

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

CFETP 1B4X1
Parts I and II
15 July 2018

AFSC 1B4X1

CYBER WARFARE OPERATIONS



CAREER FIELD EDUCATION AND TRAINING PLAN

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

RELEASABILITY: There are no releasability restrictions on this publication.

**CAREER FIELD EDUCATION AND TRAINING PLAN
CYBER WARFARE OPERATIONS
AFSC 1B4X1**

TABLE OF CONTENTS

PART I

<u>Preface</u>	4
<u>Abbreviations/Terms Explained</u>	5
<u>Section A - General Information</u>	10
Purpose of the CFETP	
Use of the CFETP	
Coordination and Approval of the CFETP	
<u>Section B - Career Field Progression and Information</u>	12
Specialty Description	
Skill/Career Progression	
Cyber Warfare Operations Apprentice (1B431)	
Cyber Warfare Operations Journeyman (1B451)	
Cyber Warfare Operations Craftsman (1B471)	
Cyber Warfare Operations Superintendent (1B491)	
1B4X1 Career Path Chart	
Training Decisions	
Community College of the Air Force Academic Programs	
Career Field Path	
1B4X1 Cyber Warfare Operations Career Path Table	
<u>Section C - Skill Level Training Requirements</u>	22
Purpose	
Specialty Qualification Requirements	
Apprentice (3-Level) Training	
Journeyman (5-Level) Training	
Craftsman (7-Level) Training	
Superintendent (9-Level) Training	
<u>Section D - Resource Constraints</u>	26
Purpose	
Apprentice (3-Level) Training	
Journeyman (5-Level) Training	
Craftsman (7-Level) Training	
Superintendent (9-Level) Training	
<u>Section E - Transition Training Guide</u>	26

Part II

[Section A - Specialty Training Standard](#)27

[Section B - Course Objective List](#)53

[Section C - Support Materials](#).....53

Air Force Job Qualification Standards and Air Force Qualification Training Packages

[Section D - Training Course Index](#)53

Purpose

Air Force In-Residence Courses

Air University Courses

Exportable Courses

[Section E - MAJCOM-Unique Requirements](#)53

OPR: 333TRS/TRR

Approved By: CMSgt Robert J. Agard AFCFM (SAF/CIO A6SF)

Supersedes: CFETP 1B4X1, dated 01 November 2014

Pages: 53

CAREER FIELD EDUCATION AND TRAINING PLAN
CYBER WARFARE OPERATIONS
AFSC 1B4X1

PART I

Preface

1. This Career Field Education and Training Plan (CFETP) is a comprehensive education and training document that identifies life-cycle education/training requirements, training support resources and minimum core task requirements for this specialty. The CFETP will provide personnel a clear career path to success and instill rigor in all aspects of career field training.
2. The CFETP documents the career field training program and consists of two parts. Management uses both parts in conjunction with Training Business Area (TBA) to plan, manage and control training within the career field. **NOTE:** Civilians occupying associated positions will use Part II to support duty position qualification training.
 - 2.1. Part I provides information necessary for overall management of the specialty. Section A explains how everyone will use the plan; Section B identifies career field progression information, duties and responsibilities, training strategies and career field path; Section C associates each level with specialty qualifications (knowledge, education, experience, training and other); Section D indicates resource constraints (e.g., funds, manpower, equipment, facilities); and Section E identifies transition training guide requirements for SSgt through MSgt.
 - 2.2. Part II includes the following: Section A identifies the Specialty Training Standard (STS) and includes duties, tasks, Training References (TRs) to support training, AETC-conducted training, wartime course and core task and correspondence course requirements. Section B contains the Course Objectives List (COL) and training standards supervisors will use to determine if Airmen satisfied training requirements. Section C identifies available support materials (e.g., Qualification Training Package, which may be developed to support proficiency training). Section D identifies a training course index supervisors can use to determine resources available to support training. Included here are both mandatory and optional courses; and Section E identifies MAJCOM-unique training requirements supervisors can use to determine additional training required for the associated qualification needs. At unit level, supervisors and trainers will use Part II to identify, plan and conduct training commensurate with the overall goals of this plan.
3. Use of the guidance provided in this CFETP provides the foundation for effective and efficient training for individuals in this career field at the appropriate points in their careers. This plan enables the Air Force to train today's work force for tomorrow's jobs.

Abbreviations/Terms Explained

This section provides a common understanding of the terms that apply to the Cyber Warfare Operations CFETP.

Advanced Training (AT). A formal course of training that leads to a technical or supervisory level of an Air Force Specialty (AFS). Training is for selected Airmen at the advanced level of an AFS.

Air and Space Expeditionary Force (AEF). The AEF is the Air Force's methodology for organizing, training, equipping, and sustaining rapidly responsive air and space forces to meet defense strategy requirements. Through the AEF, consisting of enabler and tempo banded capabilities the Air Force supports defense strategy requirements using a combination of both permanently assigned and rotational (allocated) forces.

Air Education Training Command (AETC). Responsible for the recruiting, training and education of Air Force personnel. AETC also provides pre-commissioning, professional military and continuing education.

Air Force Career Field Manager (AFCFM). Representative appointed by the respective HQ USAF Deputy Chief of Staff or Under Secretariat to ensure that assigned Air Force specialties are trained and utilized to support Air Force mission requirements.

Air Force Enlisted Classification Directory (AFECD). The official directory for all military enlisted classification descriptions, codes, and identifiers. Establishes the occupational structure of the Air Force enlisted force. The occupational structure is flexible to permit enlisted personnel to specialize and develop their skills and abilities while allowing the Air Force to meet changing mission requirements. Individual enlisted personnel have a joint responsibility with commanders and supervisors at all levels to fully develop their abilities consistent with Air Force needs and within the established patterns of specialization.

Air Force Job Qualification Standard (AFJQS). A comprehensive task list that describes a particular job type or duty position. Supervisors use the AFJQS to document task qualification. The tasks on AFJQSs are common to all persons serving in the described duty position.

Air Force Qualification Training Package (AFQTP). An instructional course designed for use at the unit to qualify or aid qualification in a duty position, program, or on a piece of equipment. It may be printed, computer-based, or other audiovisual media.

Air Force Specialty (AFS). A group of positions (with the same title and code) that require common qualifications.

Air Force Tactics, Techniques and Procedures (AFTTP). AFTTPs describe the proper employment of specific Air Force assets, individually or in concert with other assets, to accomplish detailed objectives.

Air University Associate-to-Baccalaureate Cooperative (AU ABC). Allows Airmen to turn a Community College of the Air Force Associates Degree into a Bachelor's Degree from an accredited university. The ABC program has established a partnership with various civilian higher-education institutions to offer four-year degree opportunities via distance learning. The participating schools will accept all of the credits earned by Airmen who have attained a CCAF degree and apply them to a Bachelor's degree related to their Air Force specialty.

Air University/AFCD (Air Force Career Development Academy). The result of a reorganization of Air Force Institute for Advanced Distributed Learning (AFIADL); provides access to the Extension Course Institute.

Career Field Education and Training Plan (CFETP). A CFETP is 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. CFETPs are officially posted at <http://www.e-publishing.af.mil/>.

Certification. A formal indication of an individual's ability to perform a task to required standards.

Chief Enlisted Manager (CEM). Chief Master Sergeants that have extensive experience and training, and demonstrated managerial ability to plan, direct, coordinate, implement, and control a wide range of work activity. Some managerial duties and responsibilities that are common to all chief enlisted managers are: managing and directing personnel resource activities; interpreting and enforcing policy and applicable directives; establishing control procedures to meet work goals and standards; recommending or initiating actions to improve functional operation efficiency; planning and programming work commitments and schedules; developing plans regarding facilities, supplies, and equipment procurement and maintenance.

Command Line Interface (CLI). A command-line interface (CLI) is a means of interaction with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines).

Computer Based Training (CBT). A forum for training in which the student learns via a computer terminal. It is an especially effective training tool that allows the students to practice applications while they learn.

Continuation Training. Additional advanced training that exceeds the minimum upgrade training requirements and emphasizes present or future duty assignments.

Continuum of Learning (CoL). The deliberate process of combining education, training, and experience to produce the right expertise and competence to meet the Air Force's operational needs. (AFDD 1-1, Annex 1-1). The end goal is to create a culture of lifelong learning.

Core Task. A task AFSCMs identify as a minimum qualification requirement 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. Guidance for using core tasks can be found in the applicable CFETP narrative.

Course Objective List (COL). A publication derived from initial/advanced skills Course Training Standard (CTS), identifying the tasks and knowledge requirements and respective standards provided to achieve a 3-skill level in this career field. Supervisors use the COL to assist in conducting graduate evaluations in accordance with AFI 36-2201, *Air Force Training Program*.

Course Training Standard (CTS). A standard developed for all courses not governed by an STS, including specialized training packages and computer-based training courses.

Critical Tasks. Critical Tasks are tasks that require specific training and certification above and beyond other tasks. Tasks may be defined as critical either through AFI, Technical Orders, higher headquarters, or at any level in the unit.

Cross-Utilization Training. Training on non-duty AFSC specific tasks.

Defensive Cyberspace Operations (DCO). Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems (DOD Dictionary of Military and Associated Terms).

Direct Reporting Unit (DRU). Air Force subdivisions directly subordinate to the CSAF. A DRU performs a mission that does not fit into any of the MAJCOMs. A DRU has many of the same administrative and organizational responsibilities as a MAJCOM (Example of a DRU: USAF Academy).

DoD Directive 8140.01 (Cyberspace Workforce Management). Unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements.

Duty Position Tasks. The tasks assigned to an individual for the position currently held. These include, as a minimum, all core tasks that correspond to the duty position as directed by the AFCFM or MFM, and tasks assigned by the supervisor.

Education and Training Course Announcement (ETCA). Located at <https://app10-eis.aetc.af.mil/etca/SitePages/Home.aspx>, the ETCA contains specific MAJCOM procedures, fund cite instructions, reporting instructions, and listings for those formal courses the MAJCOMs or FOAs conduct or manage. The ETCA contains courses the Air Force and reserve forces conduct or administer and serves as a reference for the Air Force, DoD, other military services, government agencies, and security assistance programs.

Enlisted Specialty Training (EST). A mix of formal training (technical school) and informal training (on-the-job) to qualify and upgrade Airmen in each skill level of a specialty.

Exportable Training. Additional training via computer assisted, paper text, interactive video, or other necessary means to supplement training.

Field Operating Agency (FOA). FOAs are subdivisions of the Air Force directly subordinate to a headquarters US Air Force functional manager. An FOA performs field activities beyond the scope of any of the MAJCOMs. The activities are specialized or associated with an Air Force-wide mission (An example of a FOA is the Air Force Weather Agency).

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

Functional Area Manager (FAM). The individual accountable for the management and oversight of all personnel and equipment within a specific functional area to support the operational planning and execution. Responsibilities include, but are not limited to, developing and reviewing policy; developing, managing, and maintaining Unit Type Codes (UTC); developing criteria for and monitoring readiness reporting; force posturing; and analysis. At each level of responsibility (Headquarters Air Force, MAJCOM, Air Component, FOA, DRU, and Unit), the FAM should be the most highly knowledgeable and experienced person within the functional area and have the widest range of visibility over the functional area readiness and capability issues.

Functional Manager. An individual assigned collateral responsibility for training, classification, utilization, and career development of enlisted personnel. AFSC Functional Managers exist at MAJCOM, NAF and base level.

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

Individual Training Plan (ITP). Using AF Form 623, *On-the-Job Training Record* in conjunction with TBA. The AF Form 623 reflects past and current qualifications, and is used to

determine training requirements. It is intended to be a complete history of past training and current qualifications. Supervisors will ensure all documentation is accurate and comprehensive.

Initial Skills Training (IST). A formal school course that results in an AFSC 3-skill level award for enlisted or mandatory upgrade training to qualified officers. (AFI 36-2201, *Air Force Training Program*)

Instructional System Development (ISD). A deliberate and orderly (but flexible) process for planning, developing, implementing, and managing instructional systems. It ensures personnel are taught in a cost efficient way to become educated on the knowledge, skills, and abilities essential for successful job performance.

Major Command (MAJCOM). A MAJCOM represents a major Air Force subdivision having a specific portion of the Air Force mission. Each MAJCOM is directly subordinate to HQ USAF. MAJCOMs are interrelated and complementary, providing offensive, defensive, and support elements.

Master Task Listing (MTL). A comprehensive list (100%) of all tasks performed within a work center and consisting of the current CFETP or AFJQS and locally developed AF Forms 797 (as a minimum). Should include tasks required for deployment and/or UTC requirements.

