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

CFETP 1B4X1
Parts I and II
16 Oct 2023

AFSC 1B4X1

CYBER WARFARE OPERATIONS

CAREER FIELD EDUCATION AND TRAINING PLAN

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

TABLE OF CONTENTS

PART I

Part II

OPR: 333TRS/TRR
Approved By: CMSgt Joseph R. Ippolito, 1BXXX AFCFM (HAF A2/6C)
Supersedes: CFETP 1B4X1, dated 15 Jul 2018
Pages: 72

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 myLearning 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 to implement; Section B identifies career field progression information, duties and responsibilities, training strategies, and the 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/AFCDA (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.

Cyber Effects Operations (CEO). Delivering an effect within the cyberspace war fighting domain.

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 AFCFMs 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 by defeating on-going or imminent malicious cyber activities/actors (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://usaf.dps.mil/teams/app10-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 myLearning. 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 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.

Work Center Job Qualification Standard (WCJQS). Work center document that standardizes on-the-job training for Airmen assigned to cyber warfare operations. This document identifies

the majority of duties and tasks required to attain qualification. Use this document to plan and record all duty-position related training, and as a basis for preparing a Master Task Listing (MTL) for each functional area. The WCJQS is used by unit training managers, supervisors, trainers, trainees, and other training functions to plan, conduct, and document OJT.

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 AFCFM, HAF A2/6C. 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, additions, and 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. Plans and conducts Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), Department of Defense Information Network (DoDIN) Operations, and Cyber Network Operations (CNO)/cryptologic activities 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, degrade, disrupt, destroy, manipulate, and mitigate adversarial access to sovereign national or partner 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(s) to be awarded AFSC 1B431. Current requirements were identified and validated during the STRT held 12-16 June 2023.

5.2. Cyber Warfare Operations Journeyman (1B451). To qualify for the 5-skill level, Airmen must: (1) complete the 5-level Career Development Course(s) (CDC), if applicable; (2) meet mandatory requirements listed in the specialty description in the Air Force Enlisted Classification Directory (AFECD) and CFETP. Once qualifications are met, Airmen must be upgraded unless not recommended by their commander. Supervisors may identify and standardize local tasks for inclusion in the STS with the AFCFM approval. Coordinate requests for AFCFM approval through the MAJCOM FM. UGT consists of completing duty position training and/or certification, any specified core task training, and appropriate courses as outlined in the WCJQS.

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 CDCs, if applicable (3) meet mandatory requirements listed in the specialty description in the AFECD and CFETP. Once qualifications are met, Airmen must be upgraded unless not recommended by their commander. Individuals in retraining status are subject to the same requirements. Supervisors may identify and standardize local tasks for inclusion in the STS with the AFCFM approval. Coordinate requests for AFCFM approval through the MAJCOM FM.

5.4. Cyber Warfare Operations Superintendent (1B491). SMSgts must upgrade upon promotion notification and completion of mandatory requirements listed in the AFECD.

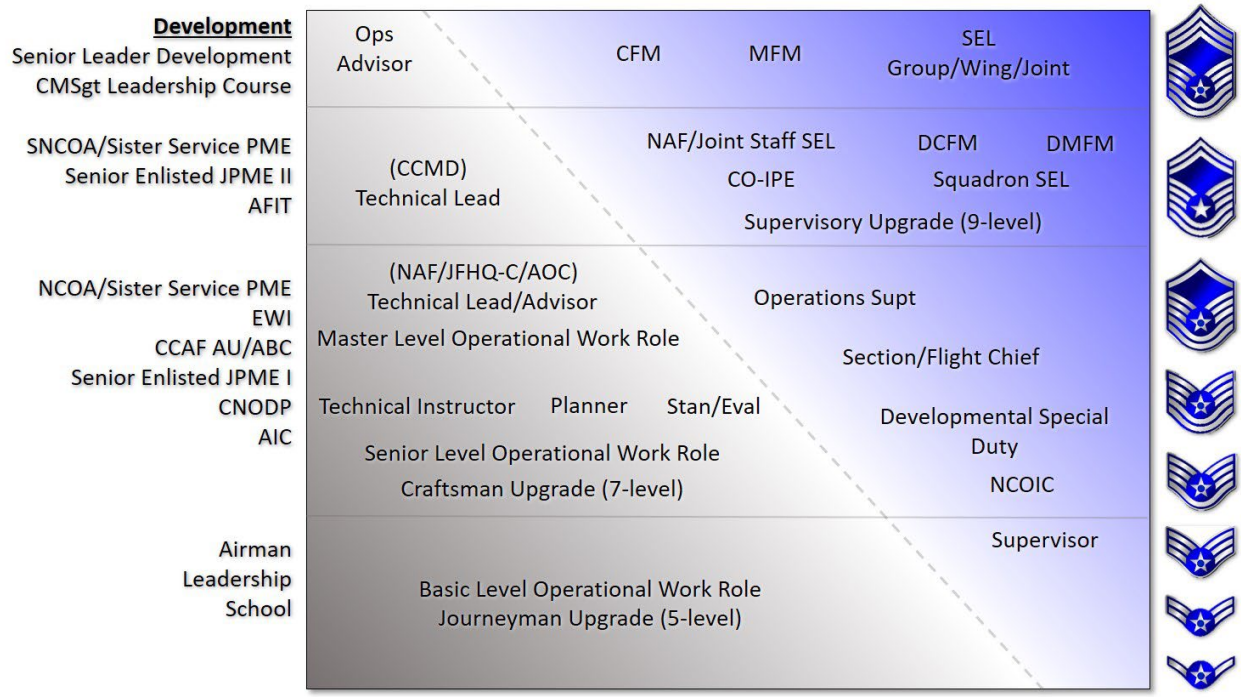
5.5. Occupational Badges. The Cyberspace Operations Badge is the Cyber Warfare Operations occupational badge and is authorized to be worn by 1BXXX Airmen. See AFI 36-2903, *Dress and Personal Appearance of Air Force Personnel* for proper wear guidance. The below guidance outlines requirements for the wear of the Basic, Senior, and Master Cyberspace Operations badges.

5.5.1. Basic Cyberspace Operations Badge: This badge will be worn upon graduation of the Cyber Warfare Operations Initial Skills Training Course.

5.5.2. Senior Cyberspace Operations Badge: This badge will be worn after award of 7-skill level.

5.5.3. Master Cyberspace Operations Badge: This badge will be worn upon award of 9-skill level or worn as a Master Sergeant with 5 years experience within the 1BXXX, Cyber Warfare Operations career field.

1BXXX Career Path Chart



5.6. Enlisted Development Team (EDT).

5.6.1. 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 into key leadership positions across the Air Force. CMSgts, SMSgts, and MSgts will be boarded by individual EDT panels. The EDT may recommend other developmental opportunities for Cyber Warfare Airmen 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.

5.6.2. Process: EDT panel members are appointed by the 1BXXX AFCFM and are comprised of senior 1B leaders across the force with the appropriate strategic vision and experience to ensure diversity and inclusion are considered. Members meeting the EDT can express their own desires through the Individual Development Plan (IDP) for consideration by the board. During the EDT review process, EDT panel members assess billets for key leadership or key

development position designation. EDT panel members will also board and evaluate each 1Bs past performance, duty history and experience, scope of responsibility, decorations, and IDP input to determine appropriate development and vector recommendations. Once complete, 1Bs will be made aware of their vector/tier through myVector.

6. Training Decisions.

6.1. Three-Skill Level Course. The 3-skill level course is overhauled 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. 7-level core task requirements as well as CDC requirements have been adjusted to meet the needs of the operational community.

6.4. Nine-Skill Level Upgrade Requirements. Completion of the Cyber Defense Operations Superintendent Course has been removed as a 9-level upgrade requirement. However, 1B4 E-7s and above may enroll and take the course as desired. The course may be found on the AETC myLearning site under course identifier AFQTP1D7XX-225F.

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 Weaponeering 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 training CCMD and Joint Force Command (JFC) staffs on the integration of cyberspace operations into CCMD/JFC level planning. Its scope has been expended 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 and 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 uses 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 intelligene/security-related specialties the opportunity to enroll in professional intelligence undergraduate or graduate-level sudy 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 MSTI is a graduate degree program requiring complation of an 11-month course of study consisting of five required courses, seven electives, and thesis courses. 1D7/1B4 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. Baccaulaureate 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 stude best practices with leaders of industry. The assignment is ten months in length. Since 2015, 1B4s selected for this program have been assigned to companies such as Amazon, Apple, and USAA. However, the CFM will source appropriate industry partners to maximize the program's return on investment once the member completes the fellowship. 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 (AFIT), 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 futher 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.milsuite.mil/book/groups/af-cnodp.

