Wartime Tasks Column it indicates the CFM has mandated this task as a core 5-level requirement. The training to satisfy this requirement is either provided through OJT, CBTs, CDCs, or a combination.

(7) When this code is used in the Core & Wartime Tasks Column it indicates the CFM has mandated this task as a core 7-level requirement. The training to satisfy this requirement is either provided through OJT, CBTs, CDCs, or a combination.

Tasks, Knowledge, and Proficiency Level

1. DOD CYBER FUNDAMENTALS	
1.1. Concepts	B
1.2. Doctrine, Policy, and Guidance	B
1.3. Cyberspace	B
1.4. Global Information Grid (GIG)	B
1.5. National Strategy	B
1.6. Command and Control Relationships	B
2. CYBER ORGANIZATIONS AND MISSIONS	
2.1. Air Force	B
2.2. DoD/Joint Forces	B
2.3. Combined Forces	B
3. CYBER CAREER FORCES	
3.1. Career Paths	B
3.2. Officer	B
3.3. Enlisted	B
3.4. Civilians	B
3.5. Contractors	B
3.6. Training	B
4. ENTERPRISE NETWORKS	
4.1. Supported Missions	B
4.2. Core Services	B
4.3. Plans and Programs	B
5. MISSION ASSURANCE	
5.1. Information Operations (IO)	B
5.2. Information Security	B
5.3. Operations Security	B
5.4. Physical Security	B
5.5. Enterprise Information Management (EIM)	B
5.6. Certification and Accreditation	B
5.7. Maintenance Management	B
6. CONTINUITY OF OPERATIONS (COOP)	
6.1. Sustainment	B
6.2. Disaster Recovery	B
6.3. Contingency Operations	B
6.4. Combining Mission Assurance and COOP	2b
7. INFORMATION TECHNOLOGY SYSTEMS	
7.1. Air Force Networks (AFNet)	B
7.2. LandWarNet	B
7.3. Navy Marine Corps Intranet (NMCI)	B
7.4. Defense Enterprise Computing Centers (DECC)	B
8. DOMAIN OPERATIONS	
8.1. Standardization and Evaluation	B
8.2. Mission Platforms	B
8.3. Operations Maintenance Management	B
9. COMMUNICATIONS TECHNOLOGY SYSTEMS	
9.1. Internet Protocol Systems	B
9.2. Radio Systems	B
9.3. Voice Systems	B
9.4. Industrial Systems	B
9.5. Air Field Systems	B

9.6. Space Systems	B
9.7. Air Defense Systems	B
9.8. Airborne Network Systems	B
9.9. Command & Control Network Systems	B
10. TRANSMISSION SYSTEMS	
10.1. Concepts	B
10.2. Structure	B
10.3. Signal Characteristics	B
10.4. Spectrum	B
10.5. Mediums	B
10.6. Multiplexing	B
11. DEPLOYED OPERATIONS	
11.1. Planning	B
11.2. Deployed Systems	B
11.3. Organizations	B
11.4. Expeditionary Concepts	B
11.5. Perform Mobilization	2b
11.6. Operations	B
12. INFORMATION ASSURANCE/CYBER SURETY	
12.1. Roles and Responsibilities	B
12.2. Emissions Security	B
12.3. Communication Security	B
12.4. Computer Security	B
12.5. Operations Security	B
12.6. Physical Security	B
13. STANDARDIZATION AND EVALUATION	
13.1. Policies and Procedures	B
13.2. Initial Qualification Training (IQT)	B
13.3. Mission Qualification Training (MQT)	B
13.4. Combat Mission Ready (CMR)	B
14. CERTIFICATION AND ACCREDITATION	
14.1. Department of Defense (DoD) Information Assurance C&A Process (DIACAP)	B
14.2. Policies and Procedures	B
14.3. Authority to Operate (ATO) and Authority to Connect (ATC) Decisions	B
14.4. Enterprise Mission Assurance Support Service (eMASS)	B
15. SECURITY TOOLS EMPLOYMENT	
15.1. Security Tools and Countermeasures	B
15.2. Establish and Conduct Cyber Surety Validation and Verification	2b
16. CONFIDENTIALITY, INTEGRITY AND AVAILABILITY (CIA)	
16.1. CIA Triad	B
17. ORGANIZATIONAL SECURITY	
17.1. Disposal and Destruction	B
18. BUSINESS CONTINUITY	
18.1. Environmental Controls	B
19. NETWORKING FUNDAMENTALS	
19.1. Governing Organizations and Standards	B
19.2. Computer Fundamentals	B
19.3. Digital Numbering Systems	B
19.4. Network Types	B
19.5. Networking Models	B
19.6. Network Management and Security	B
19.7. Local Area Network Cabling and Switching	B
19.8. Internet Protocol Addressing and Routing	B

19.9. Transport and Application Layer Protocols	B
19.10. Wide Area Network Fundamentals	B
19.11. Wireless Network Fundamentals	B
19.12. Perform Command-Line Interfacing and Network Configurations	2b

Tasks, Knowledge, and Proficiency Level

20. MITIGATING THREATS	
20.1. Virus and Spyware Management	B
20.2. Browser Security	B
20.3. Social Engineering Threats	B
21. CRYPTOGRAPHY	
21.1. Symmetric Cryptography	B
21.2. Public Key Cryptography	B
22. AUTHENTICATION SYSTEMS	
22.1. Perform Authentication	2b
22.2. Perform Hashing	2b
23. MESSAGING SECURITY	
23.1. E-mail Security	B
23.2. Messaging and Peer-to-Peer Security	B
24. USER AND ROLE-BASED SECURITY	
24.1. Security Policies	B
24.2. Securing File and Print Resources	2b
25. NETWORK WARFARE CONCEPTS	
25.1. Roles and Responsibilities	B
25.2. Capabilities	B
25.3. Tactics, Techniques, and Procedures	B
25.4. Area of Responsibility (AOR)	B
25.5. Adversary Planning	B
25.6. Special Access Programs (SAP)	B
25.7. Integrated Joint Special Technical Operations (IJSTO)	B
26. OFFENSIVE CYBERSPACE OPERATIONS (OCO)	
26.1. Terms and Definitions	B
26.2. Capabilities and Vectors	B
26.3. Perform Nodal Analysis	2b
26.4. Perform Operational Analysis	2b
26.5. Perform OCO Mission Planning	2b
26.6. Operations and Resource Management	B
26.7. Intelligence and Technical Gain/Loss	B
26.8. Platform Defensive Measures	B
26.9. Perform Targeting	2b
26.10. Employ Mission Execution	2b
26.11. Measures of Effectiveness/Performance	B
26.12. Prepare an After Action Report	2b
26.13. Prepare and Present OCO Mission Debrief	2b
27. AIR FORCE NETWORKS (AFNet)	
27.1. Defense-in-Depth	B
27.2. Network Management Functions	B
27.3. Network Services	B
27.4. Generate Network Operations Orders	2b
27.5. Operate Administrative Tools	2b
27.6. Perform Network Management	2b

27.7. Perform Security Measures & Defense	2b
27.8. Perform Network Simulations and Configurations	2b
27.9. Prepare and Present a Master Station Log Brief	2b
28. TELEPHONY NETWORKS	
28.1. Design and Architecture	B
28.2. Manipulate Components and Configurations	2b
28.3. Attack, Exploit & Defensive Strategies	B
28.4. Perform Security Measures & Defense	2b
28.5. Perform Telephony Mission Planning	2b
28.6. Execute Telephony Mission	2b
28.7. Prepare and Present Telephony Mission Debrief	2b
29. MOBILE NETWORKS	
29.1. Attack & Exploit Methods	B
29.2. Perform Mobile Mission Planning	2b
29.3. Execute Mobile Mission	2b
29.4. Prepare and Present Mobile Mission Debrief	2b
30. SPACE AND SATELLITE NETWORKS	
30.1. Design and Architecture	B
30.2. Components and Configurations	B
30.3. Attack, Exploit & Defensive Strategies	B
30.4. Security	B
30.5. Perform Space & Satellite Mission Analysis	2b
30.6. Develop Defensive and Offensive Courses of Action	2b
30.7. Prepare and Present Space & Satellite Mission Analysis Brief	2b
31. INTEGRATED AIR DEFENSE (IADS) NETWORKS	
31.1. Design and Architecture	B
31.2. Components and Configurations	B
31.3. Attack, Exploit & Defensive Strategies	B
31.4. Security	B
31.5. Perform IADS Mission Analysis	2b
31.6. Develop Defensive and Offensive Courses of Action	2b
31.7. Prepare and Present IADS Mission Analysis Brief	2b
32. COMMAND & CONTROL(C2) AND TACTICAL DATA LINK (TDL) NETWORKS	
32.1. Design and Architecture	B
32.2. Components and Configurations	B
32.3. Attack, Exploit & Defensive Strategies	B
32.4. Perform Security Measures & Defense	2b
32.5. Perform C2 & TDL Mission Analysis	2b
32.6. Develop Defensive and Offensive Courses of Action	2b
32.7. Prepare and Present C2 & TDL Mission Analysis Brief	2b
33. INDUSTRIAL CONTROL SYSTEMS (ICS)	
33.1. Design an Architecture	2b
33.2. Manipulate Components and Configurations	2b
33.3. Attack, Exploit & Defensive Strategies	B
33.4. Perform Security Measures & Defense	2b
33.5. Perform ICS Mission Planning	2b

33.6. Execute an ICS Mission	2b
33.7. Prepare and Present ICS Mission Debrief	2b
34. US LAWS	
34.1. Federal Communications Commission (FCC)	B
34.2. Federal Acts	B
34.3. Interagency Communications and Coordination	B
35. MILITARY CODES	
35.1. Law of Armed Conflict	B
35.2. Uniform Code of Military Justice	B
35.3. Rules of Engagement	B
36. INTERNATIONAL LEGAL GUIDANCE	
36.1. International Legal Guidance	A
37. GOVERNMENT/INDIVIDUAL INFORMATION ASSURANCE	
37.1. Legal Rights	B
37.2. Consent to Monitoring	B
37.3. Case Studies	B
38. INDUSTRY AND SERVICE POLICIES AND PROCEDURES	
38.1. Regulations for the Networking Environment	B
38.2. Air Force Instructions	B
39. LAW ENFORCEMENT AGENCIES	
39.1. Organizational Structure	B
39.2. Roles, Responsibilities, and Jurisdiction	B
40. ETHICS	
40.1. Terms and Definitions	B
40.2. Case Studies	B
41. NETWORK THREATS AND DEFENSE	
41.1. Current Cyber Threats and Attacks	B
41.2. Operate and Manage Incident Prevention, Detection, Response and Handling	2b
41.3. Cyber Network Defensive Strategies and TTP's	B
41.4. Perform Network Defense Mission Planning	2b
41.5. Execute a Network Defense Mission	2b
41.6. Prepare and Present Network Defense Mission Debrief	2b
42. FIGHTING THROUGH A CYBER ATTACK (CAPSTONE)	
42.1. Plan Cyber Operations	2b
42.2. Attack Cyber Technologies	2b
42.3. Defend Networks and Systems	2b
42.4. Prepare and Present Mission Brief and Debrief	2b
43. PUBLIC KEY INFRASTRUCTURE	
43.1. Key Management and Life Cycle	B
43.2. Certificate Server Setup	B
43.3. Web Server Security with PKI	B
44. ACCESS SECURITY	
44.1. Biometric Systems	B
44.2. Physical Access Security	B
44.3. Peripheral and Component Security	B
44.4. Storage Device Security	B

45. PORTS, PROTOCOLS AND SERVICES	
45.1. TCP/IP Review	B
45.2.Perform Protocol-based Attacks	2b
45.3. Common System Services	B
46. NETWORK SECURITY	
46.1. Common Network Devices	B
46.2. Secure Network Topologies	B
46.3. Browser-related Network Security	B
46.4. Virtualization	B
47. WIRELESS SECURITY	
47.1. Non-PC Wireless Devices	B
48. REMOTE ACCESS SECURITY	
48.1. Perform Remote Access	2b
48.2. Operate Virtual Private Networks	2b
49. AUDITING, LOGGING AND MONITORING	
49.1. System Logging	B
49.2. Server Monitoring	B
50. ORGANIZATIONAL SECURITY	
50.1. Organizational Policies	B
50.2. Education and Training	B
50.3. Disposal and Destruction	B
51. BUSINESS CONTINUITY	
51.1. Redundancy Planning	B
51.2. Backups	B
51.3. Environmental Controls	B