Master Training Plan (MTP). Employs a strategy for ensuring the completion of all work center job requirements by using a MTL and provides milestones for task, CDC completion, and prioritizes deployment/UTC, home station training tasks, upgrade, and qualification tasks.

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

Offensive Cyberspace Operations (OCO). Operations intended to project power by application of force in and through cyberspace (DOD Dictionary of Military and Associated Terms).

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

Proficiency Training. Additional training, either in-residence or exportable advanced training courses, or on-the-job training, provided to personnel to increase their skills and knowledge beyond the minimum required for upgrade.

Qualification Training. Hands-on, task performance based training designed to qualify Airmen in a specific duty position. This training program occurs both during and after the upgrade training process and is designed to provide skills training required to do the job.

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

Specialty Training Requirements Team (STRT). A meeting chaired by the AFCFM with MAJCOM FMs, AETC Training Managers, Subject Matter Experts (SME), and HQ AETC Occupational Analysis Division (OAD) in attendance. Typically held in conjunction with a Utilization and Training Workshop (U&TW) to finalize any CFETP changes or enlisted classification directory descriptions.

Specialty Training Standard (STS). An Air Force publication that describes an Air Force specialty in terms of tasks and knowledge that an Airman in that specialty may be expected to perform or to know on the job. Also identifies the training provided to achieve a 3-, 5-, 7-, or 9-skill level within an enlisted AFS. It further serves as a contract between AETC and the functional user to show which of the overall training requirements for an Air Force Specialty Code (AFSC) are taught in formal schools and correspondence courses.

Standard. An exact value, a physical entity, or an abstract concept established and defined by authority, custom, or common consent to serve as a reference, model, or rule in measuring quantities or qualities, establishing practices or procedures, or evaluating results. It is a fixed quantity or quality.

System Training Plan (STP). A living document that explains what training is needed for a system and how to obtain the training.

Task Module (TM). A group of tasks performed together within an AFS that require common knowledge, skills, and abilities. TMs are identified by an identification code and a statement.

Total Force. All collective components (active, reserve, guard, and civilian elements) of the United States Air Force.

Training Advisory Group (TAG). Chaired by the AFCFM and attended by the MAJCOM, selected DRU and FOA functional managers. The TAG sets training goals and priorities, reviews training programs and evaluates emerging training technologies. The group meets, as required, to prioritize training product development.

Training Business Area (TBA). A web-based training application that provides Air Force warfighters with global, real-time visibility into qualifications, certifications and training status of communications professionals. TBA supports base, wing and work center training management activities by automating business processes and capabilities to eliminate paper-based practices. The system centralizes management of training task data, provides user access to CFETPs/JQs and increases security through a single AF Portal log on.

Training Capability. The ability of a unit or base to provide training. Authorities consider the availability of equipment, qualified trainers, and study reference materials, and so on in determining a unit's training capability.

Training Planning Team (TPT). Comprised of the same personnel as a U&TW, TPTs are more intimately involved in training development and the range of issues examined is greater than in the U&TW forum.

Training Requirements Analysis (TRA). A detailed analysis of tasks for a particular AFSC to be included in the training decision process.

Training Setting. The type of forum in which training is provided (formal resident school, on-the-job, field training, mobile training team, self-study, etc.).

Unit Type Code (UTC). A five-character alphanumeric code identifying a specific force package of personnel and/or equipment. The UTC is the means for linking logistics and manpower details within a unit type and is used to communicate force data. The UTC represents a wartime capability designed to fill a valid contingency requirement.

Upgrade Training. Training that leads to the award of a higher skill level.

Utilization and Training Workshop (U&TW). A forum of the AFCFM, MAJCOM Functional Managers, subject matter experts (SME), and AETC training personnel that determines career ladder training requirements.

Wartime Tasks. Those tasks that must be taught when courses are accelerated in a wartime environment. In response to a wartime scenario, these tasks will be taught in the 3- level course in a streamlined training environment. These tasks are only for those career fields that still need them applied to their schoolhouse tasks.

Section A - General Information

1. Purpose of the CFETP. This CFETP provides the information necessary for AFCFMs, MAJCOM Functional Managers (MFM), commanders, training managers, supervisors, trainers and certifiers to plan, develop, manage and conduct an effective and efficient career field training program. The plan outlines the initial skills, upgrade, qualification, advanced and proficiency training that individuals in AFSC 1B4X1 should receive in order to develop and progress throughout their careers. Initial skills training is the AFS specific training an individual receives upon entry into the AF or upon retraining into this specialty for award of the 3-skill level. This training is provided by the 333rd Training Squadron (TRS) at Keesler AFB, MS. Upgrade training identifies the mandatory courses, task qualification requirements, Career Development Course (CDC) completion and correspondence courses required for award of the 5-, 7-, or 9-skill level. Qualification training is actual hands-on task performance training designed to qualify an airman in a specific duty position. This training program occurs both during and after the upgrade training process. It is designed to provide the performance skills and knowledge required to do the job. Advanced training is formal specialty training used for selected airmen. Proficiency training is additional training, either in-residence or exportable advanced training courses, or on-the-job training provided to personnel to increase their skills and knowledge beyond the minimum required for upgrade. The CFETP has several purposes, some of which are:

1.1. Serves as a management tool to plan, develop, manage, and conduct a career field training program. Also, ensures that established training is provided at the appropriate point in an individual's career.

1.2. Identifies task and knowledge training requirements for each skill level in the specialty and recommends training throughout each phase of an individual's career.

1.3. Lists training courses available in the specialty, identifies sources of the training, and provides the training medium.

1.4. Identifies major resource constraints that impact implementation of the desired career field training program.

2. Use of the CFETP. The CFETP is maintained by the 1BXXX Air Force Career Field Manager (AFCFM), SAF/CIO A6SF. MAJCOM FMs and AETC review the plan annually to ensure currency and accuracy and forward recommended changes to the AFCFM. Using the list of courses in Part II, they determine whether duplicate training exists and take steps to eliminate/prevent duplicate efforts. Career field training managers at all levels use the plan to ensure a comprehensive and cohesive training program is available for each individual in the career ladder.

2.1. AETC training personnel develop/revise formal resident and exportable training based upon requirements established by the users and documented in the STS. They also develop procurement and acquisition strategies for obtaining resources needed to provide the identified training.

2.2. MAJCOM FMs ensure their training programs complement the CFETP mandatory initial skill and upgrade requirements. They also identify the needed AFJQSs/AFQTPs to document unique upgrade and continuation training requirements. Requirements are satisfied through OJT, resident training, contract training, or exportable courseware/courses. MAJCOM developed training to support this AFSC must be included into this plan.

2.3. 81 TRSS/TSQ Qualification Training Flight (Q-Flight) personnel develop training packages (AFJQSs/AFQTPs) based on requests submitted by the MAJCOMs and according to the priorities assigned by the AFCFM.

2.4. Unit training managers and supervisors manage and control progression through the career field by ensuring individuals complete the mandatory training requirements for upgrade specified in this plan and supplemented by their MAJCOM. The list of courses in Part II is used as a reference for planning continuation or career enhancement training.

2.5. Submit recommended CFETP corrections to the 81 TRSS Q-Flight Customer Service Desk at 81 TRSS/TSQS, 601 D Street, Keesler AFB MS 39534-2235 or call DSN 597-3343. To contact electronically send email to: qflight.customer.service@us.af.mil.

2.6. Submit recommended CFETP additions/deletions through your MAJCOM Functional Manager.

3. Coordination and Approval of the CFETP. The AFCFM is the approval authority. MAJCOM representatives and AETC training personnel coordinate on the career field training requirements. The AETC training manager initiates an annual review of this document by AETC and MAJCOM functional managers to ensure the CFETP's currency and accuracy by using the list of courses in Part II to eliminate duplicate training.

Section B - Career Field Progression and Information

4. Specialty Description. Performs duties to develop, sustain, and enhance cyberspace capabilities to defend national interests from attack and to create effects in cyberspace to achieve national objectives. Conduct Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO) using established tactics, techniques and procedures (TTPs) to achieve Service, CCMD, and national objectives. Executes command and control (C2) of assigned cyberspace forces and de-conflicts cyberspace operations across the kinetic and non-kinetic spectrum. Supports cyberspace capability development, testing and implementation. Partners with Joint, Interagency, Intergovernmental, and Multinational forces to detect, deny or manipulate adversarial access to sovereign national cyberspace systems. Related DoD Occupational Subgroup: 153100

5. Skills and Career Progression.

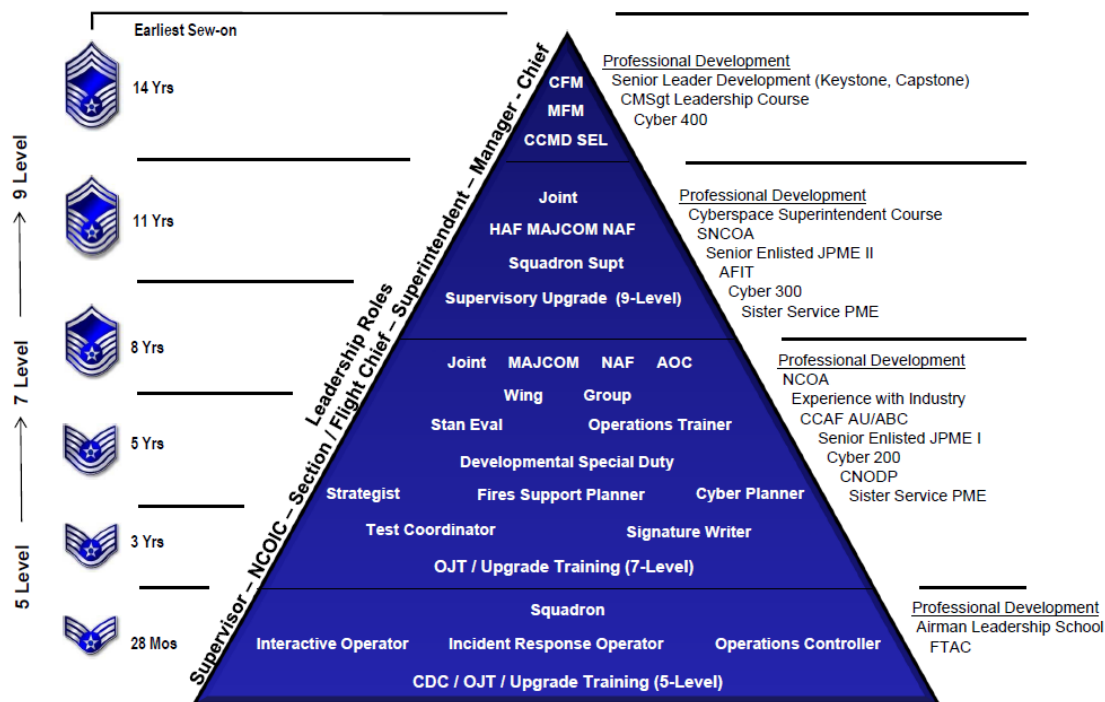
5.1. Cyber Warfare Operations Apprentice (1B431). Initial skills in this speciality consist of the tasks and knowledge provided in the 3-skill level resident 1B4X1 Cyber Warfare Operations Apprentice Course located at Keesler AFB MS. Individuals must complete the initial skills course (E3ALR1B431 0A1A) to be awarded AFSC 1B431. Current requirements were identified and validated during the STRT held 11 September 2017.

5.2. Cyber Warfare Operations Journeyman (1B451). To qualify for the 5-skill level, Airmen must: (1) complete the 5-level Career Development Course (CDC), when available; (2) complete 12 months UGT (9 months for retrainees); (3) meet mandatory requirements listed in the specialty description in the Air Force Enlisted Classification Directory (AFECD) and CFETP; and (4) be recommended by their supervisor and approved by their commander. Supervisors may identify and standardize local tasks for upgrade with the AFCFM approval. Coordinate requestes for AFCFM approval through the MAJCOM FM. UGT consists of completing duty positions training/certification, any specified core task training, and appropriate courses as outlined in the CFETP.

5.3. Cyber Warfare Operations Craftsman (1B471). To qualify for award of the 7-level, Airmen must (1) be a SSgt or higher (SrA with line number for SSgt will be entered into 7-skill level upgrade training); (2) complete mandatory CDCs (if applicable) and core tasks identified in the CFETP; (3) meet mandatory requirements listed in the specialty description in the AFECD and CFETP; (4) complete a minimum of 12 months in upgrade training (6 months if a retrainee); and (5) recommended by the supervisor for awards of the 7-skill level. Individuals in retraining status are subject to the same requirements and must complete a minimum of six months in UGT. Supervisors may identify and standardize local tasks for upgrade with the AFCFM approval. Coordinate requests for AFCFM approval through the MAJCOM FM.