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

	GRADE REQUIREMENTS		
Education and Training Requirements	***Rank***	***Earliest Sew-On***	***High Year Of Tenure (HYT)***
Basic Military Training School (BMTS)			
Apprentice Technical School (3-Skill Level)	A1C		
Upgrade To Journeyman (5-Skill Level) - Specific AFJQSs/AFQTPs for equipment at assigned location by duty position. (see NOTE 2) - Complete CDC if applicable - No minimum time in training	A1C SrA	28 months	10 Years
Airman Leadership School - Must be a SrA with 48 months time in service or be an SSgt Selectee. - Resident graduation is a prerequisite for SSgt sew-on (Active Duty Only).	**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) - Minimum rank of SSgt or SSgt Selectee. - Complete CDC if applicable. - Specific AFJQSs/AFQTPs for equipment at assigned location by duty position. - No minimum time in training	SSgt (Sel)	3 years	20 years

1B4X1 CYBER WARFARE OPERATIONS CAREER PATH			
	GRADE REQUIREMENTS		
Education and Training Requirements	***Rank***	***Earliest Sew-On***	***High Year Of Tenure (HYT)***
Non-Commisioned Officer Academy - Must be a TSgt or TSgt Selectee. - Resident graduation is a prequisite for MSgt sew-on (Active Duty Only).	TSgt	5 years	22 years
USAF Senior NCO Academy - Must be a SMSgt or SMSgt Selectee. - Resident graduation is a prerequisite for SMSgt sew-on (Active Duty Only). - Guard and Reserve who have completed NCOA may enroll in SNCOA DLC.	MSgt	8 years	24 years
Upgrade To Superintendent (9-Skill Level) **MANDATORY** - Minimum rank of SMSgt or SMSgt Selectee.	SMSgt (Sel)	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 myFSS for current information: https://myfss.us.af.mil/ or DAFI 36-2670, *Total Force Development.*

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) are 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 70 on the Air Force Electronic Data Processing Test. Armed Services Vocational Aptitude Battery (ASVAB) or Armed Forces Classification Test (AFCT) must have been taken within 2 years from date retraining application is submitted. Requires routine access to Top Secret material or similar environment, completion of a current Single Scope Background Investigation (SSBI) according to DAFMAN 16-1405, *Department of the Air Force Personnel Security Program*, 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 DAFMAN 16-1405. For award and retention of 1B431, individual must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and DAFMAN 17-1301, *Computer Security (COMPUSEC).*
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	Completion of the 1B451 Career Development Course if applicable. Completion of all STS core tasks. Completion of applicable AFJQS/AFQTPs. Completion of all local tasks assigned for the duty position to include Crew Position Certification if required for duty position.
EXPERIENCE	Qualification in and possession of AFSC 1B431 Experience performing Cyber Warfare Operations functions as outlined in Section B, para. 4.
OTHER	Requires routine access to Top Secret material or similar environment, completion of a current Single Scope Background Investigation (SSBI) according to DAFMAN 16-1405, is mandatory for award and retention of this skill level. For award and retention of 1B451, individual must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and DAFMAN 17-1301, *Computer Security (COMPUSEC).*
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	Completion of the 1B471 Career Development Course if applicable. Completion of all STS core tasks. Completion of applicable AFJQS/AFQTPs. Completion of all local tasks assigned for the duty position to include Crew Position Certification if required for duty position.
EXPERIENCE	Qualification in and possession of AFSC 1B451 Experience performing or supervising Cyber Warfare Operations functions as outlined in Section B, para. 4.
OTHER	Requires routine access to Top Secret material or similar environment, completion of a current Single Scope Background Investigation (SSBI) according to DAFMAN 16-1405, is mandatory for award and retention of this skill level. For award and retention of 1B471, individual must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and DAFMAN 17-1301, *Computer Security (COMPUSEC).*
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	All 1B471 knowledge qualifications apply to the 1B491 requirements
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 DAFMAN 16-1405, is mandatory for award and retention of this skill level. For award and retention of 1B491, individual must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and DAFMAN 17-1301, *Computer Security (COMPUSEC).*
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://usaf.dps.mil/teams/app10-etca/SitePages/Home.aspx, course ID: E3ALR1B431 0A1A

10.5.2. 1B4X1 CDCs if available, 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.

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 myLearning at https://lmsjets.cce.af.mil/moodle/course/index.php?categoryid=47

10.5.3.1. Procedures for requesting development of AFJQSs/AFQTPs are contained in AFMAN 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 144 days.

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.

2. Purpose. As prescribed in DAFMAN 36-2689, *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 DAFMAN 36-2689.

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://lms-jets.cce.af.mil/moodle/course/index.php?categoryid=10 CDC listings.

2.4. Qualitative Requirements. Attachment 2 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: None.

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 DAFMAN 36-2689, *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 SNCOs 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

LEAH G. LAUDERBACK, Lt Gen, USAF
Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance and Cyber Effects Operations

Attachments:
1. Security+ Certification CTS
2. 1B4X1 STS

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: DAFMAN 36-2689, Table 5.2

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

THIS BLOCK IS FOR IDENTIFICATION PURPOSES ONLY Personal Data – Privacy Act of 1974		
PRINTED NAME OF TRAINEE *(Last, First, Middle Initial)*	INITIALS *(Written)*	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

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

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

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

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

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

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

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

(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.

(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.

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. TASK, KNOWLEDGE, AND TECHNICAL REFERENCE	2. CORE & WARTIME TASKS	3. CERTIFICATON FOR OJT					4. PROFICIENCY CODE USED TO INDICATE TRAINING/INFORMATION PROVIDED			
		A	B	C	D	E	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	CERTIFIER INITIALS	COURSE	COURSE	COURSE	COURSE
1. CYBER WARFARE OPERATIONS FUNDAMENTALS 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), DAFMAN 36-2689, 38-201; AFMAN 36-2108; 1B4X1 CFETP; AFECD; AFOCD; CJCSI 5215.01										
1.1. Cyber Warfare Career Field Fundamentals										
1.1.1. Structure	-						A	-	-	-
1.1.2. Progression within Air Force Specialty Code 1B4X1	-						A	-	-	-
1.1.3. Explain Duties and Responsibilities of AFSC	-						A	-	-	-
1.1.4. History of Military Cyber	-						B	-	-	-
1.2. Related Cyber Career Fields										
1.2.1. Enlisted	-						B	-	-	-
1.2.2. Officer	-						B	-	-	-
1.2.3. Civilians, Contractors	-						B	-	-	-
1.3. Critical Thinking										
1.3.1. Cognitive Bias	-						A	-	-	-
1.4. Fundamentals										
1.4.1. Doctrine, Policy, TTPs and Guidance	-						A	-	-	-
1.4.2. National Strategy	-						A	-	-	-
1.4.3. Command and Control	-						A	-	-	-
1.4.4. Department of Defense Information Network (DoDIN)	-						A	-	-	-
1.4.5. Cyber Organizations and Missions	-						A	-	-	-
1.5. Cyber Mission Force										
1.5.1. Definitions and Roles/Responsibilities	-						A	-	-	-
1.5.2. Command and control	-						A	-	-	-
1.6. Mission Areas										
1.6.1. Defend the Nation	-						A	-	-	-

1.6.2. Operate and Defend the DODIN	-						A	-	-	-
1.6.3. Combatant Command Support	-						A	-	-	-
1.7. Mission Forces										
1.7.1. Cyber National Mission Force	-						A	-	-	-
1.7.2. Cyber Protection Force	-						A	-	-	-
1.7.3. Cyber Combat Mission Force	-						A	-	-	-
1.7.4. Cyber Warfare Operations	-						A	-	-	-
1.7.5. Information Operations	-						B	-	-	-
1.8. Crew Operations										
1.8.1. Operations Training	-						A	-	-	-
1.8.2. Standardization and Evaluation	-						A	-	-	-
1.8.3. Operational Procedures	-						A	-	-	-
1.8.4. Crew Resource Management	-						B	-	-	-
1.9. Operational Note Taking										
1.9.1. Operational Note Taking Applications	-						B	-	-	-
1.9.2. Take Effective Notes for Operational Mission Execution	-						2b	-	-	-
2. 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)										
2.1. US Codes										
2.1.1. US Codes (Titles 15, 17, 32)	-						A	-	-	-
2.1.2. US Codes (Title 10, 18, 50)	-						B	-	-	-
2.2. Policy and Law										
2.2.1. Executive Orders	-						A	-	-	-
2.2.2. International Laws Affecting Electronic Communications	-						B	-	-	-
2.3. US Law										

2.3.1. Intellectual Property Laws	-						A	-	-	-
2.3.2. US Law Specific to Electronic Crimes	-						A	-	-	-
2.3.3. Cyber Warfare Authorities	-						B	-	-	-
2.3.4. Authority to operate/connect	-						A	-	-	-
3. INTELLIGENCE IN CYBER WARFARE										
3.1. Intelligence Fundamentals										
3.1.1. Role of ISR w/in Cyber	-						B	-	-	-
3.1.2. Explain the function of the United States SIGINT System (USSS)	-						A	-	-	-
3.1.3. Describe the type of information provided by each intelligence discipline (ex. SIGINT, HUMINT, OSINT, ELINT, FISINT)	-						B	-	-	-
3.1.4. Describe the purpose and relationship between intelligence discipline (ex. SIGINT, HUMINT, OSINT)	-						B	-	-	-
3.1.5. Define the CRITIC Program	-						A	-	-	-
3.1.6. Identify CRITIC reportable information	-						A	-	-	-
3.1.7. The five steps of the Intelligence Cycle	-						B	-	-	-
3.1.8. Describe the correlation between IT purchase orders and target analysis	-						B	-	-	-
3.1.9. Data, Information, and Intelligence (Differences and Relationships)	-						A	-	-	-
3.1.10. Identify the Intelligence Process	-						A	-	-	-
3.1.11. Intelligence Sources/Disciplines (e.g., OSINT)	-						A	-	-	-
3.1.12. Intelligence Reports (e.g., IIR)	-						A	-	-	-
3.1.13. Tactics from Intel Sources	-						A	-	-	-
3.1.15. Identify the Joint Intelligence Preparation of the Environment (JIPOE) process	-						A	-	-	-
3.1.16. Identify PMESII	-						A	-	-	-

