Cyber (CMF 17) Career Progression Plan

Chapter 1. Duties

The cyber career management field (CMF) is designed to provide cyberspace and electronic warfare (EW) operations expertise in support of the full range of military operations by enabling actions and generating outcome based cyber effects across all domains. The cyber CMF integrates Cyberspace Electromagnetic Activities (CEMA) into operational assessments and planning processes and develops, trains, and maintains, CEMA standard operating procedures (SOP); tactics, techniques and procedures (TTPs), and battle drills. The cyber CMF is tasked to ensure freedom of maneuver within the cyberspace domain and the electromagnetic spectrum while denying the same to adversaries. This task is accomplished by creating outcome based cyber effects in support of the commander's requirements and are intended to project power in and through cyberspace by targeting enemy and hostile adversary activities and capabilities.

Chapter 2. Transformation

The cyber CMF is a professional enlisted workforce trained and equipped to maintain dominance in both offensive and defensive cyberspace operations, and ensure control of the electromagnetic spectrum as enduring maneuver capabilities. This profession requires not only cyberspace and electromagnetic competence and proficiency, but also a solid foundation of the operational characteristics of the Army with particular emphasis on the Army's maneuver force and special operations force elements. To operate as part of the cyber mission force, cyber Soldiers must thoroughly understand unique technical training and oversight requirements. Factors contributing to the development of cyber operations and electronic warfare specialists include Joint and Army doctrine, Army-wide cyber mission forces manning needs and echelon requirements, institutional training, and joint certification courses and curricula. This also includes current and future cyberspace and electromagnetic systems development, assessment, employment, and fielding.

Chapter 3. Recommended career management self-development by rank

Army wide self-development: All Soldiers bear individual responsibility for the success of their career by ensuring timely completion of Army requirements through individual effort and active participation in institutional training, assignments, self-development, and civilian educational activities. *The measures required to achieve this success are outlined in the parent document to this smartbook, DA PAM 600-25 Chapter 2 sections 13-16.*

Cyber CMF specific self-development:

a. Private-Specialist/Corporal.

(1) The quality and success of a Soldier's career is in direct proportion to the Soldier's consistent commitment to excellence regardless of the mission. Soldiers committed to achieving high goals will develop leadership skills and have the practical knowledge and ambition to put them to good use. Awards and decorations serve to recognize Soldiers for their accomplishments and tend to both motivate fellow Soldiers and build the team.

(2) Soldiers should study the history of the Cyber Corps and master the following military publications: (1) FM 3-12, (2) Joint Publication (JP) 3–12, (3) ADP 3-0, (4) ADPR 3-0, (5) ADP 5-0, (6) ADPR 5-0, (7) ATP 2-91.9 (U), (8) ATP 3-12.3; all -10 level maintenance manuals associated with their equipment; Standard Operating Procedures (SOPs); tactics, techniques, and procedures (TTPs); and battle drills.Strive to achieve honors (i.e. Commandant's List, Distinguished Graduate, or Honor Graduate) at PME schools. Complete Structured Self-Development Course/Distributed Leaders Course 1 (SSD/DLC 1) and Basic Leaders Course for Specialists/Corporals.

(3) Participate in competitive boards such as the Soldier of the Month, Quarter, or Year and Army Best Warrior Competitions to instill discipline, and improve verbal communication skills.

(4) Volunteer to participate in skill enhancing events like Cyber Challenges and Industry Competitions to broaden technical knowledge base.

(5) Soldiers may earn promotion points for technical certifications and Skillport training courses; a full list of certifications can be found on the Army Credentialing Opportunities On-line (COOL) Website. Soldiers can locate a listing of certifications associated with their MOS and skill level by viewing their MOS Career Map posted on Army Career Tracker (ACT) Website. Training modules for certification preparation can be accessed through Skillport via AKO.