5.4. Cyber Warfare Operations Superintendent (1B491). Must be at least a SMSgt (MSgt with line number for SMSgt will be entered into 9-skill level upgrade training) and meet mandatory requirements listed in the AFECD, be recommended by their supervisor, and approved by their commander for award of the 9-skill level.

1BXXX Career Path Chart



5.5. Enlisted Development Team (EDT).

5.5.1. Mission: The EDT is the deliberate force development steering group for the 1B Cyber Warfare career field. The EDT outlines the training, education, and experience requirements for critical Cyber Warfare duty positions, and provides vector recommendations for the best qualified Senior Non-Commissioned Officers (SNCOs) into key leadership positions across the Air Force. CMSgts and SMSgts will be boarded by a separate EDT panel. MSgts will not be boarded and evaluated via EDT at this time until a future determined period. The EDT also identifies other developmental opportunities for Cyber Warfare SNCOs to facilitate deliberate development. These recommendations or vectors are the EDT's collective recommendation for experience level, training, and/or education opportunity, or position type that a member should be considered and seek out for professional growth. Vectoring will consist of recommendations for identified positions (i.e. development, leadership and strategic positions) with the Cyber Warfare construct for which a member should be considered in subsequent assignments, but will not identify specific assignment locations.

5.5.2. Process: EDT membership is appointed by SAF/CIO A6SF (Cyber Warfare Career Field Manager) and is comprised of senior 1B leaders across the force with the appropriate strategic vision and experience to ensure diversity and inclusion are considered. During the EDT review process, EDT members assess billets for key leadership or key development position designation. EDT members will also board and evaluate 1B SNCO past performance, duty history and experience, scope of responsibility, decorations, and expressed desires in determining appropriate development vectors. Once complete, 1B SNCOs will be made aware of their suggested vector.

6. Training Decisions.

6.1. Three-Skill Level Course. The 3-skill level course has been overhauled in order to continue the evolution of the Cyber Warfare Operations career field. The CFM and MAJCOM Functional Managers concur on the course changes.

6.2. Five-Skill Level Upgrade Requirements. 5-level core task requirements as well as CDC requirements have been adjusted to meet the needs of the operational community.

6.3. Seven-Skill Level Upgrade Requirements. The CFM and MAJCOM Functional Managers approved the requirement of 7-level training in order to better develop leaders within the career field. However, this training will likely be rolled out in an online adaptive learning environment course rather than in the form of CDCs; once developed, course information will be disseminated to the field.

6.4. Nine-Skill Level Upgrade Requirements. Completion of the Cyberspace Superintendent Course has been removed as a 9-level upgrade requirement. However, 1B4 E-7s and above may enroll and take the Cyberspace Superintendent Course as desired. The course may be found on the AETC ADLS site under course identifier E6ACW3DX9X_00AA.

6.5. Proficiency Training. Any additional knowledge and skills that were not provided through initial skills or upgrade training fall under the auspices of continuation training. The purpose of the continuation program is to provide additional training that exceeds minimum qualification or upgrade training requirements within emphasis on present and future duty positions. MAJCOMs and joint activities must develop a continuation-training program that ensures personnel in the Cyber Warfare Operations Specialty receive the necessary training at the appropriate point in their career. The training program will identify both mandatory and optional training requirements. The below describes examples of training course opportunities that exist within the joint community and pertain to cyberspace application; it is not an exhaustive list and other opportunities may be found. The goal of capturing some of these courses is to expand awareness of existing enhancement opportunities.

6.5.1. Joint Targeting School (JTS). This school is located at Dam Neck Naval Air Station, VA and hosts four intermediate level courses. The Joint Targeting Staff Course focuses on the application of the six-step Joint Targeting Cycle at the strategic and operational levels of war and involves the presentation of concepts and theory associated with each step. The Joint Targeting Applications Course focuses on the Weaponizing process and concepts of weapon delivery accuracy, damage mechanisms, and damage criteria along with an introduction to the software tools used for damage prediction calculations. The Joint Battle Damage Assessment (BDA) Course is focused on the methodologies employed to accurately assess and communicate the effectiveness of military force delivered against a variety of generic targets and target models. The Joint Collateral Damage Estimation Course is based on Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3160.01 and focuses on the CDE Assessment Process, Casualty Estimation, Mitigation Techniques, and CDE Automation Tools.

6.5.2. Joint Intermediate Target Development Course (JITD Course). The goal of the Joint Intermediate Target Development Course is to ensure targeting analysts have the skills to develop and database any target type according to the standards directed in CJCSI 3370.01A, Target Development Standards. Work-roles who utilize this course include planners and analysts who learn to database Electronic Targeting Folder (ETF) remarks from facilities, individuals, virtual entity, equipment, and organizational (FIVE-O) target types.

6.5.3. Joint Network Attack Course (JNAC). The focus of this course is to educate staff level planners on how operations are conducted across the spectrum of Cyberspace Operations, focusing on Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO). Additionally, students are trained in the various skills to conduct OCO/DCO planning and develop an understanding of technical versus operational terminology, as well as domestic and international laws as they apply to OCO/DCO.

6.5.4. Joint Cyberspace Operations Planners Course (JCOPC). This course is sponsored by the USSTRATCOM Cyberspace Training Initiative (CTI) and managed by USCYBERCOM.

JCOPC was originally developed as a mobile training curriculum to be presented to Combatant Commands (CCMDs) in response to identified training requirements. Its purpose is to train CCMD and Joint Force Command (JFC) staffs on the integration of cyberspace operations into CCMD/JFC level planning. Its scope has been expanded to be included as part of the training pipeline for the Cyber Mission Force (CMF).

6.5.5. Joint Information Operations Planners Course (JIOPC). This course is an informative and practical course of instruction that is particularly useful for personnel who are headed to Information Operations (IO) planning jobs at the operational level of war (CCMD/JTF/JFC). The course is composed of one week of lectures on the IO core, supporting and related capabilities specified in Joint IO doctrine, followed by three weeks of lectures and practical exercises on the Joint Planning process and how to use it for IO planning.

6.5.6. Joint Advanced Cyber Warfare Course (JACWC). This course is designed to make personnel, regardless of background, effective and credible within the cyber warfare community upon graduation. JACWC provides an orientation to USCYBERCOM, the global cryptologic platform, the Intelligence Community, the US Government cyber community of interest, allies, and major partners in the conduct of cyber warfare, as well as cyber warfare threats, operations, planning, and analysis of desired effects.

6.5.7. Air Operations Center Courses. The 505th Training Squadron at Hurlburt Field, FL teaches 16 Initial Qualification Training courses for the AOC weapons system. Additionally, the squadron teaches the joint certified Joint Air Operations Center Command and Control Course (JAOC2C) to students in order to cover the theater air planning process.

6.5.8. Air Force Forces (AFFOR) Intermediate Staff Course (AISC). This is a five-day course which trains Component-Numbered Air Force (C-NAF) Forces staff personnel who conduct and support operational-level planning and execution. The course develops the foundational skills necessary to execute warfighting headquarters staff responsibilities on behalf of the Commander Air Force Forces (COMAFFOR) as part of the C-NAF in support of Joint Force Commander objectives. This course is run through the 505th Combat Training Squadron at Hurlburt Field, FL.

6.5.9. Joint C4I Cyber Course. The JC4I Cyber Course prepares students for positions that require an understanding of command, control, communications, computers, and intelligence/cyber (C4I/C). This course educates personnel from varied backgrounds to function in a joint environment. It provides a broad understanding of joint C4I/C doctrine and current policy guidance. Students apply joint C4I/C concepts and skills/procedures to prepare for duty in joint or service C4I/C staff operations and planning assignments. The program covers a wide spectrum of C4I/C that extends from the national and strategic levels to the theater and tactical levels in support of the President, Secretary of Defense, and commanders who control military forces. This course is geared at intermediate level staff officers, senior noncommissioned officers, and DoD civilian equivalents for duty in C4I/C staff operations at a Combatant Command, Joint Task Force, or Headquarters staff. The course is open to grades E-6 to E-9 and is 3-weeks long, located at the Joint Forces Staff College in Norfolk, VA.

6.5.10. Cyberspace Tactical Planner Course. This course was developed by weapons officers at the 67th Cyberspace Wing to teach large force employment, roles and responsibilities of the mission commander and tactical planners, and integration of cyberspace forces identified in Air Force Cyberspace Tasking Orders. The training program teaches Air Force Weapons School ME3C-(PC)² planning process methodology for both offensive and defensive mission sets.

6.5.11. Senior Enlisted Joint Professional Military Education (SEJPME). Both SEJPME I and II courses are stand-alone, 100% online, web-based courses that use multi-media instruction. Course eligibility is restricted to E-5 and above for SEJPME I and E-6 and above for

SEJPME II. The SEJPME courses prepare senior enlisted leaders assigned to joint organizations to successfully support activities and supervise multiple Service members. Upon completion of the course, SELs will be more competent, confident, and prepare to assimilate and effectively contribute in joint assignments as well as mentor junior enlisted leaders and other service personnel they supervise. These courses may be found on Joint Knowledge Online (JKO).

6.6. Degree Programs:

6.6.1. Air Force Institute of Technology (AFIT)

6.6.1.1. Mission: The Air Force Institute of Technology, or AFIT, is the Air Force's graduate school of engineering and management as well as its institution for technical professional continuing education. A component of Air University and Air Education and Training Command, AFIT is committed to providing defense-focused graduate and professional continuing education and research to sustain the technological supremacy of America's air and space forces.

6.6.2. National Intelligence University (NIU)

6.6.2.1. Description: The National Intelligence University (NIU) is a regionally accredited institution offering military and civilian personnel working in intelligence or intelligence/security-related specialties the opportunity to enroll in professional intelligence undergraduate or graduate-level study in full- or part-time programs. Coursework concentrates on a variety of intelligence disciplines to include collection; analysis; regional studies; information operations; intelligence, surveillance, and reconnaissance; national security issues; and strategic intelligence in the joint environment. NIU educates future leaders who are full partners with their policy, planning, and operations counterparts and who are able to anticipate and tailor the intelligence required at the national, theater and tactical levels. Classes have an Intelligence Community student mix from all services and the federal government. The college is located at Roberdeau Hall on the IC Campus Bethesda (ICC-B) in Bethesda, MD.

6.6.2.1.1. Coursework Background: In 2012, the School of Science and Technology Intelligence was approved by the Department of Education to offer a Master of Science and Technology Intelligence (MSTI) Degree to individuals in both the cyber and intelligence career fields. The approved Cyber Operations AF Specialities are 3D0X2, 3D0X3, 3D1X2, and 1B4XX. The MSTI is a graduate degree program requiring completion of an 11-month course of study consisting of five required courses, seven electives, and thesis courses. 3D/1B4 applicants will adhere to the Cyber Intelligence and Data Analytics Concentration of the MSTI program, which will include study in areas such as social networks and intelligence, foreign cyber strategies, and information influence and deception.

6.6.2.2. Eligibility Criteria:

6.6.2.2.1. NIU programs are open to military service members and U.S. government employees who are U.S. citizens and who hold finalized Top Secret/SCI clearances.

6.6.2.2.2. The program is open to Air Force activity duty and Reserve Component NCOs in the grades of E-5 select through E-8 and civilians from GG-09 to GG-15.

6.6.2.2.3. Military applicants must be PCS eligible. Further criteria are defined annually and conveyed via an AF message to the field.

6.6.2.2.4. Military members must have three years retainability upon class graduation. Personnel will incur a three-year active duty service commitment upon graduation/program completion.

6.6.2.2.5. Military members must have completed Professional Military Education commensurate with their grade.

6.6.2.2.6. Baccalaureate Degree for a regionally accredited institution and the graduate record exam (GRE) for those who do not already have a Master's degree from a regionally accredited institution. The ideal candidate will have academic exposure to science, technology, engineering or math (STEM) during their undergraduate years.