3.2. ISR Collection Management TR: JP 2-0, JP 2-01, JP 3-12	-						A	-	-	-
3.2.1. Intelligence Limitations/Problems	-						A	-	-	-
3.2.2. Collection Requirements	-						A	-	-	-
3.2.3. Commander's Critical Information Requirement (CCIR)	-						A	-	-	-
3.2.4. Priority Intelligence Requirement (PIR)	-						A	-	-	-
3.2.5. Essential Elements of Information (EEI)	-						A	-	-	-
3.2.6. Request for Information (RFI)	-						A	-	-	-
4. CYBERSPACE SYSTEMS AND PLATFORMS TR: AFTTP 3-10.3; AFDD 3-12; AFPD 10-17; AFI 31-401; JP 1-02; JP 3-12										
4.1. Introduction to SCADA/ICS										
4.1.1. Purpose	-						A	-	-	-
4.1.2. Components	-						A	-	-	-
4.1.3. Vulnerabilities	-						A	-	-	-
4.1.4. Security	-						A	-	-	-
4.2. Capabilities										
4.2.1. Workstations/Servers	-						B	-	-	-
4.2.2. Data Networks	-						B	-	-	-
4.2.3. Voice Networks	-						B	-	-	-
4.2.4. Space Networks	-						B	-	-	-
4.2.5. Battlefield Networks	-						B	-	-	-
4.2.6. AFIN	-						B	-	-	-
4.2.7. Websites/Databases	-						B	-	-	-
4.3. Vulnerabilities										
4.3.1. Workstations/Servers	-						B	-	-	-
4.3.2. Data Networks	-						B	-	-	-
4.3.3. Voice Networks	-						B	-	-	-
4.3.4. Space Networks	-						B	-	-	-

4.3.5. Battlefield Networks	-						B	-	-	-
4.3.6. AFIN	-						B	-	-	-
4.3.7. Websites/Databases	-						B	-	-	-
4.4. Components										
4.4.1. Workstations/Servers	-						B	-	-	-
4.4.2. Data Networks	-						B	-	-	-
4.4.3. Voice Networks	-						B	-	-	-
4.4.4. Space Networks	-						B	-	-	-
4.4.5. Battlefield Networks	-						B	-	-	-
4.4.6. AFIN	-						B	-	-	-
4.4.7. Websites/Databases	-						B	-	-	-
4.5. Design										
4.5.1. Workstations/Servers	-						B	-	-	-
4.5.2. Data Networks	-						B	-	-	-
4.5.3. Voice Networks	-						B	-	-	-
4.5.4. Space Networks	-						B	-	-	-
4.5.5. Battlefield Networks	-						B	-	-	-
4.5.6. AFIN	-						B	-	-	-
4.5.7. Websites/Databases	-						B	-	-	-
4.6. Security										
4.6.1. Workstations/Servers	-						B	-	-	-
4.6.2. Data Networks	-						B	-	-	-
4.6.3. Voice Networks	-						B	-	-	-
4.6.4. Space Networks	-						B	-	-	-
4.6.5. Battlefield Networks	-						B	-	-	-
4.6.6. AFIN	-						B	-	-	-
4.6.7. Websites/Databases	-						B	-	-	-
4.7. Machine Learning	-						B	-	-	-
4.8. AI	-						B	-	-	-
5. CYBER WARFARE OPERATIONS PLANNING TR: JP 1-0; JP 2-0; JP 5-0; JP 3-12; CJCSM 3122.07 Vol I/II										

5.1. Operational Mission Sets										
5.1.1. DODIN	-						A	-	-	-
5.1.2. DCO	-						A	-	-	-
5.1.3. OCO	-						A	-	-	-
5.1.4. Cryptologic	-						A	-	-	-
5.2. Joint Command and Planning Process										
5.2.1. Structure and Organization	-						A	-	-	-
5.2.2. Levels of War	-						A	-	-	-
5.2.3. Roles and Responsibilities	-						A	-	-	-
5.2.4. Command and Control (C2)	-						B	-	-	-
5.2.5. Authorities	-						B	-	-	-
5.2.6. Orders	-						A	-	-	-
5.3. Planning Process Defined (JPP)										
5.3.1. Operational vs. Tactical Planning	-						A	-	-	-
5.3.2. Deliberate Planning	-						A	-	-	-
5.3.3. Crisis Action Planning	-						A	-	-	-
5.4. Integrated Joint Special Technical Operations (IJSTO)										
5.4.1. Process	-						A	-	-	-
5.4.2. Roles and Responsibilities	-						A	-	-	-
5.5. Cyberspace Operational Planning										
5.5.1. Cyber C2	-						B	-	-	-
5.5.2. Synchronization	-						A	-	-	-
5.5.3. Weaponeering	-						A	-	-	-
5.5.4. Asset/Target Analysis										
5.5.4.1. Operational Platforms	-						B	-	-	-
5.5.4.2. Analyze blue space/operational considerations	-						C	-	-	-
5.5.4.3. Analyze red space/operational considerations	-						C	-	-	-
5.5.4.4. Analyze grey space/operational considerations	-						C	-	-	-

5.5.5. Intelligence Gain/Loss	-						A	-	-	-
5.5.6. Technical Gain/Loss	-						A	-	-	-
5.5.7. Deconfliction	-						A	-	-	-
5.5.8. Cyber Ops Assessments										
5.5.8.1. MOP/MOE	-						A	-	-	-
5.5.8.2. Conducting Ops Assessment	-						A	-	-	-
5.5.8.3. Battle Damage Indicators	-						A	-	-	-
5.5.8.4. Battle Damage Assessment	-						A	-	-	-
5.5.8.5 CONOPS/CONEMP/Mission Profiles	-						B	-	-	-
5.5.8.6. Attribution	-						B	-	-	-
5.6. Conduct DCO Mission Planning										
5.6.1. Plan A Mission	-						2b	-	-	-
5.6.2. Prepare/Present Mission Brief	-						2b	-	-	-
5.6.3. Prepare/Present Crew Brief	-						2b	-	-	-
5.6.4. Execute a Mission	-						2b	-	-	-
5.6.5. Debrief a Mission	-						2b	-	-	-
5.7. Conduct OCO Mission Planning										
5.7.1. Plan A Mission	-						2b	-	-	-
5.7.2. Prepare/Present Mission Brief	-						2b	-	-	-
5.7.3. Prepare/Present Crew Brief	-						2b	-	-	-
5.7.4. Execute a Mission	-						2b	-	-	-
5.7.5. Debrief a Mission	-						2b	-	-	-
6. NETWORKING FUNDAMENTALS TR: AFI 17-120; Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Prep Kit; IEEE 802										
6.1. Network Concepts										
6.1.1. Digital Numbering Systems (Internal Data Representation)										

6.1.1.1. Binary	-						B	-	-	-
6.1.1.2. Hexadecimal	-						B	-	-	-
6.1.1.3. Hexadecimal representations of network traffic	-						A	-	-	-
6.1.1.4. Physical Representation of Numbers	-						A	-	-	-
6.1.1.5. Convert Digital Numbers Across Formats	-						B	-	-	-
6.1.2. Standards and Frameworks										
6.1.2.1. OSI Model	-						A	-	-	-
6.1.2.2. 802.3 Local Area Networking	-						B	-	-	-
6.1.2.3. 802.3 and 802.1Q frame headers	-						B	-	-	-
6.1.2.4. 802.1Q virtual local area network (VLAN) frame and how it differs from a standard 802.3 frame	-						B	-	-	-
6.1.3. TCP/IP Suite										
6.1.3.1. Encapsulation/Decapsulation	-						B	-	-	-
6.1.3.2. Structure	-						B	-	-	-
6.1.3.3. Common ports and the services associated with them	-						A	-	-	-
6.1.3.4. Difference between regular and raw sockets	-						B	-	-	-
6.1.3.5. Contents of an Ethernet header and frame	-						B	-	-	-
6.1.3.6. Why and how frames are interpreted by different devices	-						B	-	-	-
6.1.4. Network Addressing										
6.1.4.1. Data-Link Layer										
6.1.4.1.1. Media Access Control (MAC) Addresses	-						B	-	-	-
6.1.4.2. Network Layer										
6.1.4.2.1. Perform IPv4 Subnetting	-						2b	-	-	-
6.1.4.2.2. Perform IPv4 and IPv6 packet headers analysis	-						2b	-	-	-
6.1.4.2.3. IPv6 Subnetting	-						A	-	-	-

6.1.4.2.4. IPv6 Neighbor Discovery	-						B			
6.1.4.2.5. Supernetting	-						A	-	-	-
6.1.5. Routing Protocols										
6.1.5.1. Interior	-						B	-	-	-
6.1.5.2. Exterior	-						B	-	-	-
6.1.5.3. Link-state	-						B	-	-	-
6.1.6. Protocols										
6.1.6.1. Transport protocols	-						A	-	-	-
6.1.6.2. Domain Name System (DNS)	-						B	-	-	-
6.1.6.3. Address Resolution Protocol (ARP)	-						B	-	-	-
6.1.6.4. Dynamic Host Configuration Protocol (DHCP)	-						B	-	-	-
6.1.6.5. Kerberos	-						2b	-	-	-
6.1.6.6. Various helper protocols							A	-	-	-
7.1. Advanced Networking Principles										
7.1.1. Network Types, Topologies, and Principles										
7.1.1.1. Enterprise topology	-						B	-	-	-
7.1.1.2. Packet Switched Networks	-						A	-	-	-
7.1.1.3. Circuit Switched Networks	-						A	-	-	-
7.1.1.4. Transmission Methods and Medium	-						A	-	-	-
7.1.1.5. Inter-Networking	-						A	-	-	-
7.1.1.6. Intra-Networking	-						A	-	-	-
7.1.1.7. Cloud Technology	-						B	-	-	-
7.1.1.8. Network sockets, socket tables and netstat	-						A	-	-	-
7.1.1.9. OS-specific modifications to network packets and election of ephemeral ports	-						A	-	-	-
7.1.1.10. Differences among traffic filtering methods and technologies	-						A	-	-	-