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
1. DOD CYBER FUNDAMENTALS TR: AFH 33-337; AFIs 10-401, 33-115, 33-150									
1.1. Concepts									
1.1.1. Communications Etiquette TR: AFPAM 36-2241; AFH 33-337	-					B	-	-	-
1.2. Doctrine, Policy, and Guidance									
1.2.1. Cyberspace Doctrine Principles	-					B	-	-	-
1.2.2. Information Technology Infrastructure Library (ITIL) TR: https://www.my.af.mil (under AF e-learning site) ITIL 2011 Edition Overview: Intro to ITIL Framework	-					B	-	-	-
1.3. Cyberspace									
1.3.1. Cyberspace Operations TR: AFDD 3-12, AFI 10-706; AFPD 3-13.1									
1.3.1.1. Structure	-					B	-	-	-
1.3.1.2. Missions									
1.3.1.2.1. Offensive	-					B	-	-	-
1.3.1.2.2. Defensive	-					B	-	-	-
1.3.1.2.3. Exploitation	-					B	-	-	-
1.3.1.2.4. Other (e.g. Influence Operations (IFO), Electronic Warfare (EW))	-					B	-	-	-
1.4. Air Force Information Network (AFIN)	-					B	-	-	-
1.5. National Strategy									
1.5.1. Evolution of US Strategy and Cyberspace	-					B	-	-	-
1.6. Command and Control Relationships	-					B	-	-	-
2. CYBER ORGANIZATIONS AND MISSIONS TR: AFPD 10-17; AFI 33-115, 38-101									
2.1. Air Force									
2.1.1. Communications Squadron	-					B	-	-	-
2.1.2. Air Communications Squadron (ACOMS)	-					B	-	-	-
2.1.3. Combat Communications Squadron	-					B	-	-	-
2.1.4. Expeditionary Communications Squadron	-					B	-	-	-
2.1.5. Air and Space Operations Center (AOC)	-					B	-	-	-
2.1.6. Contingency Response Wing (CRW)	-					B	-	-	-
2.1.7. Air Control Squadron (ACS)	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
2.1.8. Engineering & Installation Squadron (E&I)	-					B	-	-	-
2.1.9. Air Force Network Operations (AFNetOps)									
2.1.9.1. 24th Air Force	-					B	-	-	-
2.1.9.2. 624th Operations Center (624 OC)	-					B	-	-	-
2.1.9.3. 67th Cyberspace Wing	-					B	-	-	-
2.1.9.4. Network Operations Security Center (NOSC)	-					B	-	-	-
2.1.9.5. Enterprise Service Unit (ESU)	-					B	-	-	-
2.1.9.6. Area Processing Center (APC)	-					B	-	-	-
2.1.9.7. Enterprise Service Desk (ESD)	-					B	-	-	-
2.1.9.8. Communications Focal Point (CFP) TR: MPTO 00-33A-1001-WA-1	-					B	-	-	-
2.1.10. Cyber Mission Force									
2.1.10.1. Definitions and Roles/Responsibilities	-					B	-	-	-
2.1.10.2. Command and Control	-					B	-	-	-
2.1.10.3. Mission Areas									
2.1.10.3.1. National Mission Force	-					B	-	-	-
2.1.10.3.2. Operate and Defend the DoDIN	-					B	-	-	-
2.1.10.3.3. Combatant Command Support	-					B	-	-	-
2.1.10.4. Mission Forces									
2.1.10.4.1. National Mission Force	-					B	-	-	-
2.1.10.4.2. Protection Force	-					B	-	-	-
2.1.10.4.3. Combat Mission Force	-					B	-	-	-
2.2. DoD/Joint Forces									
2.2.1. United States Strategic Command (USSTRATCOM)	-					B	-	-	-
2.2.2. United States Cyber Command (USCYBERCOM)	-					B	-	-	-
2.2.3. Joint Information Operations Warfare Center (JIOWC)	-					B	-	-	-
2.2.4. JFCC-Space (JFCC-SPACE)	-					B	-	-	-
2.2.5. JFC-Global Strike (JFCC-GS)	-					B	-	-	-
2.2.6. Defense Information systems Agency (DISA)	-					B	-	-	-
2.3. Combined Forces									
2.3.1. Allies/Coalition NW Ops	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
2.3.2. NORAD & USNORTHCOM	-					B	-	-	-
3. CYBER CAREER FORCES TR: AFH 33-337; AFIs 33-115 v1, 36-2101, 38-101; AFPD 10-17; 3DXXX CFETP, 1B4 CFETP, 3A CFETP, 17X CFETP; AFOCD									
3.1. Career Paths									
3.1.1. Career Field Supervision and Leadership									
3.1.1.1. AF Career Field Manager	-					B	-	-	-
3.1.1.2. MAJCOM Functional Manager TR: MFM Handbook	-					B	-	-	-
3.1.2. Explain Duties/Responsibilities of AFS	-					B	-	-	-
3.1.3. Explain Qualifications	-					B	-	-	-
3.2. Officer									
3.2.1. Progression within 17X AFS	-					B	-	-	-
3.2.2. Explain Responsibilities of AFSC	-					B	-	-	-
3.2.3. AFSC Core Competencies	-					B	-	-	-
3.2.4. Read 17X CFETP/AFOCD	-					B	-	-	-
3.3. Enlisted									
3.3.1. Explain Progression within 1B4, 3DXXX, 3A Career Fields	-					B	-	-	-
3.3.2. Explain Responsibilities of Enlisted AFSCs	-					B	-	-	-
3.3.3. AFSCs Core Competencies	-					B	-	-	-
3.3.4. Read 1B4, 3DXXX, and 3A CFETP/AFECD	-					B	-	-	-
3.4. Civilians									
3.4.1. Roles and Responsibilities of Supervising Government Civilian Personnel	-					B	-	-	-
3.5. Contractors									
3.5.1. Roles and Responsibilities of Supervising Government Contract Personnel	-					B	-	-	-
3.6. Training									
3.6.1. Air Force Training Program	-					B	-	-	-
3.6.2. Training Business Area (TBA)	-					B	-	-	-
3.6.3. Coordinate with Unit Training Manager (UTM)	-					B	-	-	-
3.6.4. Develop Individual Training Plan in TBA	-					B	-	-	-
3.6.5. Conduct Initial Evaluation	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
3.6.6. Evaluate Newly Assigned Personnel and Identify Individual Training Requirements TR: AFI 36-2201; AFI 33-150; Applicable CFETP; Unit Training Manual	-					B	-	-	-
3.6.7. On-the-Job Training (OJT) TR: AFI 36-2201; and Local Directives									
3.6.7.1. Plan and Schedule OJT	-					B	-	-	-
3.6.7.2. Conduct OJT	-					B	-	-	-
3.6.7.3. Evaluate OJT	-					B	-	-	-
3.6.7.4. Manage OJT Documentation	-					B	-	-	-
3.6.7.5. Evaluate Quality of OJT and Provide Trainee Feedback TR: AFI 36-2201	-					B	-	-	-
3.6.8. Document Training Progression	-					B	-	-	-
3.6.9. Evaluate Adequacy of Training	-					B	-	-	-
3.6.10. Administer the CDC Program	-					B	-	-	-
3.6.11. Identify Additional Formal Training Requirements	-					B	-	-	-
4. MISSION ASSURANCE TR: AFTTP 3-1.CWO; AFDD 3-12; AFPD 10-17; AFI 10-1701, 33-150; CJCSM 6510.01B; JP 3-12									
4.1. Information Operations (IO)									
4.1.1. Fundamentals of Influence Operations, Electronic Warfare Operations, and Network Warfare Operations	-					B	-	-	-
4.1.2. Capabilities of Influence Operations, Electronic Warfare Operations, and Network Warfare Operations	-					B	-	-	-
4.1.3. Integrated Capabilities of Influence Operations, Electronic Warfare Operations, and Network Warfare Operations	-					B	-	-	-
4.1.4. Information Conditions(INFOCON) TR: AFI 10-710	-					B	-	-	-
4.2. Information Security TR: AFI 31-401; AFPDs 31-4, 33-2									
4.2.1. Definition	-					B	-	-	-
4.2.2. Classification Process	-					B	-	-	-
4.2.3. Declassification Process	-					B	-	-	-
4.2.4. Information Safeguards									
4.2.4.1. Privacy Act (PA)	-					B	-	-	-
4.2.4.2. For Official Use Only (FOUO)	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
4.2.4.3. Sensitive Unclassified	-					B	-	-	-
4.2.4.4. Classified	-					B	-	-	-
4.2.5. Protect or Understand Special Data Protection (e.g. Sensitive Personnel Information)	-					B	-	-	-
4.3. Operations Security TR: AFI 10-701; AFPD 10-7									
4.3.1. Definition	-					B	-	-	-
4.3.2. Background	-					B	-	-	-
4.3.3. Relationship of OPSEC to other Security Programs	-					B	-	-	-
4.3.4. Vulnerabilities									
4.3.4.1. Open Conversations	-					B	-	-	-
4.3.4.2. Electronic Communication	-					B	-	-	-
4.3.4.3. Social Media	-					B	-	-	-
4.3.4.4. Family/Friends	-					B	-	-	-
4.3.4.5. Critical Information	-					B	-	-	-
4.4. Physical Security TR: AFI 31-101; AFPD 31-1									
4.4.1. Definition	-					B	-	-	-
4.4.2. Secure Area Access Management	-					B	-	-	-
4.4.3. Facility Security Requirements	-					B	-	-	-
4.4.4. Identify Violations Procedures	-					B	-	-	-
4.4.5. Report Violations Procedures	-					B	-	-	-
4.4.6. Classified Material Control									
4.4.6.1. Storage	-					B	-	-	-
4.4.6.2. Transport	-					B	-	-	-
4.4.6.3. Handling	-					B	-	-	-
4.4.6.4. Destruction	-					B	-	-	-
4.4.6.5. Classified Waste	-					B	-	-	-
4.4.6.6. Marking	-					B	-	-	-
4.5. Enterprise Information Management TR: AF EIM CONOP; AF EIM Strategy									
4.5.1. Definition	-					B	-	-	-
4.5.2. Capabilities	-					B	-	-	-
4.5.3. Collaborative Technology	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
4.5.4. Information Management TR: AFPD 33-3; AFIs, 33-121, 33-129; AFH 33-337; AFMANs 33-152, 33-326; 37-104 (will convert to AFI 33-396) and TO 31S5-4-7205-8-1 PKI Fundamentals									
4.5.4.1. Electronic Communications	-					B	-	-	-
4.6. Certification and Accreditation									
4.6.1. Certification and Accreditation Process	-					B	-	-	-
4.7. Maintenance Management									
4.7.1. Fire Protection Procedures TR: AFI 91-202, chap 6; Command and Local Directives									
4.7.1.1. Fire Extinguishers	-					B	-	-	-
4.7.1.2. Describe Fire Protection Procedures for Electronic Equipment	-					B	-	-	-
4.7.1.3. Describe Fire Protection Procedures for Critical Communications Facilities	-					B	-	-	-
4.7.2. Work Center Safety program TR: AFI 91-202, chaps 1, 2.2 thru 2.3, and 4; AFI 91-203 chap 1; Command and Local Directives									
4.7.2.1. Manage Work Center Program	-					B	-	-	-
4.7.2.2. Conduct Job Safety Analysis	-					B	-	-	-
4.7.2.3. Document AF Form 55	-					B	-	-	-
4.7.2.4. Conduct Inspections	-					B	-	-	-
4.7.3. Safety Precautions and Guidelines TR: AFI 91-203, AFQTP 3DXXX-202A									
4.7.3.1. AF Consolidated Occupational Safety Instruction and its Importance TR: AFI 91-203	-					B	-	-	-
4.7.3.2. Electrostatic Discharge	-					B	-	-	-
4.7.3.3. Communications Systems Grounding, Bonding and Shielding	-					B	-	-	-
4.8. Security Tools and Countermeasures									
4.8.1. Defense-in-Depth	-					B	-	-	-
4.8.2. Network Warfare Support (NS) Capabilities and Limitations	-					B	-	-	-
4.8.3. Network Defense (NetD) Capabilities and Limitations	-					B	-	-	-
4.8.4. Threat Capabilities and Limitations and their Applicability to the Current Mission	-					B	-	-	-
4.9. Roles and Responsibilities	-					B	-	-	-
4.10. Emissions Security TR: AFSSI 7700; AFPD 33-2									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
4.10.1. Definition	-					B	-	-	-
4.10.2. Notifications	-					B	-	-	-
4.10.3. Vulnerabilities	-					B	-	-	-
4.10.4. Protected Distribution System (PDS)	-					B	-	-	-
4.10.5. Separation	-					B	-	-	-