6.6.2.2.7. Other eligibility requirements apply. See call for nominations guidance or below Application Process.

6.6.2.2.8. Application Process: Air Staff calls for nominations for this program annually in the summer to fall timeframe via formal message traffic. For further information on applying to the National Intelligence University, visit <http://www.ni-u.edu/>

6.7. Education With Industry (EWI).

6.7.1. Program Overview: The Education with Industry (EWI) program is a highly selective, competitive non-degree educational assignment within an industry related to the student's career field. The program uses a hands-on educational experience to provide students with management skills and technical expertise as they study best practices with leaders of industry. The assignment is ten months in length. Since 2015, when the program was opened to enlisted, 1B4s selected for this opportunity have been assigned to United Services Automobile Association (USAA) in San Antonio, Texas to learn data security and cyber incident response skills. However, the CFM will source appropriate industry partners to maximize the program's return on investment. The program follows an academic year calendar, which begins in late August or early September and ends in late June. Both defense- and non-defense-focused companies can host students. EWI is an Air Force Level Base Developmental Education program under the Force Development concept. It is sponsored by SAF/AQ and managed by the Air Force Institute of Technology (AFI), more specifically AFIT/ENEL. The governing AFI for this program is AFI 36-2639.

6.8. Joint-Computer Network Operations Development Program (J-CNODP).

6.8.1. Program Overview: J-CNODP is technically demanding three-year program with a follow-on assignment individually tailored to each applicant to best capitalize on his/her expertise. This is an opportunity for a select group of highly technically-inclined individuals to further develop their skills in the areas of secure system design, vulnerability analysis, computer network defense (CND), and computer network exploitation (CNE). The goal of the program is to develop a cadre of technical leaders who will improve the Department of Defense's and each military service's Computer Network Operations (CNO) capabilities. The J-CNODP program is made up of CNODP, the National Security Agency's (NSA) program for civilians that includes 10 or more slots annually for military members, and USCYBERCOM's Joint Cyber Development Program (JCDP), which allocates 20 slots for military members. All 30 slots are competitive across the services.

6.8.2. Additional Information: J-CNODP begins with three to four months of "core training", which consists of both internal and external classes to enhance the intern's technical skills and bridge gaps between typical Computer Science/Engineering curriculum and those necessary for Computer Network Attack / Exploitation / Defense. Following core training, J-CNODP interns tour for six to twelve months each in various offices at NSA and USCYBERCOM, working as a CNO developer, operator, and/or analyst. The total time spent touring offices is 30 months, resulting in three to five tours for each intern; however, interns choose the tours they want to work. Each intern must complete at least one offensive and at least one defensive tour during the program. These tours are not limited to the primary NSA campus but most will be within 30 miles of Fort Meade. JCDP participants must also complete one tour in support of USCYBERCOM. The final three months of the program are spent working one of two team "final projects", which are hard CNO problems that NSA and USCYBERCOM need solved.

More details can be found at: <https://www.my.af.mil/gcss-afbvpcp/USAF/ep/browse.do?programId=tE3494DD04620202F0146456118E7042F&channelPageId=s88B4F00B42B9FCA60142DD69530D02F6>

6.8.3. Eligibility Criteria:

6.8.3.1. Must hold a TS/SCI clearance based on an adjudicated Single Scope Background Investigation (SSBI) prior to arrival at NSA. Additionally, selected applicants must possess a current Counter-Intelligence Polygraph before the class start date.

6.8.3.2. Individuals applying to J-CNODP must meet PCS eligibility requirements. Each applicant must have at least two years TOS before the RNLTD stated in the call for applications. The member cannot have any other pending voluntary assignment applications or an assigned PCS.

6.8.3.3. Enlisted military grades include E-5/E-6 and less than 14 years Total Active Federal Military Service (TAFMS) is required to start the program.

6.8.3.4. Bachelor’s Degree plus advanced courses or equivalent experience in the areas of Computer Engineering, Computer Science, Electronic or Electrical Engineering, or Applied Mathematics are highly desired but not required. Additionally, demonstrated programming skills in C or C++, Python, and some Assembly are desired. Applicants with experience in other compiled or interpreted languages should still apply.

7. Community College of the Air Force (CCAF) Academic Programs. Enrollment in CCAF occurs upon completion of basic military training. CCAF provides the opportunity for all enlisted members to obtain an Associate in Applied Science degree. Refer to the AF Virtual Education Center (accessible via the AF Portal, <https://www.my.af.mil>) for CCAF credits earned for technical training courses attended. In order to be awarded a CCAF AAS degree, students must complete the program before they separate from the Air Force, retire, or are commissioned as an officer.

7.1. The Cybersecurity (0CYC) program applies to the 1B4X1 career field.

7.1.1. Degree Requirements: Individuals must hold the 5-skill level at the time of program completion.

	Semester hours
Technical Education.....	24
Leadership, Management, and Military Studies	6
Physical Education.....	4
General Education.....	15
Program Electives	15
Total	64

7.1.2. Technical Education (24 semester hours): A minimum of 12 semester hours of technical core subjects and courses must be applied and the remaining semester hours will be applied from technical core/technical elective subjects and courses. Requests to substitute comparable courses or to exceed specified semester hour values in any subject/course must be approved in advance by the technical branch of the CCAF Administrative Center.

7.1.3. Leadership, Management, and Military Studies (LMMS)(6 semester hours): Professional military education (PME) and/or civilian management courses accepted in transfer and/or by testing credit. See CCAF General Catalog for application of civilian management courses.

7.1.4. Physical Education (4 semester hours): Satisfied upon completion of basic military training.

7.1.5. General Education (15 semester hours): Courses must meet the criteria for application of courses to the General Education requirement and be in agreement with the definitions of applicable General Education subjects/courses as outlined in the CCAF General Catalog.

7.1.6. General Education Mobile (GEM): GEM is a partnership between CCAF and civilian academic institutions to offer general education courses to meet CCAF A.A.S. degree requirements. Courses are offered via distance learning which reduces CCAF educational impact of deployments, PCS and family commitments.

7.1.7 Program Elective (15 semester hours): Courses applying to technical education, LMMS or general education requirements; natural science courses meeting general education requirement application criteria; foreign language credit earned at Defense Language Institute or through the Defense Language Proficiency Test; maximum 9 Semester Hours of CCAF degree-applicable technical course credit otherwise not applicable to program of enrollment.

7.2. See the current CCAF General Catalog for details regarding the Associates of Applied Science in Cybersecurity. The catalog is available at your education office.

7.3. Additional off- duty education is a personal choice that is encouraged for all. Individuals desiring to become an AETC Instructor must possess as a minimum an associate degree or should be actively pursuing an associate degree. Special Duty Assignment (SDA) requires an AETC instructor candidate to have a CCAF degree or be within one year of completion (45 semester hours). A degreed faculty is necessary to maintain accreditation through the Southern Association of Colleges and Schools.

8. Career Field Path. Table 8.1. identifies career milestones for the 1B4X1 Air Force specialty.

Table 8.1.

1B4X1 CYBER WARFARE OPERATIONS CAREER PATH			
	<i>GRADE REQUIREMENTS</i>		
<i>Education and Training Requirements</i>	<i>Rank</i>	<i>Earliest Sew-On</i>	<i>High Year Of Tenure (HYT)</i>
Basic Military Training School (BMTS)			
Apprentice Technical School (3-Skill Level)	A1C		
Upgrade To Journeyman (5-Skill Level) MANDATORY - Minimum 9 months OJT training for retrainees. - Complete appropriate CDC. - Specific AFJQSs/AFQTPs for equipment at assigned location by duty position. (see NOTE 2) OPTIONAL AETC Supplemental training courses as determined by MAJCOM.	A1C SrA	28 months	8 Years
EPME Phase 1 - Airman Leadership School - Resident course. - 3-6 years time in service. * Refer to AFI 36-2301, <i>Developmental Education</i> .	Trainer - Qualified and certified to perform the task to be trained. - Must attend formal AF Training Course. - Recommended by the supervisor.		
Upgrade To Craftsman (7-Skill Level) MANDATORY - Minimum rank of SSgt. - 12 months OJT. Minimum 6 months - Complete appropriate CDC. - Specific AFJQSs/AFQTPs for equipment at assigned location by duty position. OPTIONAL AETC Supplemental training courses as determined by MAJCOM.	SSgt	3 years	15 years
EPME Phase 2 – Non-Commisioned Officer Academy - Airmen who are selected for promotion to SSgt or complete ALS may enroll in the NCO Distance	TSgt	5 years	20 years

1B4X1 CYBER WARFARE OPERATIONS CAREER PATH			
	GRADE REQUIREMENTS		
<i>Education and Training Requirements</i>	<i>Rank</i>	<i>Earliest Sew-On</i>	<i>High Year Of Tenure (HYT)</i>
Learning Course (DLC). - Completed DLC is a requirement to attend resident NCOA - Airmen who completed the DLC and were ineligible to attend resident EPME due to TIS restrictions prior to 30 Jun 2017 will not be required to attend the respective resident courses. * Refer to AFI 36-2301, <i>Developmental Education</i> , and MyPers.			
EPME Phase 3 - USAF Senior NCO Academy - Airmen who have completed NCOA may enroll in SNCO DLC. - Completed DLC is a requirement to attend resident SNCOA - Airmen who completed the DLC and were ineligible to attend resident EPME due to TIS restrictions prior to 30 Jun 2017 will not be required to attend the respective resident courses. * Refer to AFI 36-2301, <i>Developmental Education</i> , and MyPers.	MSgt	8 years	24 years
Upgrade To Superintendent (9-Skill Level) MANDATORY - Minimum rank of SMSgt.	SMSgt	11 years	26 Years
Chief Enlisted Manager (CEM)	CMSgt	14 years	30 years

NOTE 1: Published sew-on times are Air Force averages. Refer to the myPers website for current information: <https://mypers.af.mil/>.

NOTE 2: See Part II, Sections C and D for a list of AFJQSs/AFQTPs and AETC supplemental training.

Section C - Skill Level Training Requirements

9. Purpose. The various skill levels in the career field are defined in terms of tasks and knowledge requirements for each skill level in the Cyber Warfare Operations career ladder. They are stated in broad, general terms and establish the standards of performance. Core tasks, knowledge items, and skill requirements for this specialty are identified in the STS, COL, CDCs, AFJQSs/AFQTPs, etc. Completion of the mandatory 3-level skill awarding course, CDCs, CFETP, and applicable AFJQSs/AFQTPs define the Air Force core tasks for this specialty.

10. Specialty Qualification Requirements.

10.1. Apprentice (3-Level) Training.

KNOWLEDGE	Computer Operating Systems, Software Applications, Database Concepts, Common Programming Languages, Hardware Components, Networking Fundamentals, Protocols, Network Addressing, Network Infrastructure, Telecommunications Theory, Data Communications, Wireless Technologies, Cryptography and Cyber Operation Laws
EDUCATION	For entry into this specialty, completion of high school is mandatory. Additional courses in Science, Technology, Engineering, and Mathematics (STEM) is desirable. Associate degree or higher in related fields or Information Technology (IT) Certification is desirable.
TRAINING	Completion of the Cyber Warfare Operations Apprentice course (See Part II, Section B for Course Objective List)
EXPERIENCE	None required
OTHER	Minimum score of 60 on the Air Force Electronic Data Processing Test. Requires routine access to Top Secret material or similar environment, completion of a current Single Scope Background Investigation (SSBI) according to AFI 31-501, <i>Personnel Security Program Management</i> , is mandatory for award and retention of this skill level. NOTE: Award of the 3-skill level without a completed SSBI is authorized provided an interim Top Secret clearance has been granted according to AFI 31-501. For award and retention of 1B431, individual must maintain local network access IAW AFI 17-130, <i>Cybersecurity Program Management</i> and 17-1301, <i>Computer Security (COMPUSEC)</i> .
IMPLEMENTATION	Attendance at the Cyber Warfare Operations Apprentice Course is mandatory for award of the 3-skill level unless waived by the 1B AFCFM

10.2. Journeyman (5-Level) Training.

KNOWLEDGE	All 1B431 knowledge qualifications apply to the 1B451 requirements
TRAINING	<p>Completion of the 1B451 Career Development Course.</p> <p>Completion of all STS core tasks.</p> <p>Completion of applicable AFJQS/AFQTPs.</p> <p>Completion of all local tasks assigned for the duty position to include Crew Position Certification if required for duty position.</p>
EXPERIENCE	<p>Qualification in and possession of AFSC 1B431</p> <p>Experience performing Cyber Warfare Operations functions as outlined in Section B, para. 4.</p>
OTHER	<p>Requires routine access to Top Secret material or similar environment, completion of a current Single Scope Background Investigation (SSBI) according to AFI 31-501, <i>Personnel Security Program Management</i>, is mandatory for award and retention of this skill level.</p> <p>For award and retention of 1B451, individual must maintain local network access IAW AFI 17-130, <i>Cybersecurity Program Management</i> and 17-1301, <i>Computer Security (COMPUSEC)</i>.</p>
IMPLEMENTATION	Entry into formal journeyman upgrade training is accomplished once individuals are assigned to their first duty station. Qualification training is initiated anytime individuals are assigned duties for which they are not qualified. Use OJT, CDCs, CFETP, CBTs, and AFJQSs/AFQTPs concurrently to obtain the necessary qualification for refresher and cross-utilization training.