(6) Advanced education is a critical aspect of the self-development program and Soldiers should consider efforts to begin developing an academic program around a degree that relates to their MOS using information provided on the eArmyU website or with the assistance of an educational advisor. Soldiers willing to make the required sacrifices should seize opportunities to begin an Associates Degree program preferably in a Science, Technology, Engineering and Mathematics (STEM) or Cyber Security program or accumulate two years of college credit towards an accredited college degree in any area of interest. These self-development options are based on the Soldier's own desire to excel. Ample opportunities exist for Soldiers to participate in various correspondence courses to accomplish individual educational goals. CLEP and the DANTES tests are other resources for converting previously acquired knowledge or training into college credit. Soldiers are encouraged to access Skillport training through AKO for technical training and industry certification preparation.

b. *Sergeant*.

(1) Sergeants committed to achieving high goals will develop leadership skills and have the practical knowledge and ambition to put them to good use. Sergeants should begin working in the role of "mentor" and teacher. The goal of the teacher is to ensure less experienced Soldiers sustain and build their technical and tactical skill sets, by developing and providing small team training. The goal of the mentor is to assist less experienced Soldiers in reaching their personal and professional potential.

(2) Sergeants should focus on mastering the military publications listed at the preceding skill levels and expand proficiency across the spectrum of Army doctrinal, operational, and technical publications and become familiar with where to find these publications. One such publication that can be helpful towards self-development for CMF17 is Smartbook DA PAM 611-21 Chapters 9 thru 14 found on MilSuite at https://www.milsuite.mil/book/groups/smartbookdapam611-21.

(3) Strive to achieve honors (i.e. Commandant's List, Distinguished Graduate, or Honor Graduate) at PME schools. Complete SSD/DLC 2.

(4) Participate in competitive boards such as the NCO of the Month, Quarter, or Year, Sergeant Audie Murphy, Sergeant Morales, and Army Best Warrior Competitions. These boards broaden the knowledge base, instill discipline and improve the Soldier's ability to communicate verbally to enhance confidence and build more adaptive Leaders.

(5) Volunteer to participate in skill enhancing events like Cyber Challenges and Industry Competitions to broaden technical knowledge base and mentor participating subordinate Soldiers.

(6) Sergeants may earn promotion points for technical certifications and Skillport training courses; a full list of certifications can be found on the COOL Website. Soldiers can locate a listing of certifications associated with the MOS and skill level by viewing the MOS Career Maps posted on Army Career Tracker (ACT) Website. Training modules for certification preparation can be accessed through Skillport via AKO.

(7) Sergeants should work towards an Associates Degree program preferably in a STEM or Cyber Security program, or accumulate two years of college credit towards an accredited college degree in any area of interest.

(8) Broaden their focus to include functional training such as the Airborne Course, Air Assault Course, Ranger School, and Culture and Language Training.

c. *Staff Sergeant*.

(1) Staff Sergeants should continue to become a highly sought after mentor. Mentorship requires a leader to take every opportunity to teach, counsel, or coach to build skills and confidence in Soldier(s), not limited to formal sessions which could occur at any juncture.

Mentoring develops great leaders to lead great Soldiers. Competent and confident NCOs are the result of progressive and sequential education, training, and experience. The Staff Sergeant overseas the development of team and squad training, while beginning to build junior leaders and enhancing technical and tactical skill sets.

(2) Master the military publications noted in the preceding skill levels and expand proficiency across the spectrum of Army and Joint administrative publications as necessary or required. These NCOs should know where to find military publications related to their career field and study them to become familiar with the concepts therein. One such publication that can be helpful towards self-development of CMF17 is CALL 16-13 Cyberspace Operations found on the Center for Lessons Learned (CALL) website.

(3) Strive to achieve honors (i.e. Commandant's List, Distinguished Graduate, or Honor Graduate) at PME schools. Complete SSD/DLC 3)

(4) Participate in competitive boards such as the NCO of the Month, Quarter, or Year, Sergeant Audie Murphy, Sergeant Morales, and Army Best Warrior Competitions. These boards broaden the knowledge base, instill discipline, improve the ability to communicate verbally to enhance confidence, build more adaptive leaders and they set the example for Soldiers to follow. Staff Sergeants should host Mock Boards and volunteer to for competitive board membership.