7.1.1.11. Navigate command line interface	-						2b	-	-	-
7.1.1.12. LAN technologies and their benefits and hindrances	-						A	-	-	-
7.1.1.13. How switches affect network traffic and the visibility of network traffic by other hosts	-						B	-	-	-
7.1.1.14. Access Control Lists (ACL)	-						B	-	-	-
7.2. ACTIVE DIRECTORY										
7.2.1. Features and benefits of domains	-						A	-	-	-
7.2.2. Replication in Active Directory	-						B	-	-	-
7.2.3. roles and functions of resources associated with Active Directory (e.g., user groups, computers, domain controllers)	-						B	-	-	-
7.2.4. Differences between local and domain accounts, and between domain and built-in accounts	-						B	-	-	-
7.2.5. Perform Active Directory queries/modifications and interpret query outputs (e.g., users, groups, computers, organizational units, memberships)	-						2b	-	-	-
7.2.6. Role of Group Policies, how they affect permission of users/resources, and how they get implemented in the directory tree	-						B	-	-	-
7.3. Manipulate Networking Devices										
7.3.1. Interface Address	-						2b	-	-	-
7.3.2. VLAN	-						2b	-	-	-
7.3.3. Routing Protocol	-						2b	-	-	-
7.3.4. Enumerate Configuration and Connected Devices	-						2b	-	-	-
7.3.5. Utilize MAC Table	-						2b	-	-	-
7.3.6. Copy Device Configuration	-						2b	-	-	-
7.3.7. Erase Device Configuration	-						2b	-	-	-

7.3.8. Implement Access Control List	-						2b	-	-	-
7.3.9. Implement Port Security	-						2b	-	-	-
7.3.10. Configure Port Mirroring	-						2b	-	-	-
7.3.11. Copy System Image	-						2b	-	-	-
7.3.12. Enable Secure Remote Configuration Access	-						2b	-	-	-
7.4. Network Analysis										
7.4.1. Fundamentals	-						B	-	-	-
7.4.2. Principles of active host discovery	-						A	-	-	-
7.4.3. Principles of passive host discovery	-						A	-	-	-
7.4.4. Perform TCP and UDP packets analysis	-						2b	-	-	-
7.4.5. Capture Traffic	-						2b	-	-	-
7.4.6. Analyze Traffic	-						2b	-	-	-
7.4.7. Identify the hardware manufacturer from network traffic	-						2b	-	-	-
7.4.8. Passive OS fingerprinting (p0f)	-						B	-	-	-
7.4.9. Conduct passive OS fingerprinting (p0f)	-						2b	-	-	-
7.4.10. Identify the OS version from network traffic	-						2b	-	-	-
7.4.11. Identify the patch release of OS software from network traffic	-						2b	-	-	-
7.4.12. Identify Services and Applications on a Network	-						2b	-	-	-
7.4.13. Analyze Protocol Data Units	-						2b	-	-	-
7.4.14. Ethernet Frame Structure	-						2b	-	-	-
7.4.15. Address Structure	-						2b	-	-	-
7.4.16. Packet Structure	-						2b	-	-	-
7.4.17. Classful	-						2b	-	-	-
7.4.18. Classless	-						2b	-	-	-
7.4.19. Private/Public	-						2b	-	-	-

7.4.20. Implement Session Recovery from Raw Traffic	-						2b	-	-	-
7.4.21. Identify Encoded Traffic	-						2b	-	-	-
7.4.22. Identify Malicious Traffic	-						2b	-	-	-
7.4.23. Perform internetworking routing analysis	-						2b	-	-	-
7.4.24. Interpret and generate IPTABLES filter rules	-						2b	-	-	-
7.4.25. Detect the existence of proxy server through traffic	-						2b	-	-	-
7.4.26. Analyze Protocols/Components	-						2c	-	-	-
7.4.27. Function of a Berkley Packet Filter (BPF)	-						A	-	-	-
7.4.28. Prepare a BPF	-						2b	-	-	-
7.4.29. Use a BPF to filter packets entering a network interface	-						2b	-	-	-
7.4.30. Use a BPF to extract key information from an ether frame	-						2b	-	-	-
8. OPERATING SYSTEMS TR: AF e-Learning, Linux: Basic System Administration Learning Track; UNIX Essentials Learning Track; FedVTE: Windows Operating System Security										
8.1. Windows OS										
8.1.1. Windows Basics										
8.1.1.1. Evolution of the Windows family of OSs	-						A	-	-	-
8.1.1.2. Differences in variants of Microsoft Windows	-						B	-	-	-
8.1.1.3. Windows Command Shell and PowerShell	-						A	-	-	-
8.1.1.4. Windows network naming schemes (e.g., TCP/IP naming vs. NetBIOS naming)	-						B	-	-	-
8.1.1.5. Computer's network configuration: Media Access Control (MAC) addressing, Internet Protocol addressing, Address resolution Protocol (ARP), Domain Name Resolution (DNS)	-						B	-	-	-

8.1.1.6. Windows Management Instrumentation Command-Line (WMIC)	-						B	-	-	-
8.1.1.7. Windows page files	-						A	-	-	-
8.1.1.8. x86 and x64 architectures	-						A	-	-	-
8.1.1.9. Tools used to connect to remote Windows File System	-						A	-	-	-
8.1.1.10. Host names and host name resolution	-						B	-	-	-
8.1.1.11. NetBIOS name resolution	-						B	-	-	-
8.1.1.12. Well-known NetBIOS suffixes (services)	-						B	-	-	-
8.1.1.13. Purpose and use of named pipes and mailslots	-						A	-	-	-
8.1.1.14. Routing	-						B	-	-	-
8.1.1.15. IP routing tables, including what information is included in each column	-						B	-	-	-
8.1.1.16. Purpose and use of Remote Procedure Call (RPC) and the endpoint mapper service	-						B	-	-	-
8.1.1.17. Function of a thread	-						B	-	-	-
8.1.1.18. Drivers	-						B	-	-	-
8.1.1.19. How the system determines which services and device drivers to initialize	-						A	-	-	-
8.1.1.20. Tools used to view and modify the computer's network configuration	-						B	-	-	-
8.1.1.21. Use of the Netstat tool and its output	-						A	-	-	-
8.1.1.22. IPv4 and IPv6 entries in the hosts file	-						B	-	-	-
8.1.1.23 Virtualization	-						B	-	-	-
8.1.1.24. Containerization	-						2b	-	-	-
8.1.2. Components										
8.1.2.1. Kernel										

8.1.2.1.1. Kernel and user address space	-						B	-	-	-
8.1.2.1.2. Key differences in kernel architectures	-						A	-	-	-
8.1.2.2. Registry										
8.1.2.2.1. Registry files	-						A	-	-	-
8.1.2.2.2. Structure and contents of the Windows Registry	-						B	-	-	-
8.1.2.2.3. Locations within the registry that store values of forensic relevance	-						A	-	-	-
8.1.2.2.4. Locations within the registry used for persistence	-						B	-	-	-
8.1.2.2.5. Service parameters (e.g., start values and dependencies) stored in the registry	-						B	-	-	-
8.1.2.2.6. Registry key containing network configuration information that is forensically relevant	-						B	-	-	-
8.1.2.2.7. When changes to the registry are expected to take effect	-						A	-	-	-
8.1.2.2.8. Utilize Registry	-						2b	-	-	-
8.1.2.2.9. Locate a machine SID in the registry	-						2b	-	-	-
8.1.2.2.10. Demonstrate the use of GUI tools and the command-line registry editor to query, view, analyze, create, and modify registry entries	-						2b	-	-	-
8.1.2.3. Boot Process										
8.1.2.3.1. Relationship between the boot process and the registry	-						B	-	-	-
8.1.2.3.2. Steps in the boot process from power-on to OS initialization	-						A	-	-	-
8.1.2.3.3. Hard disk layouts (e.g., Master Boot Record [MBR] disks, GUID Partition Table [GPT] disks)	-						A	-	-	-
8.1.2.3.4. Role of the MBR	-						A	-	-	-
8.1.2.3.5. Partition boot sector (PBS) is located and how its information is used by a system	-						A	-	-	-

8.1.2.3.6. System startup security features (e.g., BitLocker drive encryption and Trusted Platform Module [TPM])	-						A	-	-	-
8.1.2.3.7. Boot Configuration Database (BCD), including tools and components for modification	-						B	-	-	-
8.1.2.3.8. Examine and modify the boot configuration files	-						2b	-	-	-
8.1.3. File Structure										
8.1.3.1. FAT	-						A	-	-	-
8.1.3.2. NTFS	-						A	-	-	-
8.1.3.2.1. Terms associated with NTFS	-						A	-	-	-
8.1.3.2.2. NTFS attribute parameters	-						A	-	-	-
8.1.3.3. Important Windows file locations	-						A	-	-	-
8.1.3.4. SYSWOW64 file redirection	-						B	-	-	-
8.1.3.5. Master File Table (MFT) and its attributes	-						A	-	-	-
8.1.3.6. Well-known MFT entries	-						A	-	-	-
8.1.3.7. File and its attributes	-						B	-	-	-
8.1.3.8. File locations that can be used to autostart programs	-						B	-	-	-
8.1.3.9. Tools used to view the properties and characteristics of a file	-						A	-	-	-
8.1.3.10. Demonstrate the use of tools to view the properties and characteristics of a file	-						2b	-	-	-
8.1.3.11. Attrib command and the attributes it modifies	-						A	-	-	-
8.1.3.12. Folders that contain x86 and x64 binaries	-						A	-	-	-
8.1.3.13. File permissions and how they are affected by file operations	-						B	-	-	-
8.1.3.14. File times associated with a file and how they are affected by file operations	-						B	-	-	-