10.3. Craftsman (7-Level) Training.

KNOWLEDGE	All 1B451 knowledge qualifications apply to the 1B471 requirements
TRAINING	<p>Completion of the 1B471 Career Development Course.</p> <p>Completion of all STS core tasks.</p> <p>Completion of applicable AFJQS/AFQTPs.</p> <p>Completion of all local tasks assigned for the duty position to include Crew Position Certification if required for duty position.</p>
EXPERIENCE	<p>Qualification in and possession of AFSC 1B451</p> <p>Experience performing or supervising Cyber Warfare Operations functions as outlined in Section B, para. 4.</p>
OTHER	<p>Requires routine access to Top Secret material or similar environment, completion of a current Single Scope Background Investigation (SSBI) according to AFI 31-501, <i>Personnel Security Program Management</i>, is mandatory for award and retention of this skill level.</p> <p>For award and retention of 1B471, individual must maintain local network access IAW AFI 17-130, <i>Cybersecurity Program Management</i> and 17-1301, <i>Computer Security (COMPUSEC)</i>.</p>
IMPLEMENTATION	Entry into OJT is initiated when individuals obtain the necessary rank and skill level. Qualification training is initiated anytime an individual is assigned duties for which they are not qualified. Use OJT, CBTs, CDCs, CFETP, and AFJQSs/AFQTPs concurrently to obtain the necessary qualification for refresher and cross-utilization training.

10.4. Superintendent (9-Level) Training

KNOWLEDGE	Resource Management, Manpower and Organization, Training Management, Deployment Management and Base/Unit Functional Management
TRAINING	None
EXPERIENCE	Qualification in and possession of AFSC 1B471 Managing and directing Cyber Warfare Operations personnel and processes.
OTHER	Requires routine access to Top Secret material or similar environment, completion of a current Single Scope Background Investigation (SSBI) according to AFI 31-501, <i>Personnel Security Program Management</i> , is mandatory for award and retention of this skill level.
IMPLEMENTATION	Entry into OJT is initiated when individuals are selected for the rank of SMSgt. Qualification training is initiated anytime individuals are assigned duties for which they are not qualified.

10.5. Training Sources.

10.5.1. AFSC specific training – 333 TRS, Keesler AFB, MS at <https://app10-eis.aetc.af.mil/etca/SitePages/Home.aspx>, course ID: E3ALR1B431 0A1A

10.5.2. 1B4X1 CDCs will be available through the Unit Training Manager. Once the individual has been validated and enrolled into the program, he or she will receive a link to the online CDCs. Paper-based CDCs are no longer supported. As of this publication, CDCs are still in the final stages of approval by AFCDA and are not yet available.

10.5.3. AFJQSs/AFQTPs are Air Force publications and are mandatory for use by personnel in upgrade or qualification training. They are developed by the 81 TRSS (Q-Flight), Keesler AFB, MS and may be downloaded from <https://cs2.eis.af.mil/sites/10445/default.aspx>.

10.5.3.1. Procedures for requesting development of AFJQSs/AFQTPs are contained in AFI 17-204, *Air Force On-the-Job Training Products for Cyberspace Support Enlisted Specialty Training*. AFJQSs/AFQTPs are listed in Part II, Section C, of this CFETP.

Section D - Resource Constraints

11. Purpose. This section identifies known resource constraints that preclude optimal/desired training from being developed or conducted, including information such as cost and manpower. Included are narrative explanations of each resource constraint and an impact statement describing what effect each constraint has on training, the resources needed, and actions required to satisfy the training requirements.

12. Apprentice (3-Level) Training.

12.1. Impact. Course content and length changed to 97 days. Revised content as identified by the field includes blocks on scripting and operational-level planning concepts.

12.2. Resources Required. None

12.3. Action Required. None

12.4. OPR/Target Completion Date.

13. Journeyman (5-Level) Training.

13.1. Impact. None.

13.2. Resources Required. None.

13.3. Action Required. None.

13.4. OPR/Target Completion Date. None.

14. Craftsman (7-Level) Training.

14.1. Impact. None.

14.2. Resource Required. None.

14.3. Action Required. None.

14.4. OPR/Target Completion Date.

15. Superintendent (9-Level) Training.

15.1. Impact. None.

15.2. Resource Required. None.

15.3. Action Required. None.

15.4. OPR/Target Completion Date. None.

Section E - Transition Training Guide

There are currently no transition training requirements. This area is reserved.

PART II

Section A - Specialty Training Standard

1. Implementation. This STS will be used for technical training provided by AETC for the 3-level class beginning 27 Jul 2018.

2. Purpose. As prescribed in AFI 36-2201, *Air Force Training Program*, this STS:

2.1. Lists in column 1 (Task, Knowledge, and Technical Reference) the most common tasks, knowledge, and technical references necessary for Airmen to perform duties in the 3-, 5-, 7-, and 9-skill level. Column 2 (Core Tasks) identifies, by skill level specialty-wide training requirements. NOTE: Core tasks are minimum task training requirements for upgrade.

2.2. Provides certification for OJT. Column 3 is used to record completion of tasks and knowledge training requirements. Use automated training management systems to document qualifications, if available. For initial certification or transcribing documentation complete the columns in accordance to AFI 36-2201.

2.3. Shows formal training and correspondence course requirements. Column 4 shows the proficiency to be demonstrated on the job by the graduate as a result of training on the task/knowledge and the career knowledge provided by the correspondence course. See the Air Force Career Development Academy (AFCDA) CDC/eCDC catalog maintained at https://cs2.eis.af.mil/sites/13243/AFKN_Docs/e-CDC_CDC%20Catalog current CDC listings.

2.4. Qualitative Requirements. Attachment 3 contains the tasks, knowledge, and proficiency levels referenced in paragraph 2.1. Columns are marked with a proficiency code to indicate subjects taught. An X in the proficiency code column indicates a lack of student man years and instructor resources. Trainees without prerequisites specified in Education and Training Course Announcement (ETCA) cannot be expected to meet proficiency levels indicated.

PREREQUISITES: Possession of DoD 8570.1M qualifying certification as well as completion of IT Fundamentals (Attachments 2 and 1).

2.5. Becomes a job qualification standard (JQS) for on-the-job training when placed in AF Form 623, *Individual Training Record* folder, and used according to AFI 36-2201, *Air Force Training Program*.

2.6. Is a guide for development of promotion tests used in the Weighted Airman Promotion System (WAPS). Specialty Knowledge Tests (SKT) are developed at the AETC Airmen Advancement Division by senior NCOs with extensive practical experience in their career fields. The tests sample knowledge of STS subject matter areas judged by test development team members as most appropriate for promotion to higher grades. Questions are based upon study references listed in the Enlisted Promotion References and Requirements Catalog (EPRRC). Individual responsibilities are listed in chapter 1 of AFI 36-2605, *Air Force Military Personnel Testing System*. WAPS is not applicable to the Air National Guard or Air Reserve Forces.

3. Recommendations. Comments and recommendations are invited concerning the quality of AETC training. A Training Feedback Hotline has been installed for the supervisors' convenience. For a quick response to concerns, call our Training Feedback Hotline at DSN 597-4566, or e-mail us at 81TRG.TGE.Workflow@us.af.mil. Reference this STS and identify the specific area of concern (paragraph, training standard element, etc).

BY ORDER OF THE SECRETARY OF THE AIR FORCE

OFFICIAL

BRADFORD J. SHWEDO, Lieutenant General, USAF
Chief, Information Dominance and
Chief Information Officer

Attachments:

1. IT Fundamentals Course Training Standard (CTS) *
2. Security+ Certification CTS *
3. Specialty Training Standard (STS) 1B4X1

* This course is currently going through a re-write. The CTS for IT Fundamentals and Security+ will be changing when the new courses come online.

PREFACE

NOTE 1: Dashed items in this CTS are not part of the original CTS created at the March 2009 IT Fundamentals conference however, they are the specific objectives taught in the IT Fundamentals course designed to meet the CTS requirements.

NOTE 2: Unless otherwise stated, students may be allowed two assists from the instructor and still successfully achieve the proper level of proficiency. An instructor assist is anytime an instructor must intercede to provide guidance to a student which leads to a satisfactory completion of the objective or to prevent the student from continuing in a manner that will lead to an unsatisfactory conclusion, safety violation, or damage to equipment.

NOTE 3: All 3-level tasks will be trained if a wartime surge is ordered.

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 only help 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.		
X This mark is used alone in 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.		

1. ELECTRONICS SUPPORT SUBJECTS

- | | |
|---|---|
| 1.1. Safety | B |
| 1.2. First Aid | A |
| 1.3. Personal and Family Countermeasures (CM) | A |

2. DIGITAL NUMBERING SYSTEMS (Internal Data Representation)

- | | |
|------------------------------------|---|
| 2.1. Conversions | |
| 2.1.1. Binary | B |
| 2.1.2. Hexadecimal | B |
| 2.1.3. Binary Coded Decimal | A |
| 2.2. Calculate Hexadecimal Numbers | X |

3. BASIC COMPUTER FUNDAMENTALS

- | | |
|---|---|
| 3.1. Communications/Network Protocols | |
| 3.1.1. Connection Oriented Communication | A |
| 3.1.2. Connectionless Oriented Communication | A |
| 3.1.3. International Standards Organization (ISO) Open Systems Interconnect (OSI) Model | A |
| 3.1.4. TCP/IP | A |
| 3.1.5. Department of Defense (DoD) Standards Protocol | A |
| 3.1.6. IPV4/IPV6 | A |
| 3.1.7. Ports (IP) | A |
| 3.2. Network Theory/Components | |
| 3.2.1. Components | |
| 3.2.1.1. Component Principles | B |
| 3.2.1.2. Central Processing Unit (CPU) | A |
| 3.2.1.3. Computer memory | A |
| 3.2.1.4. Input/output (I/O) Devices | A |
| 3.2.1.5. Storage Devices | A |
| 3.2.1.6. Peripherals (Printers, FAX, Scanners, etc) | A |
| 3.2.2. Network Types | |
| 3.2.2.1. Wired (LAN, WAN, MAN) | A |
| 3.2.2.2. Wireless | A |
| 3.2.2.3. Virtual Private Network (VPN) | A |
| 3.2.2.4. Video Teleconference | A |

3.2.2.5. Topologies (Star, Ring, Bus, Hybrid, etc)	A
3.3. Data Terminal Equipment/Data Communications Equipment (DTE/DCE)	
3.3.1. Modems	A
3.3.2. Converters	A
3.3.3. Gateways	A
3.3.4. Switches	A
3.3.5. Bridges/Routers	A
3.3.6. Encryption/COMSEC Devices (Data and Voice)	A
3.3.7. Communications Mediums	A
3.3.8. Multiplexing	
3.3.8.1. Multiplexers	A
3.3.8.2. Wave Division Multiplexing	A
3.3.8.3. Time Division Multiplexing	A
3.4. Software	
3.4.1. Operating Systems (UNIX, Windows, LINUX, etc.)	A
3.4.2. Applications (Word, Excel, PowerPoint, SharePoint, etc.)	A
3.4.3. Infectious and Malicious Software	A
4. CRYPTOLOGY (Bound & Unbound)	
4.1. Bulk Encryption	A
4.2. Information Encryption Techniques	A
4.3. Separation Requirements	A
5. NETWORK FAULT ISOLATION TECHNIQUES	
5.1. Network Error Detection	1a
5.2. Network Error Correction	1a
5.3. Network Flow Control	1a
5.4. Transmission Impairments	1a
5.5. Network Management Concepts and Responsibilities	B
6. CYBER SECURITY	
6.1. Cyber Vulnerabilities	A
6.2. Vulnerability Preventative Measures	A
6.3. Identity Management	A
6.4. Wireless Network Security	A

7. COMMUNICATIONS AND INFORMATION PROFESSIONALS

- 7.1. Organizations A
- 7.2. Communications Competencies A
- 7.3. Expeditionary Communications X