4.11. Communications Security TR: AFIs 31-401, 33-201 (v2); AFPDs 31-4, 33-2									
4.11.1. Definition	-					B	-	-	-
4.11.2. Vulnerabilities	-					B	-	-	-
4.11.3. Safeguarding Information	-					B	-	-	-
4.11.4. Explain cryptology (Bound & Unbound) Concepts									
4.11.4.1. Bulk Encryption	-					B	-	-	-
4.11.4.2. Information Encryption Techniques	-					B	-	-	-
4.11.4.3. Separation Requirements	-					B	-	-	-
4.11.5. Identify Insecurities	-					B	-	-	-
4.11.6. Report Insecurities	-					B	-	-	-
4.11.7. Protect COMSEC Material TR: AFI 33-201 (V2), sec E, paras 20.1 thru 20.6.1. and Local COMSEC Directives									
4.11.7.1. Store COMSEC Material Equipment TR: AFI 33-201 (V2), Sec E, paras 19.1 thru 19.5 and Local COMSEC Directives	-					B	-	-	-
4.11.7.2. Store Controlled Cryptographic Equipment TR: AFI 33-201 (V2), Sec E, paras 19.1 thru 19.5 and Local COMSEC Directives	-					B	-	-	-
4.11.7.3. Explain procedures for Destroying Cryptographic Equipment and Materials TR: AFI 33-201 (V2), Sec G, paras 27 thru 32 and Local Directives	-					B	-	-	-
4.11.7.4. Explain How to Report Physical, Personnel, and Cryptographic Security Violations TR: AFI 33-201 (V2), and Local Directives	-					B	-	-	-
4.11.7.5. Protect Organization's Mission Critical Information TR: AFI 10-701; AFPD 10-7; MAJCOM/FOA Directives; and Local Directives	-					B	-	-	-
4.12. Computer Security (COMPUSEC) TR: AFIs 33-2200; AFPD 33-2; AFMAN 33-282									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
4.12.1. Definition	-					B	-	-	-
4.12.2. Vulnerabilities	-					B	-	-	-
4.12.3. Processing Classified Information	-					B	-	-	-
4.12.4. Identify Insecurities	-					B	-	-	-
4.12.5. Report Insecurities	-					B	-	-	-
4.12.6. Information Assurance TR: AFI 33-200 and AFI 33-210									
4.12.6.1. Definition	-					B	-	-	-
4.12.6.2. Threats and Vulnerabilities	-					B	-	-	-
4.12.6.3. Protective Measures	-					B	-	-	-
4.13. CIA Triad	-					B	-	-	-
4.14. Disposal and Destruction	-					B	-	-	-
4.15. Environmental Controls	-					B	-	-	-
5. CONTINUITY OF OPERATIONS (COOP)									
5.1. Risk and Vulnerability Assessment TR: AFIs 91-203, 91-302	-					B	-	-	-
5.2. Sustainment	-					B	-	-	-
5.3. Disaster Recovery	-					B	-	-	-
5.4. Contingency Operations	-					B	-	-	-
5.5. Combining Mission Assurance and COOP	-					2b	-	-	-
6. INFORMATION TECHNOLOGY SYSTEMS TR: AFI 13 Series, CJCSI 6211.02C, JP 6-0									
6.1. Air Force Information Network (AFNet) Architecture									
6.1.1. Non-Secure Internet Protocol Router Network (NIPRNET)	-					B	-	-	-
6.1.2. Secret Internet Protocol Router Network (SIPRNET)	-					B	-	-	-
6.2. Enterprise Service Centers (ESCs)									
6.2.1. Network Operations Security Center (NOSC)	-					B	-	-	-
6.2.2. Enterprise Service Unit (ESU)	-					B	-	-	-
6.2.3. Enterprise Service Desk (ESD)	-					B	-	-	-
6.2.4. Role of Integrated Network Operations and Security Centers (I-NOSC)	-					B	-	-	-
6.3. Joint Information Environment (JIE)	-					B	-	-	-
6.4. Supported Enterprise Missions									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
6.4.1. DoD Information Network (DoDIN)	-					B	-	-	-
6.4.2. Role of the DoDIN in Supporting Operations	-					B	-	-	-
6.4.3. Defense Information Systems Network (DISN)	-					B	-	-	-
6.4.4. Defense Switched Network (DSN)	-					B	-	-	-
6.4.5. Defense Red Switch Network (DRSN)	-					B	-	-	-
6.4.6. Joint World-wide Intelligence Communications System (JWICS)	-					B	-	-	-
6.4.7. National Security Agency (NSA) Net	-					B	-	-	-
6.5. Core Enterprise Services									
6.5.1. Knowledge Management TR: AF EIM CONOP; AF EIM Strategy; AF Portal Publishing Training Site; Air Force Portal Content Publishing Training Guides; TO 00-33D-3001-W-1 and AFI 33-129									
6.5.1.1. Air Force Portal									
6.5.1.1.1. Program Objectives	-					B	-	-	-
6.5.1.2. Roles	-					B	-	-	-
6.5.1.3. Collaborative Technology	-					B	-	-	-
6.5.2. Records Management Program TR: AFPDs 33-1, 33-3; AFIs 33-332, 33-364; AFMANs 37-104 (will convert to AFI 33-396), 33-363; AF Records Information Management System (AFRIMS); AF Electronic Records management Solution Guide									
6.5.2.1. Program Objectives	-					B	-	-	-
6.5.2.2. Definition of Official Records	-					B	-	-	-
6.5.2.3. User Responsibilities	-					B	-	-	-
6.5.2.4. Business Rules for Electronic Files (e-Files)	-					B	-	-	-
6.6. Standardization and Evaluation in the Domain	-					B	-	-	-
6.7. Mission Platforms in the Domain									
6.7.1. Global Broadcast Service (GBS) TR: T.O. 31R2-4-1899-1 WA-1	-					B	-	-	-
6.7.2. Global Positioning System (GPS)	-					B	-	-	-
6.7.3. Distributed Common Ground System (DCGS)	-					B	-	-	-
6.7.4. Battle Control System-Fixed	-					B	-	-	-
6.7.5. Unit Level-Unit Command and Control (UL-UC2)	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
6.7.6. Nuclear Command and Control Systems TR: CJCSI 3231.01B Nuclear Command and Control Extremely Sensitive Operation									
6.7.6.1. National Military Command Center (NMCC)	-					B	-	-	-
6.7.6.2. Global High Frequency Network	-					B	-	-	-
6.7..6.3. Strategic Automated Command and Control System (SACCS)	-					B	-	-	-
6.7.6.4. Military Strategic and Tactical Relay (MILSTAR) Satellite	-					B	-	-	-
6.7.6.5. Minimum Essential Emergency Communications Network (MEECN)	-					B	-	-	-
6.7.7. Long Haul Communications Elements									
6.7.7.1. DoD Teleports	-					B	-	-	-
6.7.7.2. Standard Tactical Entry Points	-					B	-	-	-
6.8. Operations Maintenance Management									
6.8.1. Plan and Organize Maintenance Activities	-					B	-	-	-
6.8.2. Direct Systems Analysis Design, Programming, Operations and Maintenance	-					B	-	-	-
6.8.3. Direct Systems Management, Technical Support, and Resource Management	-					B	-	-	-
6.8.4. Management Plans and Provide Implementation and Development Functions in a Maintenance Environment	-					B	-	-	-
6.8.5. Technical Orders									
6.8.5.1. Describe Technical Orders TR: TO 00-5-1	-					B	-	-	-
6.8.5.2. Identify Time Compliance Technical Orders (TCTO) Procedures TR: https://www.my.af.mil/etims/ETIMS/index.jsp; AFI 33-150; TO 00-5-15-WA-1, TO 00-33A-1001-WA-1 and applicable TCTOs	-					B	-	-	-
6.8.5.3. Implement Time Compliance Technical Orders (TCTO) Procedures and Document Completion TR: https://www.my.af.mil/etims?ETIMS/index.jsp ; AFI 33-150; TO 00-5-15-WA-1, TO 00-33A-1001-WA-1; and applicable TCTOs	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
6.8.5.4. Standard Installation Practices Technical Order (SIPTO) TR: TOs 31-10-2; 31-10-3; 31-10-4; 31-10-5; 31-10-6; 31-10-7; 31-10-9; 31-10-10; 31-10-11; 31-10-12; 31-10-14; 31-10-19; 31-10-20; 31-10-21; 31-10-23; 31-10-24; 31-10-27; 31-10-28; 31-10-29; 31-10-32; 31-10-33; 31-10-34	-					B	-	-	-
7. CYBER RELATED TECHNOLOGIES TR: https://www.my.af.mil (under AF e-Learning site); TO 31-1-141-2WA-1 Ch. 7, 9, and 10)									
7.1. Internet Protocol Systems TR: https://www.my.af.mil (under AF e-Learning site)									
7.1.1. TCP/IP	-					B	-	-	-
7.1.2. IPv4/IPv6	-					B	-	-	-
7.1.3. Ports (IP)	-					B	-	-	-
7.2. Radio Systems									
7.2.1. Antennas									
7.2.1.1. Transmitters									
7.2.1.1.1. Amplitude Modulation	-					B	-	-	-
7.2.1.1.2. Frequency Modulation	-					B	-	-	-
7.2.2. Receivers									
7.2.2.1. Amplitude Modulation	-					B	-	-	-
7.2.2.2. Frequency Modulation	-					B	-	-	-
7.2.3. Modulation Techniques									
7.2.3.1. Amplitude Modulation	-					B	-	-	-
7.2.3.2. Frequency Modulation	-					B	-	-	-
7.2.3.3. Phase Modulation	-					B	-	-	-
7.2.3.4. DAMA	-					B	-	-	-
7.2.3.5. Frequency Hopping	-					B	-	-	-
7.2.3.6. Time-Division (CDMA and GSM)	-					B	-	-	-
7.2.4. RoIP	-					B	-	-	-
7.2.5. HPW	-					B	-	-	-
7.3. Voice Systems									
7.3.1. POTS	-					B	-	-	-
7.3.2. VoIP	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
7.3.3. VoSIP	-					B	-	-	-
7.3.4. Coalition	-					B	-	-	-
7.4. Industrial Systems	-					B	-	-	-
7.5. Space Systems									
7.5.1. Air Force Satellite Control network (AFSCN)	-					B	-	-	-
7.5.2. Defense Meteorological Satellite Program (DMSP)	-					B	-	-	-
7.5.3. SPACECOM Digital Information Network (SDIN)	-					B	-	-	-
7.6. Air Defense Systems									
7.6.1. Air Defense System Integration	-					B	-	-	-
7.6.2. Joint Range Extension	-					B	-	-	-
7.6.3. Tactical Receive System	-					B	-	-	-
7.7. Airborne Network Systems	-					B	-	-	-
7.8. Command & Control Network Systems	-					B	-	-	-
7.9. Data Mining & Analytics	-					B	-	-	-
7.10. GIS	-					B	-	-	-
8. TRANSMISSION SYSTEMS TR: TO 31-1-141-2WA-1 Ch. 7, 9, and 10									
8.1. Concepts									
8.1.1. Synchronous Digital Communications	-					B	-	-	-
8.1.2. Isochronous Digital Communications	-					B	-	-	-
8.1.3. Asynchronous Digital Communications	-					B	-	-	-
8.1.4. Communications Systems Components									
8.1.4.1. Wired Communications Systems	-					B	-	-	-
8.1.4.2. Wireless Communications Systems	-					B	-	-	-
8.1.4.3. Wireless-Wireline Systems Interface	-					B	-	-	-
8.1.5. Systems Troubleshooting Techniques	-					B	-	-	-
8.2. Structure									
8.2.1. Signal Formats	-					B	-	-	-
8.3. Signal Characteristics									
8.3.1. Signal Rate	-					B	-	-	-
8.3.2. Bit Count Integrity	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
8.4. Spectrum	-					B	-	-	-
8.5. Mediums									
8.5.1. Transmission Lines	-					B	-	-	-
8.5.2. Fiber Optics	-					B	-	-	-
8.5.3. Data Bus	-					B	-	-	-
8.5.4. Antennas	-					B	-	-	-
8.5.5. Waveguides	-					B	-	-	-
8.5.6. Use Test Equipment									
8.5.6.1. Multimeters (Analog/Digital)	-					B	-	-	-
8.5.6.2. Oscilloscope	-					B	-	-	-
8.5.6.3. Signal/Function Generator	-					B	-	-	-
8.5.6.4. Line tester	-					B	-	-	-
8.6. Multiplexing	-					B	-	-	-
9. DEPLOYED OPERATIONS TR: https://aef.afpc.randolph.af.mil, https://jkodirect.jten.mil/Atlas2/faces/page/login/Login.seam , AFIs 10-401, 10-403, 21-109, 33-201 v2, 23-101									