8.1.3.15. Differences between copy and move operations on file attributes	-						B	-	-	-
8.1.4. Users and Groups										
8.1.4.1. Local logon and domain logon	-						B	-	-	-
8.1.4.2. Information that is stored in an access token	-						A	-	-	-
8.1.4.3. User rights, including common rights and rights assigned to built-in groups	-						B	-	-	-
8.1.4.4. How groups work, including differences between groups on a local computer and those on a domain controller	-						B	-	-	-
8.1.4.5. Group Policy Object (GPO) queries and modifications	-						A	-	-	-
8.1.4.6. Permission inheritance	-						B	-	-	-
8.1.4.7. Security components of the interactive logon process	-						A	-	-	-
8.1.4.8. How user authentication occurs	-						A	-	-	-
8.1.4.9. Authentication process using Kerberos	-						A	-	-	-
8.1.4.10. Security identifiers (SIDs) and relative identifiers (RIDs)	-						A	-	-	-
8.1.4.11. How RIDs are created and where they are stored	-						B	-	-	-
8.1.4.12. Identify the user associated with an NTUSER.dat file	-						2a	-	-	-
8.1.4.13. Extract registry values from a NTUSER.dat file not currently loaded on HKCU	-						2a	-	-	-
8.1.4.14. Practice associating a user SID with a user profile	-						2b	-	-	-
8.1.4.15. Assess effective permissions given various user and group situations	-						2c	-	-	-
8.1.4. Utilize CLI	-						2c	-	-	-
8.1.4.1. Standard methods of transferring files	-						B	-	-	-

8.1.4.2. Perform a given set of tasks from the command line	-						2b	-	-	-
8.1.4.3. Demonstrate the use of command-line tools to query and modify the Directory Services database	-						2b	-	-	-
8.1.4.4. Demonstrate the use of CLI tools to view and manage the computer's network configuration	-						2b	-	-	-
8.1.4.5. Perform a system characterization using a Netstat listing	-						2b	-	-	-
8.1.4.6. Use host tools to perform network discovery	-						2b	-	-	-
8.1.5. Manipulate System										
8.1.5.1. User Accounts	-						2b	-	-	-
8.1.5.2. File Systems	-						2b	-	-	-
8.1.5.3. Network Shares	-						2b	-	-	-
8.1.5.4. Network Settings	-						2b	-	-	-
8.1.6. Processes & Services										
8.1.6.1. How network connections are affected by adjusting various services	-						A	-	-	-
8.1.6.2. Active processes, active resources, and system users	-						A	-	-	-
8.1.6.3. Process priorities	-						A	-	-	-
8.1.6.4. Function of service parameters (e.g., start values and dependencies) stored in the registry	-						B	-	-	-
8.1.6.5. System processes such as idle, Session Manager Subsystem Service (SMSS) and logon	-						B	-	-	-
8.1.6.6. How different tools are used to view, manage, and enumerate processes	-						B	-	-	-
8.1.6.7. Local Inter Process Communication (IPC) over TCP/UDP	-						B	-	-	-
8.1.6.8. Manipulate services using the Services Controller (SC) utility and services.msc	-						2b	-	-	-
8.1.6.9. Perform a system characterization using a process list	-						2b	-	-	-

8.1.6.10. Perform analysis of process listing output to determine the OS, users logged on, system uptime, user logged-in time and user account activity	-						2b	-	-	-
8.1.6.11. Analyze Processes and Services	-						2c	-	-	-
8.1.7. Window Security										
8.1.7.1. Abnormal or suspicious activity on a host	-						A	-	-	-
8.1.7.2. Auditing and its purpose	-						B	-	-	-
8.1.7.3. Types of auditing that are performed, to include how auditing occurs on the system	-						A	-	-	-
8.1.7.4. System's audit policy	-						A	-	-	-
8.1.7.5. Auditable events	-						A	-	-	-
8.1.7.6. System's event logs	-						A	-	-	-
8.1.7.7. Access control as it relates to object security	-						A	-	-	-
8.1.7.8. How access control is implemented	-						A	-	-	-
8.1.7.9. Steps involved in evaluating a system's integrity	-						B	-	-	-
8.1.7.10. Methods used to identify suspicious processes	-						B	-	-	-
8.1.7.11. Process used for collecting user/usage information, scheduled processes, directory listings, log files, etc.	-						A	-	-	-
8.1.7.12. State of the remote system	-						B	-	-	-
8.1.7.13. Tools that can be used for Windows forensic evaluations (e.g., psloggedon, logon sessions, net session, listdlls, handle, driverquery, psservice, autorunsc)	-						A	-	-	-
8.1.7.14. Common activities to harden an OS and the implications to the system if it is not hardened	-						A	-	-	-
8.1.7.15. Windows memory protections (e.g., Address Space Layout Randomization [ASLR] and Data Execution Prevention [DEP])	-						B	-	-	-

8.1.7.16. Purpose of Windows File Protection (WFP) and Windows Resource Protection (WRP)	-						A	-	-	-
8.1.7.17. Features and functionality of WFP and WRP	-						A	-	-	-
8.1.7.18. Registry keys and settings applicable to WFP	-						A	-	-	-
8.1.7.19. Determine Integrity of a Windows System										
8.1.7.19.1. Logs	-						2b	-	-	-
8.1.7.19.2. Use tools to view the system's event logs	-						2b	-	-	-
8.1.7.19.3. Demonstrate the use of tools to manage the system's audit policy	-						2b	-	-	-
8.1.7.19.4. Examine forensically relevant registry keys to identify abnormal or suspicious activity on a host	-						2b	-	-	-
8.1.7.19.5. Use tools to collect volatile data (e.g., socket states, processes)	-						2b	-	-	-
8.1.7.19.6. Determine if a live process is suspicious by reviewing loaded modules, associated files, and network connections	-						2b	-	-	-
8.1.7.19.7. Perform a tactical survey on a remote system to determine: OS characteristics; purpose and/or role of the remote system; running processes and resources in use; network configuration and activity; if a user is logged on and the user's activities; potential presence of suspicious software	-						2b	-	-	-
8.1.7.19.8. Examine network interfaces, network connections, routing tables, etc., to identify abnormal or suspicious activity on a host	-						2b	-	-	-
8.1.7.19.9. Examine NetBIOS information, currently running services and currently installed drivers to identify abnormal or suspicious activity on a host	-						2b	-	-	-
8.1.7.19.10. Firewall	-						2b	-	-	-

8.1.7.19.11. Examine the execution of a shell script	-						2b	-	-	-
8.1.7.19.12. Demonstrate Windows-specific situational awareness	-						2b	-	-	-
8.1.7.19.13. Determine the integrity level of a host by examining and integrating the output of several tools	-						2b	-	-	-
8.2. *NIX										
8.2.1. *NIX Basics										
8.2.1.1. Linux-based distros (Kali, Sec-Onion, SELinux, Ubuntu, etc.)	-						A	-	-	-
8.2.1.2. Differences among common listening ports on various UNIX systems	-						A	-	-	-
8.2.1.3. Local name resolution process on a UNIX host	-						B	-	-	-
8.2.1.4. UNIX remote procedure call () concepts	-						A	-	-	-
8.2.1.5. Shells and scripting	-						A	-	-	-
8.2.1.6. Common command shells, shell modes, and key features and functionalities	-						B	-	-	-
8.2.1.7. Virtualization	-						B	-	-	-
8.2.1.8. Containerization	-						2b	-	-	-
8.2.2. Components										
8.2.2.1. Kernel	-						B	-	-	-
8.2.2.2. Drivers	-						B	-	-	-
8.2.2.3. Socket tables	-						A	-	-	-
8.2.3. Boot Process										
8.2.3.1. Boot process differences between UNIX variants	-						B	-	-	-
8.2.3.2. Environment initialization and its implications	-						B	-	-	-
8.2.3.3. Explain the post-kernel boot process	-						2b	-	-	-
8.2.3.4. Determine a system's current and startup network configuration	-						2b	-	-	-

8.2.3.5. Investigate boot configuration files	-						2b	-	-	-
8.2.3.6. Resource Allocation	-						2b	-	-	-
8.2.4. Processes and Services										
8.2.4.1. Processes	-						A	-	-	-
8.2.4.2. Process Lifecycle	-						B	-	-	-
8.2.4.3. Local Inter Process Communication (IPC) over TCP/UDP	-						B	-	-	-
8.2.4.4. Mechanisms of process instantiation on UNIX systems	-						A	-	-	-
8.2.4.5. Typical processes from a process list in UNIX variants	-						A	-	-	-
8.2.5. File Structure										
8.2.5.1. File system metadata	-						B	-	-	-
8.2.5.2. Network file systems	-						A	-	-	-
8.2.5.3. Standard methods of transferring files	-						B	-	-	-
8.2.6. Utilize CLI										
8.2.6.1. Use the inetd/xinetd service	-						2b	-	-	-
8.2.6.2. Conduct file transfers with netcat	-						2b	-	-	-
8.2.6.3. Conduct uncommon methods of file transfers	-						2b	-	-	-
8.2.6.4. Packages	-						2b	-	-	-
8.2.6.5. Regular Expressions	-						2b	-	-	-
8.2.6.6. Use host tools to perform network discovery	-						2b	-	-	-
8.2.6.7. Determine which processes start at boot time	-						2b	-	-	-
8.2.7. Manipulate System										
8.2.7.1. User Accounts	-						2b	-	-	-
8.2.7.2. File Systems	-						2b	-	-	-
8.2.7.3. Network Shares	-						2b	-	-	-
8.2.7.4. Network Settings	-						2b	-	-	-
8.2.8. *NIX Security										

8.2.8.1. Why a survey is conducted and how information is gathered	-						B	-	-	-
8.2.8.2. Key pieces of information in a survey	-						B	-	-	-
8.2.8.3. Risk assessments of UNIX systems	-						A	-	-	-
8.2.8.4. System auditing and logging, including system logging, application logging and security logs	-						B	-	-	-
8.2.8.5. Types of actions that may contribute to entries within log files	-						B	-	-	-
8.2.8.6. Process Investigation	-						2b	-	-	-
8.2.8.7. Analyze Processes and Services	-						2c	-	-	-
8.2.8.8. Logs	-						2b	-	-	-
8.2.8.9. Network Security	-						2b	-	-	-
8.2.8.10. Demonstrate survey analysis and risk assessment	-						2b	-	-	-
8.2.8.11. Perform file system analysis	-						2b	-	-	-
8.2.8.12. Evaluate UNIX processes from a system integrity perspective	-						2c	-	-	-
8.2.8.13. Perform output of network-related utilities analysis	-						2b	-	-	-
8.2.8.14. Perform entries within socket tables analysis	-						2b	-	-	-
8.2.8.15. Access Control	-						2b	-	-	-
8.2.8.16. Use common tools and techniques to determine system integrity on a UNIX system	-						2c	-	-	-
8.2.8.17. Containerization	-						2b	-	-	-
8.3. Mobile Operating Systems										
8.3.1. Overview	-						B	-	-	-
8.3.2. Components	-						B	-	-	-
8.3.3. Virtualization	-						B	-	-	-
8.3.4. Containerization	-						2b	-	-	-
8.6. Internet of Things (IOT)										