8. RISK MANAGEMENT (RM) TR: AFIs 90-802, 91-203, 91-302

- 8.1. RM A

9. PUBLICATIONS AND DIRECTIVES TR: AFINDs 5 & 8; AFIs 33-Series

- 9.1. Department of Defense (DoD) X
- 9.2. Air Force X
- 9.3. Commercial/Vendor publications X
- 9.4. DISA Publications X
- 9.5. Technical Orders (TO) X
- 9.6. Standard Installation Practices Technical Order (SIPTO) X
- 9.7. Enterprise Information Architecture (EIA)/ Telecommunications Industry Association (TIA) X
- 9.8. Military Standard (MIL STD) X

10. LEGAL/ETHICS TR: USC TITLE 10, 18 and 50; Joint Information Doctrine (Joint Pub 3-13); AF Information Operations Doctrine 3-13; Health Insurance Portability and Accountability Act (HIPAA)

- 10.1. US Codes (e.g. Titles 10, 15, 18, 32, 50) (e.g. Constitutional Authority, legal aspects of rules of engagement, homeland defense, Posse Comitatus, US Charter Paradigm, Schmidt Analysis) A
- 10.2. Rules of Engagement (ROE)
 - 10.2.1. Policy A
 - 10.2.2. Security Tools A
 - 10.2.3. Cyber Management Ethics A
 - 10.2.4. System Monitoring A
- 10.3. Special Data Protection (i.e. sensitive personnel information) A

11. C4I SECURITY TR: ACP 122; AFIs 10-712, 33-129, 33-102, 33-332 33-138; AFKAG-1&2; AFMAN 33-326; DOD 5200.1-R

- 11.1. Operations Security (OPSEC) TR: AFI 10-701; AFPD 10-7
 - 11.1.1. Definition X
 - 11.1.2. Relationship of OPSEC to other security programs X
 - 11.1.3. Vulnerabilities X

11.1.4. Critical Information	X
11.2. Information Security TR: AFI 31-401; AFPD 31-4, 33-2	
11.2.1. Information safeguards	
11.2.1.1. Unclassified	
11.2.1.1.1. Privacy Act (PA)	A
11.2.1.1.2. For Official Use Only (FOUO)	A
11.2.1.1.3. Sensitive Unclassified	A
11.2.1.2. Classified	A
11.3. Communications Security (COMSEC) TR: AFI 31-401; AFPDs 33-2 and 31-4	
11.3.1. Definition	A
11.3.2. Vulnerabilities	A
11.3.3. Safeguarding Information	A
11.4. Emission Security (EMSEC) TR: AFI 33-203 (V1), AFPD 33-2	
11.4.1. Definition	A
11.4.2. Notifications	A
11.4.3. Vulnerabilities	A
11.4.4. Protected Distribution System (PDS)	A
11.5. Computer Security (COMPUSEC) TR: AFI 33-200; AFMAN 33-282; AFPD 33-2	
11.5.1. Definition	A
11.5.2. Vulnerabilities	A
11.6. Physical Security TR: AFI 31-101; AFPD 31-1	
11.6.1. Definition	A
11.6.2. Secure Area Access Management	X
11.6.3. Facility Security Requirements	X
11.6.4. Classified Material Control	
11.6.4.1. Storage	A
11.6.4.2. Transport	A
11.6.4.3. Handling	A
11.6.4.4. Destruction	X
11.6.4.5. Classified Waste	X
11.7. Information Assurance TR: AFI 33-200	

11.7.1. Definition	A
11.7.2. Threats and Vulnerabilities	A
11.7.3. Protective Measures	A
11.8. Information Conditions (INFOCON)	A
12. AIR AND SPACE EXPEDITIONARY FORCE (AEF)	
12.1. Equipment (e.g. LOGDET)	X
12.2. Personnel (e.g. MANFOR)	X
13. ENTERPRISE SYSTEMS TR: AFI 13 Series	
13.1. Defense Information Systems Network (DISN)	A
13.2. Defense Switched Network (DSN)	A
13.3. Non-secure Internet Protocol Router Network (NIPRNET) TR: DISACs 370-P120-3, 310-P70-73, 310-P70-74, 310-P70-75	A
13.4. Secure Networks	
13.4.1. Secret Internet Protocol Router Network (SIPRNET)	A
13.4.2. Defense Red Switch Network (DRSN)	A
14. ORGANIZATIONAL STRUCTURE	
14.1. Communication Squadron	X
14.2. Combat Communications Squadrons	X
14.3. Expeditionary Communications Squadron	X
14.4. Air Force Network Operations (AFNETOPS)	X
14.5. Air Force Network Operations Center (AFNOC)	X
14.6. Integrated Network Operations Security Center (INOSC)	X
14.7. Enterprise Service Unit (ESU)	X
14.8. Area Processing Center (APC)	X
14.9. Enterprise Service Desk (ESD)	X
15. CYBER OPERATIONS	
15.1. Structure	A
15.2. Missions	
15.2.1. Offensive	A
15.2.2. Defensive	A
15.2.3. Exploitation	A
15.2.4. Other (e.g. Influence Operations (IFO), Electronic Warfare (EW))	A
15.3. Network Warfare Fundamentals	

15.3.1. Control Systems (e.g. Supervisory Control and Data Acquisition (SCADA) networks)	A
15.3.2. Tactical Data Link (TADL) networks	A
15.3.3. Network Exploitation Capabilities	A
15.4. Cyber Capabilities	
15.4.1. Affects on adversary decision makers	A
15.4.2. Role of cyber operations in achieving military and national goals and objectives	A
15.4.3. Information Superiority	X
15.4.4. Role of 624th Operations Center	X
15.4.5. Role of 67th Cyberspace Wing	X
15.4.6. Role of 688th Cyberspace Wing	X
15.4.7. Role of an Air Operations Center (AOC)	X
15.4.8. Ops Defensive Measures	A
15.4.9. Ops Capabilities	A

Code	Definition
K	Subject Knowledge Training - The verb selection identifies the individual's ability to identify facts, state principles, analyze, or evaluate the subject.
P	Performance Training - Identifies that the individual has performed the task to the satisfaction of the course; however, the individual may not be capable of meeting the field requirements for speed and accuracy.
pk	Performance Knowledge Training - The verb selection identifies the individual's ability to relate simple facts, procedures, operating principles, and operational theory for the task.
-	No training provided in the course or CDC.
X	Training is required but not provided due to limitations in resources.
Each STS element is written as a behavioral statement. The detail of the statement and verb selection reflects the level of training provided by resident training and CDCs.	

Table source: AFI 36-2201, figure A4.4.

Task, Knowledge, and Proficiency Level

1. SECURITY+ CERTIFICATION

1.1. Network Security

- 1.1.1. Implement security configuration parameters on network devices and other technologies pk
- 1.1.2. Given a scenario, use secure network administration principles pk
- 1.1.3. Explain network design elements and components K
- 1.1.4. Given a scenario, implement common protocols and services pk
- 1.1.5. Given a scenario, troubleshoot security issues related to wireless networking pk

1.2. Compliance and Operational Security

- 1.2.1. Explain the importance of risk related concepts K
- 1.2.2. Summarize the security implications of integrating systems and data with third parties K
- 1.2.3. Given a scenario, implement appropriate risk mitigation strategies pk
- 1.2.4. Given a scenario, implement basic forensic procedures pk
- 1.2.5. Summarize common incident response procedures K
- 1.2.6. Explain the importance of security related awareness and training K
- 1.2.7. Compare and contrast physical security and environmental controls K
- 1.2.8. Summarize risk management best practices K

1.2.9. Given a scenario, select the appropriate control to meet the goals of security	pk
1.3. Threats and Vulnerabilities	
1.3.1. Explain types of malware	K
1.3.2. Summarize various types of attacks	K
1.3.3. Summarize social engineering attacks and the associated effectiveness with each attack	K
1.3.4. Explain types of wireless attacks	K
1.3.5. Explain types of application attacks	K
1.3.6. Analyze a scenario and select the appropriate type of mitigation and deterrent techniques	pk
1.3.7. Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities	pk
1.3.8. Explain the proper use of penetration testing versus vulnerability scanning	K
1.4. Application, Data and Host Security	
1.4.1. Explain the importance of application security controls and techniques	K
1.4.2. Summarize mobile security concepts and technologies	K
1.4.3. Given a scenario, select the appropriate solution to establish host security	pk
1.4.4. Implement the appropriate controls to ensure data security	pk
1.4.5. Compare and contrast alternative methods to mitigate security risks in static environments	K
1.5. Access Control and Identity Management	
1.5.1. Compare and contrast the function and purpose of authentication services	K
1.5.2. Given a scenario, select the appropriate authentication, authorization or access control	pk
1.5.3. Install and configure security controls when performing account management, based on best practices	pk
1.6. Cryptography	
1.6.1. Given a scenario, utilize general cryptography concepts	pk
1.6.2. Given a scenario, use appropriate cryptographic methods	pk
1.6.3. Given a scenario, use appropriate PKI, certificate management and associated components	Pk

<p><i>THIS BLOCK IS FOR IDENTIFICATION PURPOSES ONLY</i></p> <p>Personal Data – Privacy Act of 1974</p>		
PRINTED NAME OF TRAINEE (<i>Last, First, Middle Initial</i>)	INITIALS (<i>Written</i>)	LAST 4 OF SSAN
PRINTED NAME OF TRAINER AND CERTIFYING OFFICIAL AND WRITTEN INITIALS		
N/I	N/I	
N/I	N/I	
N/I	N/I	
N/I	N/I	
N/I	N/I	
N/I	N/I	

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		
<p>* 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)</p> <p>** 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.</p> <p>(-) This mark is used alone in Proficiency Codes Course columns to show that training is required but not given due to limitations in resources.</p> <p>NOTE: All tasks and knowledge items shown with a proficiency code are trained during wartime.</p> <p>(-) When this code is used in the Core & Wartime Tasks Column it indicates that the qualification is a local determination.</p> <p>(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.</p> <p>(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.</p> <p>(5-) When this code is used in the Core Task Column it indicates the CFM has selected this task as core 5-level tasks if loaded to the unit's WTA. This code indicates that training to satisfy this requirement is normally provided through OJT.</p> <p>(7-) When this code is used in the Core Task Column it indicates the CFM has selected this task as core 7-level tasks if loaded to the unit's WTA. This code indicates that training to satisfy this requirement is normally provided through OJT.</p>		

CDC Column. The use of proficiency coding indicates the level of knowledge training provided by the CDCs. Information pertaining to the meaning of the code can be located in the STS coding system table.