9.1. Planning									
9.1.1. UTC Management									
9.1.1.1. Designed Operational Capability (DOC) Statement	-					B	-	-	-
9.1.1.2. Logistical Detail (LOGDET)	-					B	-	-	-
9.1.1.3. Manpower Force Packaging System (MANFOR)	-					B	-	-	-
9.1.1.4. AEF Posturing	-					B	-	-	-
9.1.1.5. Deployment Sourcing	-					B	-	-	-
9.1.2. Readiness Status Reporting									
9.1.2.1. Status of Resource and Training (SORTS)	-					B	-	-	-
9.1.2.2. AEF UTC Reporting Tool (ART)	-					B	-	-	-
9.1.2.3. Defense Readiness Reporting System (DRRS)	-					B	-	-	-
9.2. Deployed Systems									
9.2.1. C4ISR Platforms									
9.2.1.1. Air Operations Centers (AOC)	-					B	-	-	-
9.2.1.2. Ground Theater Air Control Systems (GTACS)	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
9.2.1.3. Air Support Operations Centers	-					B	-	-	-
9.2.1.4. Remote Piloted Aircraft (RPA)	-					B	-	-	-
9.2.2. Installation Notification and Warning System	-					B	-	-	-
9.3. Organizations									
9.3.1. Joint Task Force (JTF) Organizational Structure									
9.3.1.1. Unified/Combatant Commands (COCOM)	-					B	-	-	-
9.3.1.2. Air Force Component Commander (AFCC)	-					B	-	-	-
9.3.1.3. Joint Force Air Component Commander (JFACC)	-					B	-	-	-
9.3.1.4. Commander, Air Forces (COMAFFOR)	-					B	-	-	-
9.4. Expeditionary Concepts									
9.4.1. Concepts of Aerospace Expeditionary Force (AEF) Employment									
9.4.1.1. Deployment Process Overview	-					B	-	-	-
9.4.1.2. AEF Tempo Banding	-					B	-	-	-
9.4.1.3. Enable Forces	-					B	-	-	-
9.4.1.4. Deployment Planning and Execution	-					B	-	-	-
9.4.1.5. Unit Type Codes (UTC)	-					B	-	-	-
9.4.2. Force Module Communications Support Concept									
9.4.2.1. Open the Air Base	-					B	-	-	-
9.4.2.2. Command and Control	-					B	-	-	-
9.4.2.3. Establish the Air Base	-					B	-	-	-
9.4.2.4. Generate the Mission	-					B	-	-	-
9.4.2.5. Operate the Air Base	-					B	-	-	-
9.4.2.6. Robust the Air Base	-					B	-	-	-
9.5. Mobilization									
9.5.1. Deployment Procedures									
9.5.1.1. Describe Load Plan	-					B	-	-	-
9.5.1.2. Explain Pallet Build-Up Air and Surface Procedures	-					B	-	-	-
9.5.1.3. Explain Hazardous Cargo Preparation	-					B	-	-	-
9.6. Tactical Communications TR: AFPAM 10-100; MAJCOM and Local Directives									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
9.6.1. Tactical Communications Capability									
9.6.1.1. Contingency Response Groups (CRG)	-					B	-	-	-
9.6.1.2. Theater Deployable Communications (TDC)	-					B	-	-	-
9.6.1.3. Engineering & Installation (E&I)	-					B	-	-	-
9.6.2. Aeromedical Evacuation Support	-					B	-	-	-
9.7. Air Operations Center									
9.7.1. AOC Role	-					B	-	-	-
10. CERTIFICATION AND ACCREDITATION									
10.1. DoD Certification and Accreditation	-					B	-	-	-
10.2. Policies and Procedures	-					B	-	-	-
10.3. Authority to Operate (ATO) and Authority to Connect (ATC) Decisions	-					B	-	-	-
10.4. Enterprise Mission Assurance Support Service (eMASS)	-					B	-	-	-
11. NETWORK FUNDAMENTALS TR: https://www.my.af.mil (under AF e-Learning site), AFI 33-150; Cisco CCNA/CCENT Exam 640-802, 620-822, 620-816 Prep Kit									
11.1. Governing Organizations and Standards TR: AFDD 3-13, Information Operations; Health Insurance Portability and Accountability Act (IPAA), http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, USC TITLE 10, 18, and 50									
11.1.1. Department of Defense (DoD)/Joint Publications TR: http://www.dtic.mil/whs/directives/corres/pub1.htm	-					B	-		-
11.1.2. Air Force Publications TR: AFI 33-360; AFPD 33-4	-					B	-		-
11.1.3. Enterprise Information Architecture (EIA)/Telecommunications Industry Association (TIA) standards TR: http://global.ihs.com/, www.eia.org, http://skillport.books24x7.com/toc.aspx?bookid=33886, http://www.tiaonline.org/standards/tia-standards-overview	-					B	-		-
11.1.4. Military Standard (MILSTD) TR: http://www.dsp.dia.mil/APP_UIL/displayPage.aspx?action=contentid=66	-					B	-		-
11.1.5. DISA Publications TR: http://www.disa.mil/About/DISA-Issuances	-					B	-		-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
11.1.6. Department of Defense (DoD) Standards Protocol	-					B	-		-
11.1.7. Rules of Engagement (ROE)									
11.1.7.1. Policy	-					B	-		-
11.1.7.2. Security Tools	-					B	-		-
11.1.7.3. Cyber Management Ethics	-					B	-		-
11.1.7.4. System Monitoring	-					B	-		-
11.1.8. Institute of Electrical and Electronics Engineers (IEEE) Standards									
11.1.8.1. IEEE 802	-					B	-	-	-
11.1.8.2. IEEE 802.1X	-					B	-	-	-
11.1.8.3. IEEE 802.3	-					B	-	-	-
11.1.8.4. IEEE 802.11	-					B	-	-	-
11.2. Computer Fundamentals TR: https://www.my.af.mil (under AF e-Learning site)									
11.2.1. Components	-					B	-	-	-
11.2.2. Component Principles	-					B	-	-	-
11.2.3. Central Processing Unit (CPU)	-					B	-	-	-
11.2.4. Computer Memory	-					B	-	-	-
11.2.5. Input/output (I/O) Devices	-					B	-	-	-
11.2.6. Storage Devices	-					B	-	-	-
11.2.7. Peripherals (Printers, Fax, Scanners, etc.)	-					B	-	-	-
11.3. Digital Numbering Systems TR: Cisco CCNA/CCENT Exam 640-802, 640-816									
11.3.1. Formats									
11.3.1.1. Binary	-					B	-	-	-
11.3.1.2. Hexadecimal	-					B	-	-	-
11.3.1.3. Binary Coded Decimal	-					B	-	-	-
11.3.1.4. Calculate Hexadecimal Numbers	-					B	-	-	-
11.3.2. Physical Representation of Numbers	-					B	-	-	-
11.3.3. Convert Digital Numbers Across Formats	-					B	-	-	-
11.3.4. Boolean Logic Arguments	-					B	-	-	-
11.4. Network Types									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
11.4.1. Wired (LAN, WAN, MAN)	-					B	-	-	-
11.4.2. Wireless	-					B	-	-	-
11.4.3. Virtual Private Network (VPN)	-					B	-	-	-
11.4.4. Video Teleconference	-					B	-	-	-
11.4.5. Topologies	-					B	-	-	-
11.4.6. Theory and Operation of Switching Devices (ATM, ISDN, GIG-E)	-					B	-	-	-
11.5. Networking Models									
11.5.1. Connection Oriented Communication	-					B	-	-	-
11.5.2. Connectionless Oriented Communication	-					B	-	-	-
11.5.3. International Standards Organization (ISO) Open Systems Interconnect (OSI) Model	-					B	-	-	-
11.5.4. Protocol Data Units	-					B	-	-	-
11.6. Network Management and Security									
11.6.1. Network Management Concepts and Responsibilities	-					B	-	-	-
11.6.2. Infectious and Malicious Software	-					B	-	-	-
11.6.3. Cyber Threats and Vulnerabilities	-					B	-	-	-
11.6.4. Vulnerability Preventative Measures	-					B	-	-	-
11.6.5. Identity Management	-					B	-	-	-
11.6.6. Wireless Network Security	-					B	-	-	-
11.7. Local Area Network Cabling and Switching									
11.7.1. Wired (LAN, WAN, MAN)	-					B	-	-	-
11.7.2. Theory and Operation of Switching Devices (ATM, ISDN, GIG-E)	-					B	-	-	-
11.7.3. Network Devices									
11.7.3.1. Modems	-					B	-	-	-
11.7.3.2. Converters	-					B	-	-	-
11.7.3.3. Gateways	-					B	-	-	-
11.7.3.4. Switches	-					B	-	-	-
11.7.3.5. Multiplexers	-					B	-	-	-
11.7.3.6. Bridges/Routers	-					B	-	-	-
11.7.3.7. Encryption Devices	-					B	-	-	-
11.7.4. Communications Mediums	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
11.7.5. LAN Architecture	-					B	-	-	-
11.7.6. Media Access Control Protocols	-					B	-	-	-
11.7.7. Packet Switched Networks	-					B	-	-	-
11.7.8. Circuit Switched Networks	-					B	-	-	-
11.7.9. Transmission methods and Medium	-					B	-	-	-
11.7.10. Inter-Networking	-					B	-	-	-
11.7.11. Intra-Networking	-					B	-	-	-
11.8. Internet Protocol Addressing and Routing									
11.8.1. Bridges/Routers	-					B	-	-	-
11.8.2. Network Addressing	-					B	-	-	-
11.8.3. Data-Link Layer									
11.8.3.1. Media Access Control (MAC)									
11.8.3.1.1. Address Structure	-					B	-	-	-
11.8.3.1.2. Ethernet Frame Structure	-					B	-	-	-
11.8.4. Network Layer									
11.8.4.1. Internet Protocol (v4 & v6)									
11.8.4.1.1. Address Structure	-					B	-	-	-
11.8.4.1.2. Packet Structure	-					B	-	-	-
11.8.4.1.3. Classful	-					B	-	-	-
11.8.4.1.4. Classless	-					B	-	-	-
11.8.4.1.5. Private/Public	-					B	-	-	-
11.8.4.1.6. Perform IPv4 Subnetting	-					B	-	-	-
11.8.4.1.7. IPv6 Subnetting	-					B	-	-	-
11.8.4.1.8. Supernetting	-					B	-	-	-
11.8.5. Routing Protocols									
11.8.5.1. Interior	-					B	-	-	-
11.8.5.2. Exterior	-					B	-	-	-
11.8.5.3. Link-state	-					B	-	-	-
11.9. Transport and Application Layer Protocols									
11.9.1. Physical and Logical Topology									
11.9.1.1. Bus	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
11.9.1.2. Star	-					B	-	-	-
11.9.1.3. Mesh	-					B	-	-	-
11.9.1.4. Hybrid	-					B	-	-	-
11.9.1.5. Media Access Control Protocols	-					B	-	-	-
11.10. Wide Area Network Fundamentals	-					B	-	-	-
11.11. Wireless Network Fundamentals									
11.11.1. Fundamentals									
11.11.1.1. Topology	-					B	-	-	-
11.11.1.2. Components	-					B	-	-	-
11.11.1.3. Security	-					B	-	-	-
11.11.2. Manipulate Wireless Access Point									
11.11.2.1. Connectivity	-					B	-	-	-
11.11.2.2. Security	-					B	-	-	-
11.12. Perform Command-Line Interfacing and Network Configurations									
11.12.1. Network Fault Isolation Techniques									
11.12.1.1. Perform Network Error Detection	-					2b	-	-	-
11.12.1.2. Perform Network Error Correction	-					2b	-	-	-
11.12.1.3. Describe Network Flow Control	-					2b	-	-	-
11.12.1.4. Identify Transmission Impairments	-					2b	-	-	-
11.12.1.5. Network management Concepts and Responsibilities	-					2b	-	-	-
11.12.2. Cisco Router and Switch									
11.12.2.1. Navigate Cisco IOS command line interface	-					2b	-	-	-
11.12.2.2. Configure Cisco Device Security IAW Applicable STIG	-					2b	-	-	-
11.12.2.3. Manipulate Networking Devices									
11.12.2.3.1. Interface Address	-					2b	-	-	-
11.12.2.3.2. VLAN	-					2b	-	-	-
11.12.2.3.3. Routing Protocol	-					2b	-	-	-
11.12.2.4. Enumerate Configuration and Connected Devices	-					2b	-	-	-
11.12.2.5. Utilize MAC Table	-					2b	-	-	-