(5) Participate in skill enhancing and volunteer events like local STEM groups and activities as well as Cyber Challenges and Industry Competitions to broaden technical knowledge base and network with participating agencies. These events are used as opportunities for team building and mentorship to subordinate Soldiers and keep technical skills sharp and relevant, plus develop positive community relationships and grow professionals both inside and outside of the service.

(6) Awards and decorations serve to recognize Soldiers for their accomplishments and tend to both motivate fellow Soldiers and build the team. Staff Sergeants should write and submit award recommendations for subordinates and mentor Soldiers on achievements that warrant unit recognition.

(7) Staff Sergeants should begin working toward a Bachelors Degree preferably in a STEM or Cyber Security program or accumulate four years of college credits towards an accredited degree in any area of interest. Staff Sergeants may also consider applying for the Degree Completion Program/Cooperative Degree Program IAW AR 621-1.

(8) Broaden their focus to include functional training such as Battle Staff, Master Fitness Trainer (MFT), Master Resilience Trainer (MRT), Equal Opportunity (EO), and Sexual Harassment/Assault Response and Prevention (SHARP) representative to add value to the organization.

(9) Staff Sergeants should seek opportunities to be placed in generating force and broadening assignments which will separate them from their peers. Generating and broadening assignments include: Drill Sergeant, Recruiter, ALC Small Group Leader, AIT Instructor/Training Developer, DISA, NSA, DIA, DEA, and Training with Industry (TWI).

(10) Staff Sergeants should maintain awareness of their continuing education (CE) hours and maintenance fees associated with credentials to remain current and seek additional credentialing as listed on the COOL Website.

d. *Sergeant First Class*.

(1) As NCOs become more senior in rank, self-motivated development becomes more important. Activities such as professional reading, technical certifications, and college courses assist the Senior NCO in developing organizational leadership skills needed to coach, teach, and mentor Soldiers. Development of writing and speaking skills are essential and are a matter of particular emphasis. Subjects such as organizational behavior, personnel management, time management, Army and Joint operations, and battle staff functions should be emphasized as essential to a Sergeant First Class.

(2) Doctrinal, management, and operational topics should begin to assume a greater portion of reading materials. These Soldiers should master the military publications noted in the preceding skill levels, in addition to joint publications that can be found on the Joint Chief of Staff webpage such as: CJCSI 1805.01B, CJCSI 6245.01A, CJCSI 3100.01D, CJCSM 3150.07E to expand knowledge of Army and Joint cyberspace doctrinal principles.

(3) Strive to achieve honors (i.e. Commandant’s List, Distinguished Graduate, or Honor Graduate) at PME schools. Complete SSD/DLC 4.

(4) Sergeants First Class should look to host Mock Boards at the section, platoon and company level and serve as a competitive board member.

(5) Participate in and coordinate skill enhancing events like local STEM groups and activities as well as Cyber Challenges and Industry Competitions to broaden technical knowledge base and network with participating agencies. Volunteering is a critical aspect of a senior NCO and building trust as well as developing our youth enhances community trust and relationships, while setting our next generation up for success.

(6) Sergeants First Class should write and submit award recommendations for subordinates and mentor Soldiers on achievements that warrant unit recognition. The Sergeant First Class should review all subordinate leader initated award and personnel actions prior to submission.

(7) As advanced education gains increased importance, Sergeants First Class should strive to complete a Bachelor’s Degree preferably in a STEM or Cyber Security program or accumulate four years of college credits towards an accredited degree in any area of interest. Sergeants First Class may also consider applying for the Degree Completion Program/Cooperative Degree Program IAW AR 621-1.

(8) Broaden their focus to include functional training such as Battle Staff, Master Fitness Trainer (MFT), Master Resilience Trainer (MRT), Equal Opportunity (EO), and Sexual Harassment/Assault Response and Prevention (SHARP) representative to add value to the organization.