8.6.1. IOT Devices	-						B	-	-	-
8.6.2. IOT Security	-						B	-	-	-
8.6.3. IOT Vulnerabilities	-						B	-	-	-
8.6.4. Busybox	-						B	-	-	-
9. SCRIPTING										
9.1. Batch										
9.1.1. Purpose of a batch script	-						A	-	-	-
9.1.2. Create a Batch Script	-						2b	-	-	-
9.1.3. Create a PowerShell Script	-						2b	-	-	-
9.1.4. Create a Bash Script	-						2b	-	-	-
9.1.5. Demonstrate basic familiarity with shell script programming and trace through the execution of a shell script	-						2b	-	-	-
9.1.6. Python Boolean Expressions	-						2b	-	-	-
9.2. Python										
9.2.1. Python Imports, keywords, reserved words	-						B	-	-	-
9.2.2. Python Data Types	-						B	-	-	-
9.2.3. Python Numbers	-						B	-	-	-
9.2.4. Python Variables	-						B	-	-	-
9.2.5. Python Objects	-						B	-	-	-
9.2.6. Python Set Types	-						B	-	-	-
9.2.7. Python Control Flow	-						B	-	-	-
9.2.8. Python Conditionals and Comparators	-						B	-	-	-
9.2.9. Python Operators	-						B	-	-	-
9.2.10. Python Loops, continue, break statements	-						B	-	-	-
9.2.11. Python Built in functions	-						B	-	-	-
9.2.12. Python Exception Handling	-						B	-	-	-
9.2.13. Python Lists/Tuple, and Dictionaries/Set, manipulation	-						B	-	-	-
9.2.14. Python Arrays	-						B	-	-	-
9.2.15. Python Data Structures	-						B	-	-	-

9.2.16. Python Classes and scope (global vs local), init, self, inheritance, object instantiation	-						B	-	-	-
9.2.17. Develop Python Regular Expressions	-						2b	-	-	-
9.2.18. Create Python Functions	-						2b	-	-	-
9.2.19. Use pseudocode to design an algorithm and implement it in Python	-						2b	-	-	-
9.2.20. Execute Python String manipulation	-						2b	-	-	-
9.2.21. Perform Python File IO and Manipulation	-						2b	-	-	-
9.2.22. Use Python Standard in and standard out	-						2b	-	-	-
9.2.23. Use Python Process Execution, pipe standard out and standard error streams	-						2b	-	-	-
9.2.24. Use Python Sockets	-						2b	-	-	-
9.2.25. Use socket programming in Python TCP applications	-						2b	-	-	-
9.2.26. Use socket programming in Python UDP applications	-						2b	-	-	-
9.2.27. Use socket programming in Python Generate raw network packets	-						2b	-	-	-
9.2.28. Use Scapy for Python Manipulate packets	-						2b	-	-	-
9.2.29. Python Recursive functions	-						A	-	-	-
9.2.30. Use Python to encode/decode base64 text	-						2b	-	-	-
9.2.31. Implement Python JSON objects	-						2b	-	-	-
9.2.32. Conduct Python Debugging	-						2b	-	-	-
10. DEFENSIVE CYBER OPERATIONS 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. Threat Types										
10.1.1. Internal	-						A	-	-	-
10.1.2. External	-						A	-	-	-
10.1.3. State Sponsored	-						A	-	-	-

10.1.4. Non-State Sponsored	-						A	-	-	-
10.1.5. Attributes of bots and botnets	-						B	-	-	-
10.2. DCO Theory and Methodology										
10.2.1. Defensive Theory	-						B	-	-	-
10.2.2. Defensive Methodology	-						B	-	-	-
10.3. Identify Defensive Methods										
10.3.1. Encryption	-						B	-	-	-
10.3.2. Secure Configurations	-						B	-	-	-
10.3.3. Common security products	-						B	-	-	-
10.3.4. Secure Enclaves	-						B	-	-	-
10.3.5. Vulnerability Scanning	-						B	-	-	-
10.3.6. Boundary Protection	-						B	-	-	-
10.3.7. Big Data analytics	-						B	-	-	-
10.3.8. sensor placement	-						B	-	-	-
10.4. Defensive Tools										
10.4.1. Endpoint Detection and Response (EDR)	-						B	-	-	-
10.4.2. Honeypots	-						A	-	-	-
10.4.3. Reverse Engineering	-						B	-	-	-
10.4.4. Trusted tools	-						B	-	-	-
10.4.5. Intrusion Detection/Pretention (Host/Network)	-						B	-	-	-
10.4.6. Differences between signature-based and heuristic-based detection	-						A	-	-	-
10.4.7. Identify the steps of risk analysis from the perspective of defenders	-						A	-	-	-
10.4.8. Network monitoring	-						B	-	-	-
10.4.9. Application logging	-						B	-	-	-
10.4.10. Registry keys to query	-						B	-	-	-
10.4.11. How rootkits work in user and kernel mode	-						B	-	-	-

10.5. 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										
10.5.1. Methodology	-						B	-	-	-
10.5.2. Incident Categories	-						B	-	-	-
10.5.3. Remote Evidence Collection	-						A	-	-	-
10.5.4. Reporting	-						A	-	-	-
10.5.5. Forensics	-						B	-	-	-
10.5.6. Incident Recovery	-						A	-	-	-
10.6. 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										
10.6.1. Fundamentals	-						A	-	-	-
10.6.2. Secure Programming	-						A	-	-	-
10.6.3. Agile Development Process	-						A	-	-	-
10.6.4. Reverse Engineering	-						A	-	-	-
10.6.5. Weaponization	-						A	-	-	-
10.6.6. Provisioning	-						A	-	-	-
10.6.7. Operational Frameworks	-						A	-	-	-
10.6.8. Functional Evaluation Fundamentals	-						A	-	-	-
10.6.9. Fuzzing Fundamentals	-						A	-	-	-
10.6.10. Real-Time Operations and Innovation	-						A	-	-	-
10.7. Conduct DCO										
10.7.1. Actively Defend										
10.7.1.1. Workstations/Servers	-						2b	-	-	-
10.7.1.2. IP Networks	-						2b	-	-	-
10.7.1.3. Wireless Networks	-						2b	-	-	-
10.7.1.4. Websites/Databases	-						2b	-	-	-
10.7.2. Conduct Defensive Actions										
10.7.2.1. Forensics	-						2b	-	-	-
10.7.2.2. Intrusion Detection	-						2b	-	-	-

10.7.2.3. Conduct risk analysis to determine whether to continue an operation or move to an incident response operation	-						2c	-	-	-
10.7.2.4. Identify UNIX logs	-						2b	-	-	-
10.7.2.5. Summarize Windows logs and event identifiers (ID)	-						2b	-	-	-
10.7.2.6. Identify threats on a target	-						2b	-	-	-
10.7.2.7. Demonstrate a working knowledge of various computer security threats	-						2b	-	-	-
10.7.2.8. Analyze traffic to locate covert channels	-						2b	-	-	-
10.7.2.9. Determine persistence vectors of malware on target machines	-						2b	-	-	-
10.7.2.10. Assess malware on a UNIX system	-						2b	-	-	-
10.7.2.11. Differentiate between what is normal and what is suspicious on the system	-						2b	-	-	-
10.7.2.12. Assess malware on a Windows system	-						2b	-	-	-
10.7.2.13. Examine processes running on the system	-						2b	-	-	-
10.7.2.14. Evaluate running DLLs	-						2b	-	-	-
10.7.2.15. Perform data analysis	-						2b	-	-	-
10.7.2.16. Malware Analysis	-						2b	-	-	-
10.7.2.17. Document findings of anomalous connections	-						2c	-	-	-
10.7.2.18. Analyze current state against baselines	-						2c	-	-	-
10.7.2.19. Analyze logs	-						2b	-	-	-
10.7.2.20. Security Information and Event Management (SIEM)	-						2b	-	-	-
10.7.2.21. Security Orchestration, Automation, and Response (SOAR)	-						2b	-	-	-
10.7.2.22. Demonstrate remote host forensics to obtain situational awareness and determine malicious activity	-						2b	-	-	-

11. OFFENSIVE CYBER OPERATIONS TR: AFTTP 3-10.3; AFDD 3-12; AFPD 17-2; AFI 16-1404; DoD Dictionary of Military and Associated Terms; JP 3-12										
11.1. OCO Theory and Methodology										
11.1.1. Tradecraft	-						C	-	-	-
11.1.2. Access methods used by hackers	-						B	-	-	-
11.1.3. Buffer Overflow Tactics and Techniques	-						B	-	-	-
11.1.4. Privilege Escalation	-						B	-	-	-
11.1.5. Rootkits	-						B	-	-	-
11.1.6. Redirection and Triggering	-						B	-	-	-
11.1.7. Collection/Exfiltration	-						B	-	-	-
11.1.8. Social Engineering	-						B	-	-	-
11.1.9. Web Exploitation	-						B	-	-	-
11.1.10. Persistent Access	-						B	-	-	-
11.1.11. Man-in-the-Middle	-						B	-	-	-
11.1.12. (Distributed) Denial of Service	-						B	-	-	-
11.1.13. Obfuscation	-						B	-	-	-
11.1.14. Principles and methods of tunneling network traffic	-						A	-	-	-
11.1.15. Different uses of SSH	-						B	-	-	-
11.1.16. Differences between forward and reverse tunnels when using SSH	-						B	-	-	-
11.1.17. How to redirect traffic using SSH forward and reverse tunnels	-						B	-	-	-
11.1.18. SSH reverse tunnels and their purpose	-						B	-	-	-
11.1.19. Difference between tunneling and redirecting network traffic	-						A	-	-	-
11.1.20. Identify the steps of risk analysis from the perspective of attackers	-						A	-	-	-