11.12.2.6. Copy Device Configuration	-					2b	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
11.12.2.7. Erase Device Configuration	-					2b	-	-	-
11.12.2.8. Implement Access Control List	-					2b	-	-	-
11.12.2.9. Implement Port Security	-					2b	-	-	-
11.12.2.10. Configure Port Mirroring	-					2b	-	-	-
11.12.2.11. Copy System Image	-					2b	-	-	-
11.12.2.12. Enable Secure Remote Configuration Access	-					2b	-	-	-
11.13. Network Address Translation	-					B	-	-	-
12. WINDOWS OPERATING SYSTEMS TR: AF e-Learning site; Microsoft Windows 7 Learning Track									
12.1. Windows Operating System Family	-					B	-	-	-
12.2. Windows Kernel	-					B	-	-	-
12.3. Windows Boot Process	-					B	-	-	-
12.4. Windows File System Structure									
12.4.1. FAT	-					B	-	-	-
12.4.2. NTFS	-					B	-	-	-
12.5. Windows Networking									
12.5.1. Network Shares	-					B	-	-	-
12.5.2. Network Settings	-					B	-	-	-
12.6. Windows System Programs	-					B	-	-	-
12.7. Windows Application Programs	-					B	-	-	-
12.8. Windows Authentication	-					B	-	-	-
12.9. Perform Windows Command Line Commands	-					2b	-	-	-
12.10. Windows Memory Management	-					B	-	-	-
12.11. Windows Server 2008	-					B	-	-	-
12.12. NT File System (NTFS)	-					B	-	-	-
12.13. Local Account Management									
12.13.1. User Accounts	-					B	-	-	-
12.14. Security ID Numbers	-					B	-	-	-
12.15. Authentication Protocols	-					B	-	-	-
12.16. Kerberos	-					B	-	-	-
12.17. NT LAN Manager (NTLM)	-					B	-	-	-
12.18. Windows Registry									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
12.18.1. Utilize Registry	-					B	-	-	-
12.19. IIS Logging	-					B	-	-	-
12.20. Snapshot Contents	-					B	-	-	-
12.21. Snapshots via Batch Scripting	-					B	-	-	-
12.22. Windows Change Detection and Analysis	-					B	-	-	-
13. MOBILE OPERATING SYSTEMS									
14. VIRTUAL ENVIRONMENTS									
14.1. Definition & Uses	-					B	-	-	-
14.2. Types of Virtual Machines									
14.2.1. Virtual Desktop/Thin-Client Workstation Technology	-					B	-	-	-
14.2.2. Citrix Terminology/Product	-					B	-	-	-
14.3. VMWare Terminology/Products	-					B	-	-	-
14.4. Microsoft Terminology/Products	-					B	-	-	-
14.5. Virtual Networking	-					B	-	-	-
14.6. Virtual Storage	-					B	-	-	-
14.7. Virtual Security	-					B	-	-	-
14.8. Editing VM Configuration Files	-					B	-	-	-
14.9. Licensing	-					B	-	-	-
14.10. Installation, Setup, Booting and Controlling	-					2b	-	-	-
15. PROGRAMMING CONCEPTS AND SCRIPTING									
15.1. Problem Solving with Programming	-					B	-	-	-
15.2. Planning, Flowcharts, Pseudo code	-					B	-	-	-
15.3. Compiler/Interpreter	-					B	-	-	-
15.4. Libraries	-					B	-	-	-
15.5. Procedures, Loops, Functions	-					B	-	-	-
15.6. Variables	-					B	-	-	-
15.7. Compile/Debug	-					2b	-	-	-
15.8. Intro to C	-					B	-	-	-
15.9. Intro to Python									
15.9.1. Create Python Script	-					B	-	-	-
15.10. Intro to PERL	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
15.11. Scripting Lab	-					1a	-	-	-
16. PROJECT MANAGEMENT TR: AFIs 33-150, 36-2201, 63-501, 64-102; AFPD 36-5, 64-1; Federal Acquisition Regulation (FAR) Part 39; OMB Circular A-130; TO MPTOs 00-33A-1001-WA-1, 00-33D-3003-WA-1									
16.1. Foundational Concepts									
16.1.1. Principles of Project Managements	-					B	-	-	-
16.1.2. Complete AF e-Learning 3DXXX Project Management Training Track TR: https://www.my.af.mil (under AF e-Learning site)	-					B	-	-	-
16.1.3. Responsibilities in Project Management	-					B	-	-	-
16.1.4. Architecture TR: AFPD 33-1; AFIs 33-108, 33-210, 33-401; AFPD 33-4; CJCSI 6212.01; C4ISRDODAF 4630.8; GIG/CRD; MPTOs 00-33A-1001-WA-1, 00-33D-2002-WA-1									
16.1.4.1. Architecture Purpose	-					B	-	-	-
16.1.5. Cyberspace Systems Integrator (CSI) Concept TR: MPTO 00-33D-2002	-					B	-	-	-
16.2. Cyberspace Infrastructure Planning System TR: MPTO 00-33A-1001-WA-1, 00-33D-2002-WA-1, 00-33D-3003-WA-1, 00-33D-3004-WA-1; AFPD 33-1									
16.2.1. Purpose	-					B	-	-	-
16.2.2. Process	-					B	-	-	-
16.2.3. Maintain CIPS Visualization Components	-					B	-	-	-
16.2.4. Track Project in CIPS	-					B	-	-	-
16.2.5. CIPS CVC tool	-					B	-	-	-
16.2.6. Legacy CSIRs	-					B	-	-	-
16.3. Requirements and Work Order Management TR: AFPDs 10-6 and 33-1; AFIs 10-601; MPTOs 00-33A-1001-WA-1, 00-33D-3003-WA-1, 00-33D-3004-WA-1									
16.3.1. Site Surveys	-					B	-	-	-
16.3.2. IT Requirements									
16.3.2.1. Lifecycle	-					B	-	-	-
16.3.2.2. Procurement	-					B	-	-	-
16.3.2.3. Integrated Technical Reference Model (i-TRM)	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
16.3.3. Plans Management TR: AFPDs 10-4, 10-5; AFIs 10-402, 10-403, 10-404, 10-501, 25-101, 10-201; MPTO 00-33A-1001-WA-1									
16.3.3.1. Types of Plans									
16.3.3.1.1. Purpose	-					B	-	-	-
16.3.3.1.2. Content	-					B	-	-	-
16.3.3.1.3. Develop Plans Annex	-					B	-	-	-
16.3.3.2. IT/NSS Point of Contact (POC) for Plans									
16.3.3.2.1. Evaluate Plans to Determine IT/NSS Resource Impact	-					B	-	-	-
16.3.3.2.2. Administratively Manage Plans	-					B	-	-	-
16.4. Special Requirements									
16.4.1. Request Combat Communications Support	-					B	-	-	-
16.4.2. Circuit Requests									
16.4.2.1. Request for Service (RFS) (e.g. DISA web order entry)	-					B	-	-	-
16.4.2.2. Delayed Service Report	-					B	-	-	-
16.4.2.3. Completion Report	-					B	-	-	-
16.4.2.4. Connection Approval	-					B	-	-	-
16.4.2.5. Host Nation Approval TR: Local Procedures	-					B	-	-	-
16.4.3. IT/NSS Contracts TR: AFPD 33-1									
16.4.3.1. Purpose	-					B	-	-	-
16.4.3.2. Content	-					B	-	-	-
16.4.3.3. Validate Technical Solutions Against Applicable Contracts	-					B	-	-	-
16.4.3.4. Commercial Off-the-Shelf (COTS) (GSA, DoD, Contracts, 1218)	-					B	-	-	-
16.4.3.5. Government Off-the-Shelf (GOTS)	-					B	-	-	-
16.4.4. Administrative Contract Management TR: Federal Acquisition Regulation (FAR)									
16.4.4.1. Establishing and Managing a Contract	-					B	-	-	-
16.4.4.2. Types of Contracts									
16.4.4.2.1. Time and Material	-					B	-	-	-
16.4.4.2.2. Firm Fixed Price	-					B	-	-	-
16.4.4.2.3. Sole Source	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
16.4.4.2.4. Performance Based	-					B	-	-	-
16.4.4.2.5. Indefinite Delivery Indefinite Quantity	-					B	-	-	-
16.4.4.2.6. Blanket Purchase Agreement (e.g. AFWAY, PCOE)	-					B	-	-	-
16.4.4.3. Responsibilities									
16.4.4.3.1. Quality Assurance Program Coordinator	-					B	-	-	-
16.4.4.3.2. Functional Director/Commander	-					B	-	-	-
16.4.4.3.3. Quality Assurance Personnel	-					B	-	-	-
16.4.4.3.4. Unit Contract Monitor	-					B	-	-	-
16.5. Management Phases									
16.5.1. Risk Identification TR: AFPAM 90-902; OMB Circular No. A-130; MPTO 00-33A-1001-WA-1									
16.5.1.1. Technical Solutions	-					B	-	-	-
16.5.1.2. Identify Provisions for Logistic Support	-					B	-	-	-
16.5.1.3. Types (ICD, CDDP-Plan, etc.)	-					B	-	-	-
16.6. Management Meetings TR: AFPD 33-1; AFI 33-101; T.O. 00-33D-3003-WA-1									
16.6.1. Types	-					B	-	-	-
16.6.2. Impacts	-					B	-	-	-
16.7. Implementation									
16.7.1. Liaison with Base Agencies	-					B	-	-	-
16.7.2. Support Documentation	-					B	-	-	-
16.7.3. Project Material	-					B	-	-	-
16.7.4. Integrated Logistics Support Completion	-					B	-	-	-
16.7.5. Implementation Support									
16.7.5.1. Focal Point for Implementation Teams	-					B	-	-	-
16.7.5.2. Project Monitor Responsibilities	-					B	-	-	-
16.7.6. Support Agreements									
16.7.6.1. Characteristics and Responsibilities Concerning Support Agreements, Memorandums of Agreement and Memorandums of Understanding	-					B	-	-	-
16.7.6.2. Scheduling Management	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
16.7.6.3. Critical Path	-					B	-	-	-
16.7.6.4. Project Support Requirements	-					B	-	-	-
16.7.6.5. Host Nation/Federal/State/Local Requirements/Coordination	-					B	-	-	-
16.8. MILCON & CE									
16.8.1. Base Civil Engineer (BCE) Interface TR: AFIs 32-1001, 32-1021, 32-9002; AFPD 32-90; MPTO 00-33A-1001-WA-1									
16.8.1.1. Unit Focal Point Responsibilities	-					B	-	-	-
16.8.2. Military Construction Program (MCP) TR: EIA/TIA 568A, 569A, 606, 607, ETL 02-12	-					B	-	-	-
16.9. System Installation Records TR: AFPD 33-1, AFIs 33-580, 10-601, MPTOs 00-33A-1001-WA-1, 00-33D-3003-WA-1, 00-33D-3004-WA-1									
16.9.1. Purpose	-					B	-	-	-
16.9.2. Content	-					B	-	-	-
16.9.3. Responsibilities									
16.9.3.1. Base IT/NSS Installation Records Manager	-					B	-	-	-
16.9.3.2. Work Centers	-					B	-	-	-
16.9.4. Drawing Records									
16.9.4.1. Processing	-					B	-	-	-
16.9.4.2. Reviews	-					B	-	-	-
16.9.4.3. Index	-					B	-	-	-
16.9.5. System Accreditation	-					B	-	-	-
16.10. Project Acceptance									
16.10.1. Agreements TR: AFIs 25-201, 33-114 (v1); AFPD 25-2; DoDI 4000.19; MPTO 00-33A-1001-WA-1									
16.10.1.1. Purpose	-					B	-	-	-
16.10.1.2. Types	-					B	-	-	-
16.10.1.3. Content	-					B	-	-	-
16.10.2. Modification Management									
16.10.2.1. Control Configuration	-					B	-	-	-
16.10.2.2. Initiate Modification Proposals TR: AFI 63-131	-					B	-	-	-
16.10.3. Schedule Systems Acceptance Inspections	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
16.10.4. Material Accountability	-					B	-	-	-
16.10.5. Material Disposition	-					B	-	-	-
16.10.6. Real Property Transfer	-					B	-	-	-
16.10.7. Acceptance Documentation	-					B	-	-	-
16.11. Project Folders									
16.11.1. Project/Program Documentation	-					B	-	-	-
16.11.2. Project Documentation Content	-					B	-	-	-
16.11.3. Project Documentation Review	-					B	-	-	-
16.11.4. IT/NSS Documentation TR: AFPD 33-1; AFIs 33-580, 10-601									
16.11.4.1. Purpose	-					B	-	-	-
16.11.4.2. Content	-					B	-	-	-
16.11.4.3. Develop IT/NSS Requirement Document	-					B	-	-	-
16.11.4.4. Process IT/NSS Requirements	-					B	-	-	-
17. NETWORK WARFARE CONCEPTS TR: AFTTP 3-1.CWO; AFDD 3-12; AFPD 10-17; AFI 10-1701, 33-150; CJCSM 6510.01B; JP 3-12									