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
1. CYBER WARFARE OPERATIONS CAREER FIELD									
TR: AFH 33-337; AFIs 17-1201 (User Responsibilities and Guidance for Information Systems), 17-100 (Air Force Information Technology (IT) Service Management), 17-120 (Management of Cyberspace Support Activities), 36-2201, 38-201; AFMAN 36-2108; 1B4X1 CFETP; AFECD; AFODC; CJCSI 5215.01									
1.1. Structure	5					A	A	-	-
1.2. Progression within Air Force Specialty Code 1B4X1	5					A	A	-	-
1.3. Read CFETP 1B4X1 Part I	5					-	-	-	-
1.4. Air Force Specialty Code 1B4X1									
1.4.1. Explain Duties of AFSC	5					A	A	-	-
1.4.2. Explain Responsibilities of AFSC	5					A	A	-	-
1.4.3. AFSC Core Competencies	5					-	-	-	-
1.5. Related Cyber Career Fields									
1.5.1. Enlisted	5					A	-	-	-
1.5.2. Officer	5					A	-	-	-
1.5.3. Civilians, Contractors	5					A	-	-	-
1.6. Supervisory Duties									
1.6.1. Personnel Assignment Tools									
1.6.1.1. Unit Manpower Document (UMD)	7					-	-	A	-
1.6.1.2. Unit Personnel Management Roster (UPMR)	7					-	-	A	-
1.6.1.3. Authorization Change Request (ACR)	7					-	-	A	-
1.6.2. Orient Newly Assigned Personnel to Organization, Mission, Training and Certification Requirements	7					-	-	A	-
1.6.3. Training									
1.6.3.1. Air Force Training Program	5					-	B	-	-
1.6.3.2. Plan and Schedule On the Job Training (OJT)	5					-	-	-	-
1.6.3.3. Coordinate with Unit Training Manager	5					-	-	-	-
1.6.3.4. Conduct Initial Evaluation	5					-	-	-	-
1.6.3.5. Evaluate Adequacy of Training	5					-	-	-	-
1.6.3.6. Administer the CDC Program	5					-	-	-	-
1.6.3.7. Use Current CFETP	5					-	-	-	-
1.6.3.8. Conduct OJT	5					-	-	-	-
1.6.3.9. Evaluate OJT	5					-	-	-	-
1.6.3.10. Manage OJT Documentation	5					-	-	-	-
1.6.3.11. Identify Additional Formal Training Requirements	5					-	A	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
2. NETWORKING CONCEPTS									
TR: AFI 17-120; Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Prep Kit; IEEE 802									
2.1. Digital Numbering Systems (Internal Data Representation)									
2.1.1. Formats									
2.1.1.1. Binary	-					B	B	-	-
2.1.1.2. Hexadecimal	-					B	B	-	-
2.1.2. Physical Representation of Numbers	-					A	-	-	-
2.1.3. Convert Digital Numbers Across Formats	-					2b	b	-	-
2.1.4. Boolean Logic Arguments	-					B	B	-	-
2.2. Standards and Frameworks									
2.2.1. OSI Model	5					B	B	-	-
2.2.2. Protocol Data Units	-					A	-	-	-
2.2.3. Institute of Electrical and Electronics Engineers (IEEE) Standards									
2.2.3.1. IEEE 802	-					A	-	-	-
2.2.3.2. IEEE 802.1X	-					A	-	-	-
2.2.3.3. IEEE 802.3	-					A	-	-	-
2.2.3.4. IEEE 802.11	-					A	-	-	-
2.3. TCP/IP Suite									
2.3.1. Encapsulation/Decapsulation	5					B	B	-	-
2.3.2. Structure	5					B	B	-	-
2.4. Network Addressing									
2.4.1. Data-Link Layer									
2.4.1.1. Media Access Control (MAC)									
2.4.1.1.1. Address Structure	-					B	B	-	-
2.4.1.1.2. Ethernet Frame Structure	-					B	B	-	-
2.4.2. Network Layer									
2.4.2.1. Internet Protocol (v4 & v6)									
2.4.2.1.1. Address Structure	-					B	B	-	-
2.4.2.1.2. Packet Structure	-					B	B	-	-
2.4.2.1.3. Classful	-					B	B	-	-
2.4.2.1.4. Classless	-					B	B	-	-
2.4.2.1.5. Private/Public	-					B	B	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
2.4.2.1.6. Perform IPv4 Subnetting	5					2b	b	-	-
2.4.2.1.7. IPv6 Subnetting	-					A	-	-	-
2.4.2.1.8. Supernetting	-					A	-	-	-
2.5. Routing Protocols									
2.5.1. Interior	-					B	-	-	-
2.5.2. Exterior	-					B	-	-	-
2.5.3. Link-state	-					B	-	-	-
2.6. Networks									
2.6.1. Physical and Logical Topology									
2.6.1.1. Bus	-					B	-	-	-
2.6.1.2. Star	-					B	-	-	-
2.6.1.3. Mesh	-					B	-	-	-
2.6.1.4. Hybrid	-					B	-	-	-
2.6.2. Media Access Control Protocols	-					B	B	-	-
2.6.3. Packet Switched Networks	-					B	B	-	-
2.6.4. Circuit Switched Networks	-					A	A	-	-
2.6.5. Transmission Methods and Medium	-					A	A	-	-
2.6.6. Inter-Networking	-					A	B	-	-
2.6.7. Intra-Networking	-					A	B	-	-
2.6.8. Inter-Process Networking	-					B	-	-	-
2.7. 802.3 Local Area Networking									
2.7.1. Cisco Router and Switch									
2.7.1.1. Navigate Cisco IOS command line interface	-					2b	-	-	-
2.7.1.2. Configure Cisco Device Security IAW Applicable STIG	-					2b	-	-	-
2.7.1.3. Manipulate Networking Devices									
2.7.1.3.1. Interface Address	-					2b	-	-	-
2.7.1.3.2. VLAN	-					2b	-	-	-
2.7.1.3.3. Routing Protocol	-					2b	-	-	-
2.7.1.4. Enumerate Configuration and Connected Devices	-					2b	-	-	-
2.7.1.5. Utilize MAC Table	-					2b	-	-	-
2.7.1.6. Copy Device Configuration	-					2b	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
2.7.1.7. Erase Device Configuration	-					2b	-	-	-
2.7.1.8. Implement Access Control List	-					2b	-	-	-
2.7.1.9. Implement Port Security	-					2b	-	-	-
2.7.1.10. Configure Port Mirroring	-					2b	-	-	-
2.7.1.11. Copy System Image	-					2b	-	-	-
2.7.1.12. Enable Secure Remote Configuration Access	-					2b	-	-	-
2.8. Virtual Private Network									
2.8.1. Protocols	-					B	B	-	-
2.8.2. Components	-					B	B	-	-
2.9. 802.11 Wireless Networking									
2.9.1. Fundamentals									
2.9.1.1. Topology	-					B	B	-	-
2.9.1.2. Components	-					B	B	-	-
2.9.1.3. Security	-					B	B	-	-
2.9.2. Manipulate Wireless Access Point									
2.9.2.1. Connectivity	-					2b	-	-	-
2.9.2.2. Security	-					2b	-	-	-
2.10. Network Traffic Analysis									
2.10.1. Fundamentals	5					B	B	-	-
2.10.2. Network Traffic Analysis Process									
2.10.2.1. Capture Traffic	5					2b	-	-	-
2.10.2.2. Analyze Traffic	5					2b	-	-	-
2.10.2.3. Implement Session Recovery from Raw Traffic	-					2b	-	-	-
2.10.2.4. Identify Encoded Traffic	-					2b	-	-	-
2.10.2.5. Identify Malicious Traffic	-					2b	-	-	-
2.10.2.6. Identify the hardware manufacturer from network traffic	-					2b	-	-	-
2.10.2.7. Identify the OS version from network traffic	-					2b	-	-	-
2.10.2.8. Identify the patch release of OS software from network traffic	-					2b	-	-	-
2.10.2.9. Identify Services and Applications on a Network	5					2b	-	-	-
3. OPERATING SYSTEM CONCEPTS									
TR: AF e-Learning, Linux: Basic System Administration Learning Track; UNIX Essentials Learning Track; FedVTE: Windows Operating System Security									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
3.1. Operating System Types									
3.1.1. Windows (Desktop/Server)									
3.1.1.1. Components									
3.1.1.1.1. Kernel	5					B	B	-	-
3.1.1.1.2. Registry	5					B	B	-	-
3.1.1.1.3. Drivers	5					B	B	-	-
3.1.1.1.4. Boot Process	5					B	B	-	-
3.1.1.2. File Structure									
3.1.1.2.1. FAT	5					B	B	-	-
3.1.1.2.2. NTFS	5					B	B	-	-
3.1.1.3. Utilize CLI	5					2b	-	-	-
3.1.1.4. Utilize GUI	5					2b	-	-	-
3.1.1.5. Manipulate System									
3.1.1.5.1. User Accounts	5					2b	-	-	-
3.1.1.5.2. File Systems	5					2b	-	-	-
3.1.1.5.3. Network Shares	5					2b	-	-	-
3.1.1.5.4. Network Settings	5					2b	-	-	-
3.1.1.5.5. Services	5					2b	-	-	-
3.1.1.5.6. Firewall	5					2b	-	-	-
3.1.1.5.7. Logs	5					2b	-	-	-
3.1.1.6. Utilize Registry	5					2b	-	-	-
3.1.2. *NIX									
3.1.2.1. Components									
3.1.2.1.1. Kernel	5					B	B	-	-
3.1.2.1.2. Drivers	5					B	B	-	-
3.1.2.1.3. Boot Process	5					B	B	-	-
3.1.2.1.4. /proc	5					B	B	-	-
3.1.2.2. File Structure	5					B	B	-	-
3.1.2.3. Utilize CLI	5					2b	-	-	-
3.1.2.4. Utilize GUI	5					2b	-	-	-
3.1.2.5. Linux-based distros	5					-	A	-	-
3.1.2.6. Manipulate System									
3.1.2.6.1. User Accounts	5					2b	-	-	-
3.1.2.6.2. File Systems	5					2b	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
3.1.2.6.3. Network Shares	5					2b	-	-	-
3.1.2.6.4. Network Settings	5					2b	-	-	-
3.1.2.6.5. Services	5					2b	-	-	-
3.1.2.6.6. IP tables	5					2b	-	-	-
3.1.2.6.7. Packages	5					2b	-	-	-
3.1.2.6.8. Logs	-					2b	-	-	-
3.1.2.7. Utilize /proc	-					2b	-	-	-
3.1.3. Mobile OSs									
3.1.3.1. Overview	-					B	-	-	-
3.1.3.2. Components	-					B	-	-	-
3.1.3.3. File Structure	-					-	-	-	-
3.2. Virtualization	-					B	-	-	-
3.3. Scripting									
3.3.1. Batch	-					2b	-	-	-
3.3.2. Create Powershell Script	-					2b	-	-	-
3.3.3. Create Bash Script	-					2b	-	-	-
3.3.4. Create Python Script	-					2b	-	-	-
4. CYBER WARFARE CONCEPTS AND FUNDAMENTALS T R: AFTTP 3-10.3; AFDD 3-12; AFPD 17-2 (Cyberspace Operations); AFI 17-201 (C2 for Cyberspace Operations), 17-120; CJCSM 6510.01B; JP 3-12									
4.1. Fundamentals									
4.1.1. Doctrine, Policy, TTPs and Guidance	5					A	B	-	-
4.1.2. National Strategy	5					A	B	-	-
4.1.3. Command and Control	5					A	B	-	-
4.1.4. Department of Defense Information Network (DoDIN)	5					A	B	-	-
4.1.5. Cyber Organizations and Missions	5					A	B	-	-
4.1.6. Cyber Mission Force									
4.1.6.1. Definitions and Roles/Responsibilities	5					A	B	-	-
4.1.6.2. Command and control	5					A	B	-	-
4.1.6.3. Mission Areas									
4.1.6.3.1. Defend the Nation	5					A	B	-	-
4.1.6.3.2. Operate and Defend the DODIN	5					A	B	-	-
4.1.6.3.3. Combatant Command Support	5					A	B	-	-
4.1.6.4. Mission Forces									