(9) Sergeants First Class should seek generating force and broadening assignments which will separate them from their peers. Generating force and broadening assignments include: Drill Sergeant, Recruiter, SLC Small Group Leader, Instructor, Training with Industry (TWI), HRC Enlisted Assignments NCO/ Professional Development NCO (PDNCO), RDTE, Special Agencies, and Senior Career Manager

(10) Sergeants First Class should maintain awareness of continuing education (CE) hours and maintenance fees associated with credentials to keep them valid and seeking additional credentialing as listed on the COOL Website. In addition, they should look for opportunities to research, write, peer-review, as well as seek peer-review in an effort to publish professional articles, papers, and books.

e*. Master Sergeant/First Sergeant.*

(1) These Soldiers should recognize their increasing role as a senior NCO and pursue opportunities from various sources and publications that will enhance their understanding of “How The Army Runs” in order to influence and improve the Army’s systems that contribute to the success of their organizations.

(2) Master the military publications noted in the previous skill levels and expand proficiency across the spectrum of Army and Joint administrative, doctrinal, operational, and technical publications, as necessary or required. Continue to build on organizational and strategic understanding with emphasis on upper level management tasks covered in AR 220-45, AR 614-200, AR 840-10, CJCSM 3122.05, CJCSM 3130.01 and Capstone Concept for Joint Operations (CCJO): Joint Force 2020. Additional publications that provide for self-development at this level would be DoD Instruction (DODI) S-5240.23, and DODI 8500.01 which are found on the Executive Services Directorate, Directives Division webpage. These publications further expand knowledge in the planning and support of Army and Joint cyberspace doctrinal principles.

(3) Master Sergeants/First Sergeants should continue to exploit other distributed learning programs and broaden their focus to include functional training, pursue functional course offerings from various sources that will enhance their understanding of how the Army runs in order to influence and improve the Army’s systems and contribute to the success of their organizations.

(4) Strive to achieve honors (i.e. Commandant’s List, Distinguished Graduate, or Honor Graduate) at schools.

(5) Master Sergeants/First Sergeants should look to organize, coordinate, and actively support competitive boards such as the Army Best Warrior Competition, Industry Competitions, and Cyber Challenges to broaden the knowledge base, instill discipline and improve the Soldier's

ability to communicate verbally to enhance confidence and build more adaptive Leaders.

(6) Master Sergeants/First Sergeants should write and submit recommendations for awards for their Soldiers and mentor Soldiers on tasks that stand out to the unit for recognition.

(7) As advanced education gains increased importance, Master Sergeant/First Sergeant should strive to work towards a graduate degree preferably in a STEM or Cyber Security program or accumulate college credit towards an accredited degree in any area of interest. Master Sergeant/First Sergeant may also consider applying for the Degree Completion Program/Cooperative Degree Program IAW AR 621-1.

(8) Broaden their focus to include functional training like Battle Staff, Joint Cyberspace Operations Planners Course (JCOPC), Army Cyber Operations Planners Course (ACOPC, and Joint Network Analysis Course (JNAC)

(9) Master Sergeant/First Sergeant should look to be placed in generating and broadening assignments which will help them to stand out among their peers. Generating and broadening assignments include: Training with Industry (TWI), HRC Enlisted Assignments NCO/ Professional Development NCO (PDNCO), Senior Career Manager, and Senior Instructor

(10) Master Sergeant/First Sergeant should keep up with their continuing education (CE) and maintenance fees associated with credentials to keep them valid and seek to complete additional credentialing as listed on the COOL Website. In addition, they should look for opportunities to research, write, peer-review, as well as seek peer-review to publish professional articles, papers, and books.

f*. Sergeant Major/Command Sergeant Major.*

(1) The Sergeant Major guides cyberspace, EW, and CEMA organizations and missions in support of Army and combatant command objectives. The Sergeant Major understands and masters Joint and Army principles to integrate within the operational framework. The goal of the SGM/CSM is to continually develop organizational leadership skills needed to coach, teach, and mentor Soldiers. Outstanding communications skills are required just by the nature of the number of Soldiers their communications reach. Skills in community and public relations are also important since the SGM/CSM will often represent the command or Army in civic functions.