17.1. Terms and Definitions									
17.1.1. Network Warfare Fundamentals									
17.1.1.1. Control Systems (e.g. Supervisory Control and Data Acquisition (SCADA) Networks)	-					B	-	-	-
17.1.1.2. Identify Tactical Data Link (TADL) Networks	-					B	-	-	-
17.1.1.3. Network Exploitation Capabilities	-					B	-	-	-
17.2. Roles and Responsibilities									
17.2.1. Cyber Capabilities									
17.2.1.1. Effects on Adversary Decision Makers	-					B	-	-	-
17.2.1.2. Role of Cyber Operations in Achieving Military and National Goals and Objectives	-					B	-	-	-
17.2.1.3. Information Superiority	-					B	-	-	-
17.2.1.4. 624th Operations Center Role	-					B	-	-	-
17.2.1.5. Role of Integrated Network Operations and Security Centers (I-NOSC)	-					B	-	-	-
17.2.1.6. Role of Network Control Centers (NCC)	-					B	-	-	-
17.2.1.7. Air Operations Center (AOC) Role	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
17.2.1.8. Ops Defensive Measures	-					B	-	-	-
17.2.1.9. Ops Capabilities	-					B	-	-	-
17.2.1.10. Checklists, Standard Operating Procedures (SOP), Tactics, Techniques and Procedures (TTP)	-					B	-	-	-
17.2.2. Crew Operations									
17.2.2.1. Operations Training	-					B	-	-	-
17.2.2.2. Standardization and Evaluation	-					B	-	-	-
17.2.2.3. Operational Procedures	-					B	-	-	-
17.2.2.4. Crew Resource Management	-					B	-	-	-
17.3. Area of Responsibility (AOR)	-					B	-	-	-
17.4. Hacker Methodology									
17.4.1. OCO/DCO Theory and Methodology									
17.4.1.1. Offensive Theory	-					B	-	-	-
17.4.1.2. Defensive Theory	-					B	-	-	-
17.4.1.3. Offensive Methodology	-					B	-	-	-
17.4.1.4. Defensive Methodology	-					B	-	-	-
17.5. Capabilities & Weapon Systems									
17.5.1. Workstations/Servers	-					B	-	-	-
17.5.2. Data Networks	-					B	-	-	-
17.5.3. Voice Networks	-					B	-	-	-
17.5.4. Space Networks	-					B	-	-	-
17.5.5. Battlefield Networks	-					B	-	-	-
17.5.6. Industrial Systems	-					B	-	-	-
17.5.7. AFNET	-					B	-	-	-
17.5.8. Websites/Databases	-					B	-	-	-
17.6. Tactics, Techniques and Procedures									
17.6.1. Joint Planning TR: JP 1-0; JP 2-0; JP 5-0; JP 3-12; CJCSM 3122.07 Vol I/II									
17.6.1.1. Lines of Operations									
17.6.1.1.1. DoDIN	-					B	-	-	-
17.6.1.1.2. DCO	-					B	-	-	-
17.6.1.1.3. OCO	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
17.6.1.2. Joint Command and Planning Process									
17.6.1.2.1. Structure and Organization	-					B	-	-	-
17.6.1.2.2. Levels of War	-					B	-	-	-
17.6.1.2.3. Roles and Responsibilities	-					B	-	-	-
17.6.1.3. Command and Control (C2)	-					B	-	-	-
17.6.1.4. Authorities	-					B	-	-	-
17.6.1.5. Orders	-					B	-	-	-
17.6.1.6. Planning Process Defined (JOPP)									
17.6.1.6.1. Deliberate Planning	-					B	-	-	-
17.6.1.6.2. Crisis Action Planning	-					B	-	-	-
17.6.1.7. Integrated Joint Special Technical Operations (IJSTO)									
17.6.1.7.1. Process	-					B	-	-	-
17.6.1.7.2. Roles and Responsibilities	-					B	-	-	-
17.7. Capabilities and Vectors	-					B	-	-	-
17.8. Plan, Brief, Execute & Debrief Process									
17.8.1. Conduct OCO and DCO Mission Planning	-					B	-	-	-
17.9. Measure of Effectiveness/Performance									
17.9.1. MOP/MOE	-					B	-	-	-
17.10. Intelligence and Technical Gain/Loss									
17.10.1. Intelligence Gain/Loss	-					B	-	-	-
17.10.2. Technical Gain/Loss	-					B	-	-	-
17.11. Operations and Resource Management									
17.11.1. Crew Resource Management	-					B	-	-	-
17.12. Platform Defensive Measures									
17.12.1. Identify Defensive Methods									
17.12.1.1. Encryption	-					B	-	-	-
17.12.1.2. Secure Configurations	-					B	-	-	-
17.12.1.3. Secure Enclaves	-					B	-	-	-
17.12.1.4. Vulnerability Scanning	-					B	-	-	-
17.12.1.5. Boundary Protection	-					B	-	-	-
17.12.1.6. Intrusion Detection/Pretention (Host/Network)	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
17.13. Network Operations Orders	-					B	-	-	-
17.14. Perform Targeting									
17.14.1. Asset/Target Analysis	-					2b	-	-	-
17.15. Perform Operational Analysis									
17.15.1. Conducting Ops Assessment	-					2b	-	-	-
18. GOVERNANCE, LAW, ETHICS TR: AFDD 3-13; AFPD 10-7; AFPD 10-17; USC Title 10, 17, 18, 50; JP 3-13, 3-12									
18.1. Federal Acts									
18.1.1. US Codes (Titles 10, 14,15, 17, 18, 32, 50)	-					B	-	-	-
18.1.2. US Telecommunications Laws	-					B	-	-	-
18.2. Law of Armed Conflict									
18.2.1. LOAC Limitation Principles in Conducting Cyber Operations	-					B	-	-	-
18.3. Uniform Code of Military Justice	-					B	-	-	-
18.4. Domestic Law, Policy and Rules of Engagement									
18.4.1. Rules of Engagement (ROE)									
18.4.1.1. Policy	-					A	-	-	-
18.4.1.2. Security Tools	-					A	-	-	-
18.4.1.3. Cyber Management Ethics	-					A	-	-	-
18.4.2. Special Data Protection (i.e. Sensitive Personnel Information)	-					A	-	-	-
18.4.3. Executive Orders	-					A	-	-	-
18.4.4. US Law									
18.4.4.1. Intellectual Property Laws	-					A	-	-	-
18.4.4.2. US Law Specific to Electronic Crimes	-					A	-	-	-
18.5. International Legal Considerations									
18.5.1. International Laws Affecting Electronic Communications	-					A	-	-	-
18.6. Federal Agencies	-					-	-	-	-
18.7. Laws and Ethics	-					A	-	-	-
18.8. Legal Rights	-					B	-	-	-
18.9. Consent to Monitoring									
18.9.1. System Monitoring	-					B	-	-	-
18.10. Military Cyberspace Implications	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
18.11. Cyberspace Operations Law	-					B	-	-	-
18.12. Regulations for the Networking Environment	-					B	-	-	-
18.13. Air Force Instructions	-					B	-	-	-
19. AIR FORCE INFORMATION NETWORK (AFIN) ARCHITECTURE									
19.1. Network Management Functions	-					B	-	-	-
19.2. Network Services	-					B	-	-	-
19.3. Operate Administrative Tools	-					2b	-	-	-
19.4. Perform Network Management	-					2b	-	-	-
19.5. Perform Security Measures & Defense	-					2b	-	-	-
19.6. Perform Network Simulations and Configurations	-					2b	-	-	-
20. ADVANCED NETWORKING									
20.1. Identify IP Packet Generation/Flags	-					2b	-	-	-
20.2. Identify TCP Packet Generation/Flags	-					2b	-	-	-
20.3. Demonstrate Encapsulation/Fragmentation									
20.3.1. Encapsulation/Decapsulation	-					2b	-	-	-
20.4. Identify Internet Control Message Protocol (ICMP)	-					2b	-	-	-
20.5. Establish Maintain and Close TCP Connections	-					2b	-	-	-
21. PACKET/TRAFFIC ANALYSIS									
21.1. Normal Traffic Header/Payloads									
21.1.1. Fundamentals	-					B	-	-	-
21.2. Abnormal Traffic									
21.2.1. Network Traffic Analysis Process									
21.2.1.1. Capture Traffic	-					B	-	-	-
21.2.1.2. Analyze Traffic	-					B	-	-	-
21.2.1.3. Implement Session Recovery from Raw Traffic	-					B	-	-	-
21.2.1.4. Identify Encoded Traffic	-					B	-	-	-
21.2.1.5. Identify Malicious Traffic	-					B	-	-	-
21.2.1.6. Identify from Network Traffic the Hardware Manufacturer	-					B	-	-	-
21.2.1.7. Identify from Network Traffic the OS Version	-					B	-	-	-
21.2.1.8. Identify from Network Traffic Patch Release of OS Software	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
21.2.1.9. Identify Services and Applications on a Network	-					B	-	-	-
21.3. Anomalous - Benign	-					B	-	-	-
21.4. Malicious Traffic (Beaconing, Spearfishing, Exfil, Worm, and EXE)	-					B	-	-	-
21.5. Deep vs. Shallow Packet Inspection	-					B	-	-	-
21.6. Stateful Inspection	-					B	-	-	-
21.7. Behavioral Traffic Analysis within the AFNET	-					B	-	-	-
22. OFFENSIVE CYBERSPACE OPERATIONS (OCO) TR: AFTTP 3-1.CWO; AFDD 3-12; AFPD 10-17; AFI 31-401; JP 1-02; JP 3-12									
22.1. Perform Nodal Analysis	-					2b	-	-	-
22.2. Perform OCO Mission Planning	-					2b	-	-	-
22.3. Employ Mission Execution									
22.3.1. Identify Offensive Methods									
22.3.1.1. Buffer Overflow Tactics and Techniques	-					2b	-	-	-
22.3.1.2. Privilege Escalation	-					2b	-	-	-
22.3.1.3. Rootkits	-					2b	-	-	-
22.3.1.4. Redirection, Triggering, and Exfiltration	-					2b	-	-	-
22.3.1.5. Social Engineering	-					2b	-	-	-
22.3.1.6. Persistent Access	-					2b	-	-	-
22.3.1.7. Man-in-the-Middle	-					2b	-	-	-
22.3.1.8. (Distributed) Denial of Service	-					2b	-	-	-
22.3.1.9. Obfuscation	-					2b	-	-	-
22.3.2. Generate a Deny, Degrade, Disrupt, Destroy, or Deceive Effect									
22.3.2.1. Workstations/Servers	-					2b	-	-	-
22.3.2.2. Data Networks	-					2b	-	-	-
22.3.2.3. Voice Networks	-					2b	-	-	-
22.3.2.4. Wireless Networks	-					2b	-	-	-
22.3.2.5. Websites/Databases	-					2b	-	-	-
22.3.2.6. Space Networks	-					2b	-	-	-
22.3.2.7. Battlefield Networks	-					2b	-	-	-
22.3.2.8. Industrial Systems	-					2b	-	-	-
22.4. Prepare and Present OCO Mission Debrief	-					2b	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
22.5. Prepare and Present a Master Station Log Brief	-					2b	-	-	-
23. MOBILE NETWORKS									
23.1. Attack & Exploit Methods	-					B	-	-	-
23.2. Perform Mobile Mission Planning	-					2b	-	-	-
23.3. Execute Mobile Mission	-					2b	-	-	-
23.4. Prepare and Present Mobile Mission Debrief	-					2b	-	-	-
23.5. Defense-in-Depth	-					B	-	-	-
24. NETWORK THREATS AND DEFENSE									
24.1. Operate and manage Incident Prevention, Detection, Response and Handling	**-**					2b	**-**	**-**	**-**
24.2. Current Cyber Threats and Attacks									
24.2.1. Threat Types									
24.2.1.1. Internal	**-**					B	**-**	**-**	**-**
24.2.1.2. External	**-**					B	**-**	**-**	**-**
24.2.1.3. State Sponsored	**-**					B	**-**	**-**	**-**
24.2.1.4. Non-State Sponsored	**-**					B	**-**	**-**	**-**
24.3. Cyber Network Defensive Strategies and TTPs	**-**					B	**-**	**-**	**-**
24.4. Intel Support to Cyber Warfare									
24.4.1. Intelligence Sources	**-**					B	**-**	**-**	**-**
24.4.2. Intelligence Reports	**-**					B	**-**	**-**	**-**
24.4.3. Tactics from Intel Sources	**-**					B	**-**	**-**	**-**