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
4.1.6.4.1. National Mission Force	5					A	B	-	-
4.1.6.4.2. Protection Force	5					A	B	-	-
4.1.6.4.3. Combat Mission Force	5					A	B	-	-
4.1.7. Cyber Warfare Operations	5					A	B	-	-
4.1.8. Information Operations	5					A	B	-	-
4.2. Threat Types									
4.2.1. Internal	5					A	B	-	-
4.2.2. External	5					A	B	-	-
4.2.3. State Sponsored	5					A	B	-	-
4.2.4. Non-State Sponsored	5					A	B	-	-
4.3. OCO/DCO Theory and Methodology									
4.3.1. Offensive Theory	5					B	B	B	-
4.3.2. Defensive Theory	5					B	B	B	-
4.3.3. Offensive Methodology	5					B	-	-	-
4.3.4. Defensive Methodology	5					B	-	-	-
4.3.5. Identify Offensive Methods									
4.3.5.1. Buffer Overflow Tactics and Techniques	5					B	B	-	-
4.3.5.2. Privilege Escalation	5					B	B	-	-
4.3.5.3. Rootkits	5					B	B	-	-
4.3.5.4. Redirection and Triggering	5					B	B	-	-
4.3.5.5. Tunneling	5					2b	-	-	-
4.3.5.6. Collection/Exfiltration	5					B	B	-	-
4.3.5.7. Social Engineering	5					B	B	-	-
4.3.5.8. Web Exploitation	5					B	B	-	-
4.3.5.9. Persistent Access	5					B	B	-	-
4.3.5.10. Man-in-the-Middle	5					B	B	-	-
4.3.5.11. (Distributed) Denial of Service	5					B	B	-	-
4.3.5.12. Obfuscation	5					B	B	-	-
4.3.6. Identify Defensive Methods									
4.3.6.1. Encryption	5					B	B	-	-
4.3.6.2. Secure Configurations	5					B	B	-	-
4.3.6.3. Secure Enclaves	5					B	B	-	-
4.3.6.4. Vulnerability Scanning	5					B	B	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
4.3.6.5. Boundary Protection	5					B	B	-	-
4.3.6.6. Intrusion Detection/Pretention (Host/Network)	5					B	B	-	-
4.4. Utilize Tools									
4.4.1. Reconnaissance	-					2b	-	-	-
4.4.2. Vulnerability Assessment	-					2b	-	-	-
4.4.3. Password Cracking	-					2b	-	-	-
4.4.4. Exploitation	-					2b	-	-	-
4.4.5. Wireless	-					2b	-	-	-
4.4.6. Persistent Access	-					2b	-	-	-
4.4.7. Reverse Engineering	-					2b	-	-	-
4.4.8. Forensics	-					2b	-	-	-
4.4.9. Honeypots	-					2b	-	-	-
4.4.10. Intrusion Detection	-					2b	-	-	-
4.5. Information Assurance									
4.5.1. Roles and Responsibilities	5					B	B	-	-
4.5.2. Emissions Security	5					-	B	-	-
4.5.3. Communication Security	5					-	B	-	-
4.5.4. Computer Security	5					-	B	-	-
4.5.5. Operations Security	5					B	B	-	-
4.5.6. Physical Security	5					-	B	-	-
4.5.7. Information Security	5					-	B	-	-
4.6. Crew Operations									
4.6.1. Operations Training	5					B	B	-	-
4.6.2. Standardization and Evaluation	5					B	B	-	-
4.6.3. Operational Procedures	5					B	B	-	-
4.6.4. Crew Resource Management	5					-	A	B	-
5. LAWS AND ETHICS									
TR: AFDD 3-13 (Information Operations); AFPD 10-7; AFPD 17-2 (Cyberspace Operations); USC TITLE 10, 17, 18, 50; Joint Pub 3-13, Information Operations; Joint Pub 3-12, Cyberspace Operations; Health Insurance Portability and Accountability Act (HIPAA)									
5.1. US Codes (Titles 10, 15, 17, 18, 32, 50)	5					A	B	-	-
5.2. Rules of Engagement (ROE)									
5.2.1. Policy	5					A	B	-	-
5.2.2. Security Tools	5					A	B	-	-
5.2.3. Cyber Management Ethics	5					A	B	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
5.2.4. System Monitoring	5					A	B	-	-
5.3. Special Data Protection (i.e. Sensitive Personnel Information)	-					A	-	-	-
5.4. Policy and Law									
5.4.1. Executive Orders	5					A	B	-	-
5.4.2. International Laws Affecting Electronic Communications	5					A	B	-	-
5.4.3. US Law									
5.4.3.1. Military Law	5					A	B	-	-
5.4.3.2. Intellectual Property Laws	5					A	B	-	-
5.4.3.3. US Law Specific to Electronic Crimes	5					A	-	-	-
6. CYBER SYSTEMS TR: AFTTP 3-10.3; AFDD 3-12; AFPD 10-17; AFI 31-401; JP 1-02; JP 3-12									
6.1. Capabilities									
6.1.1 Workstations/Servers	5					B	B	-	-
6.1.2. Data Networks	5					B	B	-	-
6.1.3. Voice Networks	5					B	B	-	-
6.1.4. Space Networks	-					-	B	-	-
6.1.5. Battlefield Networks	-					-	B	-	-
6.1.6. Industrial Systems	-					A	B	-	-
6.1.7. AFIN	5					B	B	-	-
6.1.8. Websites/Databases	5					B	B	-	-
6.2. Vulnerabilities									
6.2.1. Workstations/Servers	5					B	B	-	-
6.2.2. Data Networks	5					B	B	-	-
6.2.3. Voice Networks	5					B	B	-	-
6.2.4. Space Networks	-					-	B	-	-
6.2.5. Battlefield Networks	-					-	B	-	-
6.2.6. Industrial Systems	-					A	B	-	-
6.2.7. AFIN	5					B	B	-	-
6.2.8. Websites/Databases	5					B	B	-	-
6.3. Components									
6.3.1 Workstations/Servers	-					B	-	B	-
6.3.2. Data Networks	-					B	-	B	-
6.3.3. Voice Networks	-					B	-	B	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
6.3.4. Space Networks	-					-	-	B	-
6.3.5. Battlefield Networks	-					-	-	B	-
6.3.6. Industrial Systems	-					A	-	B	-
6.3.7. AFIN	-					B	-	B	-
6.3.8. Websites/Databases	-					B	-	B	-
6.4. Design									
6.4.1 Workstations/Servers	-					B	-	B	-
6.4.2. Data Networks	-					B	-	B	-
6.4.3. Voice Networks	-					B	-	B	-
6.4.4. Space Networks	-					-	-	B	-
6.4.5. Battlefield Networks	-					-	-	B	-
6.4.6. Industrial Systems	-					A	-	B	-
6.4.7. AFIN	-					B	-	B	-
6.4.8. Websites/Databases	-					B	-	B	-
6.5. Security									
6.5.1. Workstations/Servers	-					B	-	B	-
6.5.2. Data Networks	-					B	-	B	-
6.5.3. Voice Networks	-					B	-	B	-
6.5.4. Space Networks	-					-	-	B	-
6.5.5. Battlefield Networks	-					-	-	B	-
6.5.6. Industrial Systems	-					A	-	B	-
6.5.7. AFIN	-					B	-	B	-
6.5.8. Websites/Databases	-					B	-	B	-
7. JOINT PLANNING									
TR: JP 1-0; JP 2-0; JP 5-0; JP 3-12; CJCSM 3122.07 Vol I/II									
7.1. Lines of Operations									
7.1.1. DODIN	5					A	A	B	-
7.1.2. DCO	5					A	A	B	-
7.1.3. OCO	5					A	A	B	-
7.2. Joint Command and Planning Process									
7.2.1. Structure and Organization	5					A	A	B	-
7.2.2. Levels of War	5					A	A	B	-
7.2.3. Roles and Responsibilities	-					A	A	B	-
7.3. Command and Control (C2)	5					-	-	B	-
7.4. Authorities	5					-	-	B	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
7.5. Orders	5					A	A	B	-
7.6. Planning Process Defined (JPP)									
7.6.1. Deliberate Planning	5					A	A	B	-
7.6.2. Crisis Action Planning	5					A	A	B	-
7.7. Integrated Joint Special Technical Operations (IJSTO)									
7.7.1. Process	-					A	A	B	-
7.7.2. Roles and Responsibilities	-					A	A	B	-
7.8. Cyberspace Operational Planning									
7.8.1. Cyber C2	5					B	-	B	-
7.8.2. Synchronization	5					A	B	B	-
7.8.3. Weaponneering	5					A	B	B	-
7.8.4. Asset/Target Analysis	5					-	-	B	-
7.8.5. Intelligence Gain/Loss	5					A	A	B	-
7.8.6. Technical Gain/Loss	5					A	A	B	-
7.8.7. Deconfliction	5					A	B	B	-
7.8.8. Conduct OCO and DCO Mission Planning	-					2b	b	-	-
7.8.9. Cyber Ops Assessments									
7.8.9.1. MOP/MOE	5					A	B	B	-
7.8.9.2. Conducting Ops Assessment	5					A	B	B	-
7.8.9.3. Battle Damage Assessment	5					A	B	B	-
8. CONDUCT OCO/DCO TR: AFTTP 3-10.3; AFDD 3-12; AFPD 17-2; AFI 16-1404; DoD Dictionary of Military and Associated Terms; JP 3-12									
8.1. Generate a Denial or Manipulation Effect									
8.1.1. Workstations/Servers	-					2b	-	-	-
8.1.2. Data Networks	-					2b	-	-	-
8.1.3. Voice Networks	-					-	-	-	-
8.1.4. Wireless Networks	-					2b	-	-	-
8.1.5. Websites/Databases	-					2b	-	-	-
8.1.6. Space Networks	-					-	-	-	-
8.1.7. Battlefield Networks	-					-	-	-	-
8.1.8. Industrial Systems	-					1a	-	-	-
8.2. Actively Defend									
8.2.1. Workstations/Servers	-					2b	-	-	-
8.2.2. IP Networks	-					2b	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
8.2.3. Voice Networks	-					-	-	-	-
8.2.4. Wireless Networks	-					2b	-	-	-
8.2.5. Websites/Databases	-					2b	-	-	-
8.2.6. Space Networks	-					-	-	-	-
8.2.7. Battlefield Networks	-					-	-	-	-
8.2.8. Industrial Systems	-					1a	-	-	-
8.2.9. AFIN	-					2b	-	-	-
9. INCIDENT RESPONSE									
TR: AFTTP 3-10.3; AFDD 3-12; AFPD 17-2; AFI 16-1404; DoD Dictionary of Military and Associated Terms; JP 3-12									
9.1. Methodology	5					B	-	-	-
9.2. Incident Categories	5					B	-	-	-
9.3. Remote Evidence Collection	-					-	-	-	-
9.4. Reporting	-					-	-	-	-
9.5. Forensics	-					B	-	-	-
9.6. Conduct Investigation	-					-	-	-	-
9.7. Incident Recovery	-					-	-	-	-
10. CAPABILITY DEVELOPMENT									
TR: AFTTP 3-10.3; AFDD 3-12; AFPD 17-2; AFI 16-1404; DoD Dictionary of Military and Associated Terms; JP 3-12									
10.1. Fundamentals	-					B	-	-	-
10.2. Secure Programming	-					-	-	-	-
10.3. Agile Development Process	-					-	-	-	-
10.4. Reverse Engineering	-					B	-	-	-
10.5. Weaponization	-					-	-	-	-
10.6. Provisioning	-					-	-	-	-
10.7. Operational Frameworks	-					-	-	-	-
10.8. Functional Evaluation Fundamentals	-					-	-	-	-
10.9. Fuzzing Fundamentals	-					-	-	-	-
10.10. Real-Time Operations and Innovation	-					-	-	-	-
11. INTELLIGENCE FUNDAMENTALS									
TR: JP 2-0, JP 2-01									
11.1. Data, Information, and Intelligence (Differences and Relationships)	5					-	-	-	-
11.2. Identify the Intelligence Process	7					-	-	-	-
11.3. Intelligence Sources/Disciplines (e.g. OSINT)	5					-	-	-	-
11.4. Intelligence Reports (e.g. IIR)	7					A	-	B	-
11.5. Tactics from Intel Sources	-					A	-	-	-

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE TASKS	3. OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	Course	CDC	CDC	Course
11.6. Identify the Joint Intelligence Preparation of the Environment (JIPOE) process	7					-	-	-	-
11.7. Identify PMESII	7					-	-	-	-
12. ISR COLLECTION MANAGEMENT TR: JP 2-0, JP 2-01, JP 3-12									
12.1. Intelligence Limitations/Problems	5					-	-	-	-
12.2. Collection Requirements	5					-	-	-	-
12.3. Commander's Critical Information Requirement (CCIR)	7					-	-	-	-
12.4. Priority Intelligence Requirement (PIR)	7					-	-	-	-
12.5. Essential Elements of Information (EEI)	7					-	-	-	-
12.6. Request for Information (RFI)	7					-	-	-	-
13. INTELLIGENCE INFORMED OPERATIONS TR: JP 2-0, JP 2-01, JP 5-0									
13.1. Applied to cyberspace operations, identify how intelligence informs Mission Analysis activities	7					-	-	-	-
13.2. Applied to cyberspace operations, identify how intelligence informs the operational risk assessment	7					-	-	-	-
13.3. Applied to cyberspace operations, identify how intelligence drives the tactical planning and/or operations cycle	7					-	-	-	-

Section B - Course Objective List

4. There is currently no advanced course. This area is reserved.

Section C - Support Materials

5. The most current products (JQSs/QTPs) can be found at the 81 TRSS/TSQ web page, and are available for download from the web site at <https://cs2.eis.af.mil/sites/10445/default.aspx>. Procedures for requesting product development are found in AFI 17-204.

There are currently no support materials. This area is reserved.

Section D - Training Course Index

6. **Purpose.** This section of the CFETP identifies training courses available for continuation/supplemental training. For information on all formal courses, refer to the Air Force Education and Training Course Announcements (ETCA) database, at <https://app10-eis.aetc.af.mil/etca/SitePages/Home.aspx>

7. Air Force In-Residence Courses.

<u>Course Number</u>	<u>Course Title</u>	<u>Location</u>
WCYBER200	Cyberspace 200	Wright Patterson AFB, OH
WCYBER300	Cyberspace 300	Wright Patterson AFB, OH
E7OAT17D4	Cyberspace 400	Washington DC

8. Air University A4/A6 Courses.

For a current listing of Air University A4/6 courses go to <http://www.au.af.mil/au/afiadl/>.

9. Exportable Courses.

For a current list of the available CBT courses refer to *AF e-Learning* at <https://www.my.af.mil/>.

For a current list of available online courses on FEDVTE refer to <https://fedvte.usalearning.gov/>.

Section E - MAJCOM Unique Requirements

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