(2) The Sergeant Major reads a wide-ranging selection of military and civilian professional publications on a regular basis, as well as, current publications on world politics, economics, and current events to broaden and deepen the knowledge base required for a senior Army leader. The Sergeants Major talent management overview may be accessed from the Sergeants Major Management Directorate on the HRC website.

(3) Write articles for publication in Army and public professional journals. Seek out public speaking opportunities and community involvement. Represent the Army in civic functions to enhance leadership, build trust and hone existing skill sets.

(4) Possess a Bachelor’s Degree and actively work towards completing a Master’s Degree in a chosen discipline.

(5) Broaden their focus to include functional training like Keystone and Pre-Command Course. Complete SSD/DLC 5.

(6) Sergeant Major/Command Sergeant Major should look to be placed in generating and broadening assignments which will help them to stand out among their peers. Generating and broadening assignments include: Operations SGM, Chief Career Management NCO/Proponent SGM, Joint Agency SEL, Training and Education Division SGM, CSM, and SMC Instructor

Chapter 4. MOS 17C Cyber Operations Specialist

a. Major duties. The Cyber Operations Specialist executes offensive and defensive cyberspace operations in support of the full range of military operations by enabling actions and generating effects across all domains. The Cyber Operations Specialist ensures the freedom of maneuver within the cyberspace domain and denies the same to adversaries. The Cyber Operations Specialist will generate outcome based cyber effects intended to project power by the application of force in and through cyberspace targeting enemy and hostile adversary activities and capabilities. The Cyber Operations Specialist will generate cyber effects in order to protect data, networks, net-centric capabilities, and other designated systems by detecting, identifying, and responding to attacks against friendly networks. The Cyber Operations Specialist produce integrated and synchronized cyber effects with other lethal and nonlethal actions to enable commanders to mass effects and gain advantages in cyberspace and across other domains which directly or indirectly support objectives on land by employing devices, computer programs or techniques including combinations of software, firmware, or hardware designed to create an effect in or through cyberspace. As an integral part of the national cyberspace workforce, Cyber Operations Specialists are generally aligned under standardized cyberspace work roles defined by the DoD Cyberspace Workforce Framework. A description of the primary functions relevant to the Cyber Operations Specialist are as follows: Analyst, operator, planner, and engineer.

b. Prerequisites

(1) Security Clearance: The clearance requirements to attend training is an Interim TS/SCI reflected within JPAS or current SSBI with TS/SCI eligibility reflected within JPAS. A fully adjudicated TS/SCI (SI/TK/G/HCS) reflected within JPAS will be required to complete training. Soldier must be capable of passing a counterintelligence scope polygraph (CSP) at any time to hold this MOS. Soldiers who refuse to take or fail a CSP will be reclassified.

(2) Physical demands: Rating and qualifications for initial award of MOS.Cyber Operations Specialist must possess the following qualifications:

(a) A physical demands rating of Moderate (Gold).

(b) A minimum OPAT score of Standing Long Jump (LJ) – 0120 cm, seated Power Throw (PT) – 0350 cm, Strength Deadlift (SD) – 0120 lbs., and Interval Aerobic Run (IR) – 0036 shuttles

(c) A physical profile of 222221.

(3) Qualifying scores:(a) A minimum score of 110 in aptitude area GT and a minimum score of 113 in aptitude area ST on Armed Services Vocational Aptitude Battery (ASVAB) test administered prior to 1 July 2004.(b) A minimum score of 110 in aptitude area GT and a minimum score of 112 in aptitude area ST on ASVAB tests administered on and after 1 July 2004..(c) A minimum score of 60 on the Information Communication Technology Literacy (ICTL) test (a.k.a. Cyber Test) for IET accessions on and after 1 April 2014.