24.5. Execute a Network Defense Mission	**-**					2b	**-**	**-**	**-**
24.6. Prepare and Present Network Defense Mission Debrief	**-**					2b	**-**	**-**	**-**
25. MITIGATING THREATS									
25.1. Virus and Spyware Management Program	-					B	-	-	-
25.2. Browser Security	-					B	-	-	-
25.3. Social Engineering Threats	-					B	-	-	-
26. CRYPTOGRAPHY & AUTHENTICATION									
26.1. Symmetric Cryptography	-					B	-	-	-
26.2. Asymmetric Cryptography	-					B	-	-	-
27. AUTHENTICATION METHODS									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
27.1. Authentication	-					B	-	-	-
27.2. Hashing	-					B	-	-	-
28. MESSAGING SECURITY									
28.1. E-mail Security	-					B	-	-	-
28.2. Messaging and Peer-to-Peer Security	-					B	-	-	-
29. USER AND ROLE-BASED SECURITY									
29.1. Security Policies	-					B	-	-	-
29.2. Securing File and Print Resources	-					B	-	-	-
30. PUBLIC KEY INFRASTRUCTURE									
30.1. Key Management and Life Cycle	-					B	-	-	-
30.2. Certificate Server Setup	-					B	-	-	-
30.3. Web Server Security with PKI	-					B	-	-	-
31. ACCESS SECURITY									
31.1. Biometric Systems	-					B	-	-	-
31.2. Physical Access Security	-					B	-	-	-
31.3. Peripheral and Component Security	-					B	-	-	-
31.4. Storage Device Security	-					B	-	-	-
32. PORTS, PROTOCOLS, AND SERVICES									
32.1. TCP/IP Review									
32.1.1. TCP/IP Structure	-					B	-	-	-
32.2. Perform Protocol-based Attacks	-					2b	-	-	-
32.3. Common System Services	-					B	-	-	-
33. NETWORK SECURITY									
33.1. Common Network Devices	-					B	-	-	-
33.2. Secure network Topologies	-					B	-	-	-
33.3. Browser-related Network Security	-					B	-	-	-
33.4. Virtualization	-					B	-	-	-
34. WIRELESS SECURITY									
34.1. Non-PC Wireless Devices	-					B	-	-	-
35. REMOTE ACCESS SECURITY									
35.1. Perform Remote Access	-					2b	-	-	-
35.2. Operate Virtual Private Networks									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
35.2.1. Protocols	-					2b	-	-	-
35.2.2. Components	-					2b	-	-	-
36. AUDITING, LOGGING, AND MONITORING									
36.1. System Logging	-					B	-	-	-
36.2. Server Monitoring	-					B	-	-	-
37. ORGANIZATIONAL SECURITY									
37.1. Organizational Policies	-					B	-	-	-
37.2. Education and Training	-					B	-	-	-
37.3. Disposal and Destruction	-					B	-	-	-
38. BUSINESS CONTINUITY									
38.1. Redundancy Planning	-					B	-	-	-
38.2. Backups	-					B	-	-	-
38.3. Environmental Controls	-					B	-	-	-
39. TELEPHONY									
39.1. Design and Architecture	-					B	-	-	-
39.2. Manipulate Components and Configurations	-					2b	-	-	-
39.3. Attack, Exploit & Defensive Strategies	-					B	-	-	-
39.4. Perform Security Measures & Defense	-					2b	-	-	-
39.5. Perform Telephony Mission Planning	-					2b	-	-	-
39.6. Execute Telephony Mission	-					2b	-	-	-
39.7. Prepare and Present Telephony Mission Debrief	-					2b	-	-	-
39.8. Approved Products List	-					B	-	-	-
39.9. VTC	-					B	-	-	-
40. SPACE AND SATELLITE NETWORKS									
40.1. Design and Architecture	-					B	-	-	-
40.2. Components and Configurations	-					B	-	-	-
40.3. Commercial and MILSATCOM	-					B	-	-	-
40.4. GPS	-					B	-	-	-
40.5. National Technical Means	-					B	-	-	-
40.6. Attack, Exploit & Defensive Strategies	-					B	-	-	-
40.7. Security	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
41. INTEGRATED AIR DEFENSE (IADS) NETWORKS									
41.1. Design and Architecture	-					B	-	-	-
41.2. Components and Configurations	-					B	-	-	-
41.3. Attack, Exploit & Defensive Strategies	-					B	-	-	-
41.4. Perform Security Measures and Defense	-					2b	-	-	-
41.5. Perform IADS Mission Analysis	-					2b	-	-	-
41.6. Develop Defensive and Offensive Courses of Action	-					2b	-	-	-
41.7. Prepare and Present IADS C2 and TDL Mission Analysis Brief	-					2b	-	-	-
42. COMMAND & CONTROL (C2) AND TACTICAL DATA LINK (TDL) NETWORKS									
42.1. Design and Architecture	-					B	-	-	-
42.2. Components and Configurations	-					B	-	-	-
42.3. TACS	-					B	-	-	-
42.4. Attack, Exploit & Defensive Strategies	-					2b	-	-	-
42.5. Perform Security Measures & Defense	-					2b	-	-	-
42.6. Perform C2 & TDL Mission Analysis	-					2b	-	-	-
42.7. Develop Defensive and Offensive Courses of Action	-					2b	-	-	-
42.8. Prepare and Present C2 & TDL Mission Analysis Brief	-					2b	-	-	-
43. INDUSTRIAL CONTROL SYSTEMS									
43.1. Design and Architecture	-					B	-	-	-
43..2. Manipulate Components and Configurations	-					B	-	-	-
43.3. Attack, Exploit & Defensive Strategies	-					B	-	-	-
43.4. Perform Security Measures & Defense	-					2b	-	-	-
43.5. Perform ICS Mission Planning	-					2b	-	-	-
43.6. Execute an ICS Mission	-					2b	-	-	-
43.7. Prepare and Present ICS Mission Brief	-					2b	-	-	-
44. FIGHTING THROUGH A CYBER ATTACK (CAPSTONE)									
44.1. Plan Cyber Operations	-					2b	-	-	-
44.2. Attack Cyber Technologies	-					2b	-	-	-
44.3. Defend Networks and Systems	-					2b	-	-	-
44.4. Prepare and Present Mission Brief and Debrief	-					2b	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
45. COVERING YOUR TRACKS									
45.1 Demonstrate Hiding Files in Windows	-					2b	-	-	-
45.2. Demonstrate Windows Log Editing	-					2b	-	-	-
45.3. Demonstrate Alternate Data Streams in Windows	-					2b	-	-	-
45.4. Demonstrate Reverse WWW Shell	-					2b	-	-	-
45.5. Demonstrate ICMP Tunnels	-					2b	-	-	-
45.6. Demonstrate Covert TCP	-					2b	-	-	-
45.7. Demonstrate Sniffing Backdoors	-					2b	-	-	-
45.8. Demonstrate Steganography Methods	-					2b	-	-	-
46. OFFENSIVE OPERATIONS									
46.1. Special Access Programs (SAP)	-					B	-	-	-
46.2. Integrated Joint Special Technical Operations (IJSTO)	-					B	-	-	-
46.3. Execute O/S Attack Vectors	-					2b	-	-	-
46.4. Execute Virtual Environment Attack Vectors	-					2b	-	-	-
46.5. Unified and Battlefield Systems Offensive Courses of Action	-					B	-	-	-
47. FORENSICS									
47.1. Forensic Methodology	-					B	-	-	-
47.2. Media Analysis	-					B	-	-	-
47.3. Reporting Process	-					B	-	-	-
47.4. Digital Forensics Fundamentals	-					B	-	-	-
48. DEFENSIVE OPERATIONS									
48.1. Unified and Battlefield Systems Defensive COAs									
48.1.1. Incident Response TR: AFTTP 3-1.CWO; AFDD 3-12; AFPD 10-17; AFI 31-401; JP 1-02; JP 3-12									
48.1.1.1. Methodology	-					B	-	-	-
48.1.1.2. Incident Categories	-					B	-	-	-
48.1.1.3. Remote Evidence Collection	-					B	-	-	-
48.1.1.4. Reporting	-					B	-	-	-
48.1.1.5. Forensics	-					B	-	-	-
48.1.1.6. Conduct Investigation	-					B	-	-	-
48.1.1.7. Incident Recovery	-					B	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
48.2. Execute DCO Mission	-					2b	-	-	-
49. CAPABILITY DEVELOPMENT TR: AFTTP 3-1.CWO; AFDD 3-12; AFPD 10-17; AFI 31-401; JP 1-02; JP 3-12									
49.1. Fundamentals	-					-	-	-	-
49.2. Secure Programming	-					-	-	-	-
49.3. Agile Development Process	-					-	-	-	-
49.4. Reverse Engineering	-					-	-	-	-
49.5. Weaponization	-					-	-	-	-
49.6. Provisioning	-					-	-	-	-
49.7. Operational Frameworks	-					-	-	-	-
49.8. Functional Evaluation Fundamentals	-					-	-	-	-
49.9. Fuzzing Fundamentals	-					-	-	-	-
49.10. Real-Time Operations and Innovation	-					-	-	-	-
50. WORK CENTER MANAGEMENT TR: AFI 21-103									
50.1. Management Policies									
50.1.1. Report Resources Status	-					-	-	-	-
50.1.2. Document Actions	-					-	-	-	-
50.1.3. Equipment Readiness	-					-	-	-	-
50.1.4. Staffing and Utilization	-					-	-	-	-
50.2. Quality Assurance (QA)									
50.2.1. Describe the QA Function	-					-	-	-	-
50.3. Air Force Inspection System (AFIS) TR: AFI 90-201, MPTO 00-33A-1001-WA-1									
50.3.1. Consolidated Unit Inspection (CUI)	-					-	-	-	-
50.3.2. Self-Assessment Program									
50.3.2.1. Work Center Role	-					-	-	-	-
50.3.2.2. QA Role	-					-	-	-	-
50.3.2.3. Self-Assessment Checklists (SACS)	-					-	-	-	-
50.3.2.4. Management Internal Control Toolset (MICT)	-					-	-	-	-
50.3.2.5. Perform Self-Assessment	-					-	-	-	-
50.4. Automated Information System									
50.4.1. Integrated Maintenance Data System (IMDS)	-					-	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
50.4.2. Remedy	-					-	-	-	-
50.4.3. Air Force Equipment Management System-Asset Inventory Management System (AFEMS-AIM)	-					-	-	-	-
51. RESOURCE MANAGEMENT TR: AFPDs 16-5, 33-1, 10-6, 65-6; AFIs 16-501, 10-601, 65-601 (v3)									
51.1. Financial Management									
51.1.1. Principles of Financial Management	-					-	-	-	-
51.1.2. Program Objective memorandum (POM) Cycle	-					-	-	-	-
51.1.3. Government Purchase Card Program Oversight	-					-	-	-	-
51.1.4. Shortfall Procedures	-					-	-	-	-
51.2. Funded Requirements									
51.2.1. Responsibilities	-					-	-	-	-
51.2.2. Funding Process	-					-	-	-	-
51.3. Unfunded Requirements									
51.3.1. Responsibilities	-					-	-	-	-
51.3.2. Funding Process	-					-	-	-	-
51.3.3. Develop Requirements	-					-	-	-	-
51.4. Funding Types	-					-	-	-	-
51.5. Primary and Alternate Funding Sources	-					-	-	-	-
51.6. Financial Planning (FINPLAN)	-					-	-	-	-
52. MANPOWER AND ORGANIZATION TR: AFPD 38-2, AFI 38-101, 38-201									
52.1. Manpower Requirements	-					-	-	-	-
52.2. Air Force Manpower Standard (AFMS) Application	-					-	-	-	-
52.3. Manpower Studies	-					-	-	-	-
52.4. Manpower Products									
52.4.1. Unit Manpower Document (UMD)	-					-	-	-	-
52.4.2. Authorization Change Request (ACR)	-					-	-	-	-
52.4.3. Organizational Change Request (OCR)	-					-	-	-	-
52.4.4. Program Element Code (PEC)	-					-	-	-	-
52.4.5. Unit Personnel Management Roster (UPMR)	-					-	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	2 SKILL LEVEL	3 SKILL LEVEL	Proficiency	Currency
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	IQT	MQT		
52.5. Allocating Personnel	-					-	-	-	-
52.6. Awards and Recognition									
52.6.1. Unit/Installation Awards	-					-	-	-	-
52.6.2. SAF/CIO Special Trophies and Awards TR: AFI 36-2845	-					-	-	-	-