11.1.21. Fundamental risk assessment and situational awareness as they pertain to computer security threats	-						B	-	-	-
11.1.22. Different types of shellcode	-						B	-		
11.2. Wireless Networks										
11.2.1. Topology	-						B	-	-	-
11.2.2. Components	-						B	-	-	-
11.2.3. Security	-						B	-	-	-
11.3. Conduct OCO										
11.3.1. Exploit Using Offensive Tools										
11.3.1.1. Web	-						2b	-	-	-
11.3.1.2. Hosts	-						2b	-	-	-
11.3.1.3. Active Directory	-						2b	-	-	-
11.3.1.4. Perform manipulation or denial effect in SCADA/ICS systems	-						2b	-	-	-
11.3.1.5. Reconnaissance	-						2b	-	-	-
11.3.1.5.1. Use various online tools for open-source data collection (ex. Online trade, DNS, mail, etc.)	-						2c	-	-	-
11.3.1.6. Vulnerability Assessment	-						2b	-	-	-
11.3.1.7. Password Cracking	-						2b	-	-	-
11.3.2. Metasploit										
11.3.2.1. Use Metasploit to gain access to a target	-						2b	-	-	-
11.3.2.2. Use of Meterpreter built-in commands	-						B	-	-	-
11.3.2.3. Meterpreter scripts	-						B	-	-	-
11.3.2.4. Metasploit and situational awareness	-						B	-	-	-
11.3.2.5. Employ pivoting with Metasploit	-						2b	-	-	-
11.3.2.6. Execute Tunneling	-						3c	-	-	-

11.3.2.7. Use SSH to redirect and tunnel network traffic through multiple hosts	-						3c	-	-	-
11.3.2.8. Perform network tunneling diagrams analysis	-						2b	-	-	-
11.3.2.9. Implement reverse SSH tunnels	-						2b	-	-	-
11.3.3. Manipulate Wireless Access Point										
11.3.3.1. Establish Connectivity	-						2b	-	-	-
11.3.3.2. Bypass Security	-						2b	-	-	-
11.3.3.3. Perform code injection	-						2b	-	-	-
11.3.3.4. Perform situational awareness on a UNIX system	-						2b	-	-	-
11.3.3.5. Perform log cleanup	-						2b	-	-	-
11.3.3.6. Locate security products	-						2b	-	-	-
11.3.3.7. Establish Persistent Access	-						2b	-	-	-
11.3.4. Generate Denial or Manipulation Effect										
11.3.4.1. Workstations/Servers	-						2b	-	-	-
11.3.4.2. Data Networks	-						2b	-	-	-
11.3.4.3. Wireless Networks	-						2b	-	-	-
11.3.4.4. Websites/Databases	-						2b	-	-	-
11.3.4.5. Industrial Systems	-						2b	-	-	-
11.3.5. Malware Triage										
11.3.5.1. Reverse Engineering	-						B	-	-	-
12. Air Force Basic Cyber Operations										
12.1. Operations										
12.1.1. Operations and Analysis:										
12.1.1.1. Publicly available tools/techniques	-						B	-	-	-
12.1.1.2. Security rules, regulations, precautions, and prevention techniques	-						B	-	-	-
12.1.1.3. Types of firewalls	-						B	-	-	-

12.1.1.4. Types of routers, switches, and failover recognition	-						B	-	-	-
12.1.1.5. Limitations of operational tools, concerning counter-detection	-						B	-	-	-
12.1.1.6. Location and use of tool documentation	-						C	-	-	-
12.1.1.7. Methods and procedures for communicating with tools/modules	-						B	-	-	-
12.1.1.8. Initial access to cleaning off target	-						B	-	-	-
12.1.1.9. Prepare for an operation	-						B	-	-	-
12.1.1.10. Vulnerabilities leveraged by exploitation tools	-						B	-	-	-
12.1.1.11. Threats to OPSEC when installing, using, modifying, and uninstalling tools	-						B	-	-	-
12.1.1.12. Tools/modules: purpose, use, differences, capabilities, limitations, interactions, bugs, and reasons for failure	-						B	-	-	-
12.1.1.13. Virtual infrastructure architecture, management, and maintenance	-						B	-	-	-
12.1.1.14. Tool/module location on a target and how they function	-						B	-	-	-
12.1.1.15. Detect malware or cohabitation with another actor on a target system	-						3c	-	-	-
12.1.1.16. Respond to new information, changing conditions, or unexpected obstacles	-						3c	-	-	-
12.1.1.17. Characterize target admin/user's technical abilities, habits, and skills	-						3c	-	-	-
12.1.1.18. Research and develop new tools/techniques	-						2b	-	-	-
12.1.1.19. Create virtual network for training and testing tools, techniques, and procedures	-						3c	-	-	-
12.1.1.20. Conduct determinations to continue with an operation or course of action (CoA)	-						3c	-	-	-

12.1.1.21. Enumerate user attributes	-						3c	-	-	-
12.1.1.22. Exploit vulnerabilities to gain additional access	-						3b	-	-	-
12.1.1.23. Extract credentials from hosts	-						3c	-	-	-
12.1.1.24. Formulate effective strategies	-						3b	-	-	-
12.1.1.25. Gather, attribute, and analyze forensic information	-						3b	-	-	-
12.1.1.26. Identify and analyze security products	-						3c	-	-	-
12.1.1.27. Identify and enumerate access vectors	-						3b	-	-	-
12.1.1.28. Identify endpoint and midpoint device for network expansion	-						3c	-	-	-
12.1.1.29. Identify files containing information critical	-						2b	-	-	-
12.1.1.30. Identify logging capabilities on host	-						3c	-	-	-
12.1.1.31. Identify operationally critical target groups, personnel, and systems	-						2b	-	-	-
12.1.1.32. Identify strengths and weaknesses in a network	-						3b	-	-	-
12.1.1.33. Identify vulnerabilities in a target host	-						3b	-	-	-
12.1.1.34. Identify applicable tools or tactics, techniques, and procedures (TTPs)	-						3c	-	-	-
12.1.1.35. Conduct Operator feedback	-						2b	-	-	-
12.1.1.36. Interpret device configurations	-						3c	-	-	-
12.1.1.37. Demonstrate situational awareness of target environment	-						3c	-	-	-
12.1.1.38. Perform Masquerade procedures	-						3c	-	-	-
12.1.1.39. Interpret technical materials	-						2b	-	-	-
12.1.1.40. Accomplish Developer tool documentation	-						2b	-	-	-

12.1.1.41. Recognize and report mistakes or poor tradecraft	-						3c	-	-	-
12.1.1.42. Respond to operational incidents	-						2b	-	-	-
12.1.1.43. Perform Corrective actions	-						2b	-	-	-
12.1.1.44. Identify Tool errors and OPSEC concerns	-						2b	-	-	-
12.1.1.45. Identify Operator limitations and response actions	-						3c	-	-	-
12.1.1.46. Redirect and tunnel through target systems	-						3c	-	-	-
12.1.1.47. Research non-standards within a project	-						3c	-	-	-
12.1.1.48. Perform common commands on targets	-						3c	-	-	-
12.1.1.49. Perform Troubleshooting	-						2b	-	-	-
12.1.1.50. Use core toolsets (e.g., implants, remote access tools)	-						2b	-	-	-
12.1.1.51. Use encryption	-						2b	-	-	-
12.1.1.52. Use network enumeration tools	-						2b	-	-	-
12.1.1.53. Use remote access tools	-						2b	-	-	-
12.1.1.54. Use enterprise enumeration tools	-						2b	-	-	-
12.1.1.55. Determine native host capabilities	-						3c	-	-	-
12.1.1.56. Verify file integrity for uploads and downloads	-						3c	-	-	-
12.1.1.57. Access control models	-						B	-	-	-
12.1.1.58. Mandatory Access Controls and Discretionary Access Controls	-						C	-	-	-
12.1.1.59. Use security encryptions	-						2b	-	-	-
12.1.1.60. Methods of persistence	-						B	-	-	-
12.1.1.61. Determine common computer architecture characteristic (e.g., x86, x64)	-						3c	-	-	-

12.1.1.62. Use dynamic analysis tools	-						2b	-	-	-
12.1.1.63. Identify Risk and likely outcomes of TTPs	-						3c	-	-	-
12.1.1.64. Conduct Mission pre-brief	-						2b	-	-	-
12.1.1.65. Construct a course of action using available exploitation tools and techniques	-						2b	-	-	-
12.1.1.66. Determine the purpose of a target device	-						2b	-	-	-
12.1.1.67. Transfer collected data	-						3c	-	-	-
12.1.1.68. Protecting capabilities	-						3c	-	-	-
12.1.1.69. Identify artifacts and remediate	-						2b	-	-	-
12.1.1.70. Identify running services on potential targets to determine vulnerabilities	-						3c	-	-	-
12.1.1.71. Evaluate mission complexity	-						2b	-	-	-
12.1.1.72. Evaluate mission variability	-						2b	-	-	-
12.1.1.73. Interpret scan results	-						3c	-	-	-
12.1.1.74. Model a simulated environment to conduct mission rehearsal	-						3c	-	-	-
12.1.1.75. Pair exploits to vulnerable devices	-						2b	-	-	-
12.1.1.76. Conduct Low level troubleshooting	-						2b	-	-	-
12.1.1.77. Conduct historical operational and open-source data analysis	-						2b	-	-	-
12.1.1.78. File systems analysis	-						3c	-	-	-
12.1.1.79. Assess indicators of compromise	-						3c	-	-	-
12.1.1.80. Characterize malware	-						2b	-	-	-
12.1.1.81. Draft technical documentation and guidance	-						2b	-	-	-
12.1.1.82. Evaluate configurations of auditing firewalls, perimeters, routers, and IDSs	-						2b	-	-	-