(4) Civilian Education: A high school graduate or equivalent prior to entry on active duty

(5) Formal Training: Successful completion of 17C Cyber Operations Specialist Course, conducted under the auspices of the US Army Cyber School is mandatory. Constructive credit waiver for formal training may be granted by Commandant, US Army Cyber School, Fort Gordon, GA 30905-5300.

(6) Additional information for Prerequisites are found in DA PAM 611-21 Chapters 9-14.

c. Goals for development. Soldiers serve in varying assignments from the strategic to operational-level. Due to the inherent technical specificity of MOS 17C, documented leadership positions common to other CMFs, such as team leader, squad leader, platoon sergeant, are less common. Therefore, NCOs in this CMF must strive to seek additional broadening opportunities.

(1) *Private-Specialist/Corporal*.

(a) Institutional training. Advanced Individual Training (AIT), and appropriate PME course as outlined in the Select, Train, Educate, And Promote (STEP) program. Successful graduation with honors from this course could be a significant promotion factor.

(b) Organizational Training: Organizational training for this level will prepare Soldiers to align with one of the four functions (operator, planner, analyst, and engineer) which will then develop into a work role. Organizational training is determined by the unit and include: J7 Pipeline training, Basic Joint Qualifications Requirements (JQR), T10 Basic Operator Course (T10BOC), and Methodologies.

(c) Civilian Education: College courses that work towards an Associate's Degree in any area of interest should be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM, Computer Information Systems management, Computer Science, Computer Networks and Security, Data Science, Basic Malware Analyst, and Cybersecurity.

(d) Credentialing: Seeking industry credentials is an important part of staying competitive with peers in the Cyber CMF not only for documented continuing education and promotion points but as a means to stay current with industry level technical skills and trends.

Credentials to work towards include but are not limited to: CompTIA A+, CompTIA SEC+, CompTIA NET+, CompTIA Linux+, EC-Counsel CE|H, Certified Wireless Technology Specialist (CWTS), and Cisco Certified Entry Networking Technician (CCENT)

(e) Operational assignments. Primary assignment, during the early years of a career, focus should remain at the operational level in a joint environment, building a strong base of technical expertise, basic MOS skills, and common Soldier tasks. Soldiers should seek responsibility and take advantage of opportunities to display their leadership skills, initiative, and motivation.

(f) Self-development. SSD/DLC 1. There are four functions which focus on different aspects of the cyber mission. As a guide to self-development in each one of these functions the following outlines a description of tasks to master at this level:

(1) Analyst: Work towards having a basic understanding of how to use information, collected from a variety of resources, when assessing systems, networks, hardware, software, applications, and personas to identify, analyze, and consider effects in support of commander's requirements. Conduct overall vulnerability analysis, provide risk mitigation support, understand, detect, and emulate adversary TTPs

*(2)*Operator: Work towards having a basic understanding of how to gain access to or defend against physical or logical access to network components; understand, detect, and emulate network infrastructure adversary TTPs.

(3) Planner: Work towards having a basic understanding of how to coordinate and plan operations including scheduling, gaining proper network accesses, and scoping lines of effort.

(g) (4) Engineer: This function is typically designated for higher skill levels, but can be assigned earlier based on technical expertise. Engineers are responsible for having knowledge in analysis of system vulnerabilities, product research, capability development, documentation, and implementation of software and hardware capabilities that operate in and through cyberspace and serve as a force multiplier for maneuver forces.Additional training. N/A.

(h) Special assignments. N/A.

(2) Sergeant.

(a) Institutional training: Appropriate PME course as outlined in the Select, Train, Educate, And Promote (STEP) program. Suggested training for career progression includes but is not limited to: Critical Thinking and Structured Analysis (CTSA), and Computer Network Operations Development Program (CNODP). Successful graduation with honors from these courses could be a significant promotion factor.