Section E - Additional Information

1. Suggested Reading. This section contains references and a professional reading list for cyberspace operations officers. It is not all-inclusive; however, it covers the most frequently referenced areas. The selections contained in this list cover a wide variety of subjects ranging from Air Force classification instructions to the Chief of Staff of the Air Force reading list. Familiarity with the guidance and information contained in these publications will assist in the development of knowledge in cyberspace operations officers. For a current list of the available AFIs refer to the AF e-Publishing web site accessible via the AF Portal. The helpful links in blue (and underlined) are hyperlinked to the current website.

AFI 10-404, *Base Support and Expeditionary Site Planning.* Provides for the preparation of base support plans (BSP), and expeditionary site plans (ESP); and the accomplishment of contingency site surveys across the spectrum of USAF operations for deliberate, and crisis action planning (CAP), and execution. It describes the specific requirements to translate and integrate operational requirements into Agile Combat Support (ACS) at employment sites to create and sustain operations.

Air Force Officer Classification Directory (AFOCD). Describes the various officer specialties, the coding system used to differentiate them and the knowledge, education, training and experience requirements of each specialty. The AFOCD is accessible through myPers.

AFI 36-2101, *Classifying Military Personnel (Officer and Enlisted).* Implements classification procedures and related actions for Air Force officers and enlisted.

AFI 36-2110, *Assignments*. This instruction establishes criteria for assignment of military personnel to satisfy operational, rotational, and training (including formal education and professional military education/development) requirements to include temporary duty (TDY) and change of permanent duty station (PCS). It applies to all officers and enlisted personnel on extended active duty (EAD), but does not apply to members of the Air Force Reserve or Air National Guard.

AFI 36-2201, *Air Force Training Program*. Outlines career field management responsibilities, utilization and training workshop procedures, and construction and publishing of CFETPs.

AFI 36-2301, *Developmental Education.* Provides general information on developmental education.

AFI 36-2406, *Officer and Enlisted Evaluation Systems*. Assists raters and ratees in giving and receiving performance feedback and in preparing officer performance reports and promotion recommendation forms.

AFI 36-2501, *Officer Promotions and Selective Continuation*. States the procedures for promoting active duty officers below the grade of brigadier general. This document explains how the Air Force conducts selection boards and makes promotion selections.

AFI 36-2611, *Officer Professional Development*. Provides general information on professional development common to all officers.

Career Field Education and Training Plans (CFETP) for specialties within the 1BXXX, 3AXXX and 3DXXX enlisted career fields. These plans provide guidance for the planning, development, and life cycle training requirements for airmen within these communications specialties. It identifies mandatory skills airmen should obtain during their careers as communication professionals.

Air Force Senior Leadership Biographies. Reading senior leader biographies is the first step in becoming acquainted with senior leadership and their career paths. Of note is that although there are some commonalities in their career paths, no two senior leaders rose to their position following the same path.

Command and Control Research Program Publications. The Command and Control Research Program within the Office of the Assistant Secretary of Defense (NII) publishing books on command and control, lessons learned, military transformation, and many other subjects. These books are available to the public at no cost.

Cyberspace Officer Forum (choose email certificate). This SharePoint website is a forum for sharing information pertaining to the Cyberspace Operations Officer career field. This site includes pertinent information regarding force management and development topics, to include training, education and career broadening opportunities, as well as other cross-cutting issues.

Newton's Telecommunications Dictionary. Defines over 21,000 telecommunications terms and explains complex technology in non-technical business language. This is available online through the Books 24x7 link on the IT E-Learning site which is accessible via the AF Portal.

Other Suggested Readings: Air Force Communications and Electronics Association (AFCEA) Signal Magazine, Federal Computing Week and Association for Computing Machinery Monthly Magazine.

2. URL List. This section contains a URL list for Cyberspace officers. The URLs are imbedded into the titles (hyperlinked titles are in blue font and underlined). It is not all-inclusive; however, it covers the most frequently referenced areas. The list does not imply official Department of Defense or Department of the Air Force endorsement.

Air Command and Staff College (ACSC)

Air War College (AWC)

Air Force Education and Training Course Announcements (ETCA) Database

Air Force Institute of Technology (AFIT)

Armed Forces Communications and Electronics Association

(ACM) (offers a full and unlimited access to over 3,000 online courses available to ACM Professional and Student Members on a wide range of subjects from IT to Business).

Computer Based Training (“AF IT eLearning”)

Accessible only through the AF Portal

Defense Acquisition University (DAU)

DoD Issuances (DODD, DODI, DODM, DODR)

Education with Industry, AFI 36-2639

Enlisted Classification Directory (AFECD) (accessible through myPers)

Federal Acquisition Regulation (FAR)

Information Assurance Scholarship Program (IASP)

Institute of Electrical and Electronics Engineers

International Telecommunications Union (ITU) Regulations

Joint Electronic Library

National Intelligence University

National Defense University Information Resources Management College (iCollege)

Naval Postgraduate School (NPS)

NTIA Manual of Regulations & Procedures for Federal Radio Frequency Management

Safari Books Online

School of Advanced Air and Space Studies (SAASS)

Secretary of the Air Force, Chief of Information Dominance and Chief Information Officer Special Trophies and Awards, AFI 36-2845

Squadron Officer School (SOS)

3. Professional Societies.

3.1. This is list is not all-inclusive, nor does it imply official Department of Defense or Department of the Air Force endorsement.

3.2. Air Force C4 Association (AFC4A) is a non-profit organization whose objective and purpose is to serve two primary objectives: 1) to preserve and promote the camaraderie and the collegial relationship of all those who formerly served in the functional community of the U.S. Air Force commonly referred to as “command and control, communications and computer (C4)”; and 2) to promote the well-being and the best interests of those currently and actively serving in the Air Force C4 community.

3.3. Air Force Association (AFA) is a non-profit, independent, professional military and aerospace education association promoting public understanding of aerospace power and the pivotal role it plays in the security of the nation. AFA publishes Air Force Magazine, conducts national symposia and disseminates information through outreach programs. It sponsors professional development seminars and recognizes excellence in the education and aerospace fields through national awards programs. AFA presents scholarships and grants to Air Force active duty, Air National Guard and Air Force Reserve members and their dependents; and awards educator grants to promote science and math education at the elementary and secondary school level.

3.4. Armed Forces Communications and Electronics Association (AFCEA). AFCEA is a 501(c)(6) non-profit international organization that serves its members by providing a forum for the ethical exchange of information. AFCEA is dedicated to increasing knowledge through the exploration of issues relevant to its members in information technology, communications, and electronics for the defense, homeland security and intelligence communities. A variety of courses are offered throughout the year at Fairfax VA as well as online. Check AFCEA's courses web site periodically for offerings.

3.5. Association for Computing Machinery is widely recognized as the premier membership organization for computing professionals, delivering resources that advance computing as a science and a profession; enable professional development; and promote policies and research that benefit society.

3.6. Association of Old Crows (AOC) is a not-for-profit international professional association with over 13,500 members and 180+ organizations engaged in the science and practice of Electronic Warfare (EW), Information Operations (IO), and related disciplines.

3.7. Institute of Electrical and Electronics Engineers (IEEE) is a non-profit association. It is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.

3.8. International Information Systems Security Certification Consortium (ISC)² is the global, not-for-profit leader in educating and certifying information security professionals throughout their careers.

3.9. Project Management Institute is the world's leading not-for-profit professional membership association for the project, program and portfolio management profession.