12.1.1.83. Interpret enumeration results	-						2b	-	-	-
12.1.1.84. Perform network collection tactics, techniques, and procedures (TTP)	-						3c	-	-	-
12.1.1.85. Review technical documentation and guidance	-						2b	-	-	-
12.1.1.86. Operational documentation	-						C	-	-	-
12.1.1.87. Audit and log procedures, including server-based logging	-						B	-	-	-
12.1.1.88. Basic client software applications and their attack surfaces	-						B	-	-	-
12.1.1.89. Basic server software applications and their attack surfaces	-						B	-	-	-
12.1.1.90. Common network administration best practices and impact to operations	-						B	-	-	-
12.1.1.91. Commonly used file extensions and data types for operations	-						B	-	-	-
12.1.1.92. Computer operating system fundamentals	-						B	-	-	-
12.1.1.93. Credential sources and restrictions related to credential usage	-						B	-	-	-
12.1.1.94. Current software and methodologies for proactive cyber defense and system hardening	-						B	-	-	-
12.1.1.95. Device reboots impact on tool functionality	-						B	-	-	-
12.1.1.96. Types of operations	-						B	-	-	-
12.1.1.97. Factors that would suspend or abort an operation	-						C	-	-	-
12.1.1.98. File systems and disk management	-						B	-	-	-
12.1.1.99. Historical target and projects data	-						B	-	-	-
12.1.1.100. Host-based security products and how they affect exploitation and vulnerability	-						B	-	-	-

12.1.1.101. Computer program execution	-						C	-	-	-
12.1.1.102. Host-based security products, logging, and malware effects on tool functionality	-						B	-	-	-
12.1.1.103. Other actor effects on operations	-						B	-	-	-
12.1.1.104. Unix and Windows information system services that provide authentication and logging, DNS, mail, web service, file transfer protocol (FTP) server, DHCP, firewall, and Simple Network Management Protocol (SNMP)	-						B	-	-	-
12.1.1.105. Internal and external organizational information needs, mission, structure, capabilities, relationships, and history	-						B	-	-	-
12.1.1.106. Legal authorities/restrictions, federal laws/regulations, policies, procedures, and guidelines	-						B	-	-	-
12.1.1.107. Malware triage	-						B	-	-	-
12.1.1.108. Methods and procedures for sending a payload via an implant	-						B	-	-	-
12.1.1.109. Methods and techniques used to detect exploitation activities	-						B	-	-	-
12.1.1.110. Methods, strategies, and techniques of evading detection while conducting operations	-						B	-	-	-
12.1.1.111. Methods, tools, and procedures for collecting information	-						B	-	-	-
12.1.1.112. Methods, tools, and procedures for exploiting target systems	-						B	-	-	-
12.1.1.113. Methods, tools, and techniques used to determine the path to a target host/network	-						B	-	-	-
12.1.1.114. Network construction	-						C	-	-	-
12.1.1.115. Network topology	-						B	-	-	-

12.1.1.116. Operating system command shells, configuration data	-						B	-	-	-
12.1.1.117. Operational infrastructure	-						B	-	-	-
12.1.1.118. Operational security, logging, admin concepts, and troubleshooting	-						B	-	-	-
12.1.1.119. Organization Standard Operating Procedures	-						B	-	-	-
12.1.1.120. Redirection techniques	-						B	-	-	-
12.1.1.121. Software security products and effects on exploitation and vulnerabilities	-						B	-	-	-
12.1.1.122. Structure, approach, and strategy of exploitation tools and techniques	-						C	-	-	-
12.1.1.123. System administration concepts for stand-alone operating systems	-						B	-	-	-
12.1.1.124. TCP/IP networking protocols	-						C	-	-	-
12.1.1.125. Unix/Linux and Windows operating systems structures and internals	-						B	-	-	-
12.1.1.126. Conduct active enumeration	-						3b	-	-	-
12.1.1.127. Enumerate file systems	-						3c	-	-	-
12.1.1.128. Identify installed patches and patch signatures	-						2b	-	-	-
12.1.1.129. Knowledge management	-						2b	-	-	-
12.1.1.130. Triage key elements of Malware analysis for reverse engineering to identify function and ownership of remote tools	-						1b	-	-	-
12.1.1.131. Identify Remote command line and GUI tool usage	-						3c	-	-	-
12.1.1.132. Retrieve configurations of auditing firewalls, perimeters, routers, and IDSs	-						3c	-	-	-
12.1.1.133. Retrieve memory resident data	-						3c	-	-	-

12.1.1.134. Test and evaluate capabilities for implementation	-						2b	-	-	-
12.1.1.135. Use of tools, techniques, and procedures to gain access to a target	-						3c	-	-	-
12.1.1.136. Operate automated systems to interact with target environment	-						3c	-	-	-
12.1.2. Ops Planning										
12.1.2.1. Processes for assessing and mitigating risk	-						B	-	-	-
12.1.2.2. Monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity	-						2b	-	-	-
12.1.2.3. Evasion strategies and TTPs	-						B	-	-	-
12.1.2.4. Internal and external partner reporting	-						B	-	-	-
12.1.2.5. Network administration	-						B	-	-	-
12.1.2.6. Security implications of software configurations	-						B	-	-	-
12.1.2.7. Fundamentals of digital forensics to extract actionable intelligence	-						B	-	-	-
12.1.2.8. Interpret vulnerability scanner results	-						2b	-	-	-
12.1.2.9. Conduct Technical writing	-						2b	-	-	-
12.1.2.10. Verify the integrity of all files	-						3c	-	-	-
12.1.3. Operations Reporting:										
12.1.3.1. Plan, brief, execute, and debrief a mission	-						2b	-	-	-
13. UPGRADE TRAINING TASKS										
13.1. Air Force Supervisor TR: https://www.airuniversity.af.edu/Portals/10/Foundational-Resources/AFJQS-Supervisor-230801.pdf or most current version										
13.1.1. Complete AFJQS-Supervisor	5						-	B	-	-
13.2. Doctrine										

13.2.1. Air Force Core Missions TR: https://doctrine.af.mil/; AFD Volume 1 - Basic Doctrine or potentially 'Global Vigilance, Global Reach, Global Power for America" http://www.af.mil/Portals/1/images/airpowe r/GV_GR_GP_300DPI.pdf, AFMAN 36- 2647-	5						-	B	-	-
13.2.2. Tenets of Air and Space Power TR: https://doctrine.af.mil/; AFD Volume 1 - Basic Doctrine, Global Vigilance, Global Reach, Global Power for America: http://www.af.mil/Portals/1/images/airpower/GV_GR_GP_300DPI.pdf	5						-	B	-	-
13.2.3. Joint Doctrine TR: CJCSI 3010.02E, JP 2-0, JP 2-01, JP 2-03, JP 3-0, JP 3-12, JP 3-13, JP 3-14, https://www.jcs.mil/Doctrine/Joint-DoctinePubs/	5						-	B	-	-
13.2.4. Cyber Synchronization with National Strategy TR: National Security Strategy, and National Defense Strategy	5						-	B	-	-
13.3 Cyber Warfare Operations Management										
13.3.1. Resource Management TR: AFI 65-601v1, AFI 65-601v2, AFI 65-103, AFI 64-117	7						-	-	B	-
13.3.2. Readiness TR: AFI 10-201, AFI 10-403, AFI 10-401, AFI 10-244, AF 36-2651, AEF Online https://aefonline.afpc.randolph.af.mil/default.aspx	7						-	-	B	-
13.3.3. Manpower TR: AFI 38-101, AFPD 38-2	7						-	-	B	-
13.3.4. Assignments TR: AFI 36-2110, Stabilized Tour Guide (STG), Special Duty Catalog (SPECAT)	7						-	-	B	-
13.3.5. Force Management TR: AFI 36-2670, AFI 36-2406, AFI 36-2606, AFI 36-2502, Air Force Enlisted Classification Directory	7						-	-	B	-
13.3.6. Total Force Airmen TR: AFI 36-2132, AFI 38-201, 36-2629, AFI 10-402	7						-	-	B	-
13.3.7. Program Assessments TR: AFI 90-201, 17 Series AFIs, HAF/MAJCOM directives	7						-	-	B	-
13.4 Air Force NCOIC / Section Chief TR: https://www.airuniversity.af.edu/Portals/10/Foundational-Resources/AFJQS-NCOIC-Section-Chief-230731.pdf or most current version										
13.4.1 Complete AFJQS-NCOIC / Section Chief	7						-	-	B	-
13.5 Air Force Flight Chief TR: https://www.airuniversity.af.edu/Portals/10/Foundational-Resources/AFJQS-Flight-Chief-230731.pdf or most current version										
13.5.1 Complete AFJQS-Flight Chief	7						-	-	B	-

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.

Course Number	Course Title	Location
WCYBER200	Cyberspace 200	Wright Patterson AFB, OH
WCYBER300	Cyberspace 300	Wright Patterson AFB, OH

8. Operations Training Requirements.

8.1 Operations Training Requirements are identified by the ACC (ACC A3/2/6K) Functional Area Managers for Offensive and Defensive Cyber Operations, IAW ACCI 11-252, para. 1.2.2.

8.2 Joint course requirement and training pipeline information for USCYBERCOM Cyber Mission Force (CMF) Work Roles are located at https://intelshare.intelink.gov/sites/uscybercom/Training/Lists/Joint%20Training%20Lead%20Announcements/Attachments/17/USCC%20CMF%20Training%20Pipeline%204.2.pdf

9. Air University A4/A6 Courses.

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

10. 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

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