(b) Organizational Training: Organizational training for this level should align with designated work role. Organizational training is determined by the unit and includes: Work role designated Joint Qualifications Requirements (JQR), Squad Methodologies, Gunnery I-IV, and Basic Scripting (Python, Bash, and PowerShell)

(c) Civilian Education: College courses that work towards an Associate Degree in any area of interest should be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM, Computer Information Systems, Computer Science, Computer Networks and Security, Data Science, Basic Malware Analyst, Essential C programming and Cybersecurity.

(d) Credentialing: Seeking industry credentials is an important part of staying competitive within the Cyber CMF not only for documented continuing education and promotion points but as a means to stay current with industry level technical skills and trends. Credentials to work towards include but are not limited to: GIAC Security Essentials (GSEC), GIAC Certified Forensic Examiner (GCFE), GIAC Certified Intrusion Analyst (GCIA), CompTIA Advanced Security Practitioner (CASP+), Certified Wireless Network Administrator (CWNA), Cisco Certified Network Analyst (CCNA), Cisco Certified Network Analyst- Security (CCNA-S), Cisco Certified Network Analyst-Cyber Operations (CCNA-Cyber Ops), and A Red Hat® Certified Engineer (RHCE®)

(e) Operational assignments. Primary assignment focus should remain at the operational level in a joint environment. Focus on building a strong base of technical expertise, basic MOS skills and being work role certified Basic or higher. Soldiers should seek responsibility and take advantage of opportunities to practice and display their leadership skills, initiative, and motivation.

(f) Self-development. SSD/DLC 2. Each of the four functions focuses on different aspects of the cyber mission. As a guide to self-development in each one of these functions the following

outlines a description of tasks to master at this level:

(1) Analyst: Knowledge of using analytical skills to assist in defending networks, using established analytic tradecraft to perform network mapping, basic protocol analysis, characterizing network usage, and show proficiency to conduct all-source research and analysis to develop intelligence and targeting products.

(2) Operator: The Basic Operator conducts cyberspace operations by employing tools, techniques, and procedures to generate effects. They also have the inherent responsibility of protecting tools and infrastructure throughout all phases of their operations.

(3) Planner: Basic Planners fuse analytics and intelligence into a comprehensive cyber plan. This plan is used by tactical operations elements to provide objectives and effects to be achieved by their missions.

(4) Engineer: Basic Cyberspace Capability Engineer is proficient in the C and Python programming languages at an intermediate level and has a basic-level understanding of data structures, algorithms, object oriented programming, secure design, operating systems, x86 assembly, and SQL. Basic cyberspace capability engineers are responsible for completing assigned tasks and modules with guidance and supervision from a Senior or Master cyberspace capability engineer in order to create a capability in support of operational requirements

(g) Additional training: Exploitation Analyst (EA), Remote Interactive Operator Training (RIOT).

(h) Special assignments. N/A.

(3) *Staff Sergeant*.

(a) Institutional training: Appropriate PME course as outlined in the Select, Train, Educate, And Promote (STEP) program. Suggested training for career progression includes but is not limited to: Joint Advanced Cyber Warfare Course (JACWC), Joint Network Analysis Course (JNAC), and Cyber Operator Training Course (COTC). Successful graduation with honors from these courses could be a significant promotion factor.

(b) Organizational Training: Organizational training for this level should align with designated work role. Staff Sergeants should be senior level certified in a work role. Organizational training is determined by the unit and include: Senior Joint Qualifications Requirements (JQR), Analytical Writing Essentials (AWE), Red Hat OpenStack Administrator, Senior Gunnery I-IV, Basic Scripting (Python, Bash, and PowerShell), Securing Linux, Hacker tools, techniques, exploits, and incident handling, and Sensor Basic Course

(c) Civilian Education: Complete an Associate Degree in any area of interest as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM, Computer Information Systems, Computer Science, Computer Networks and Security, Data Science, Basic Malware Analyst, Essential C programming, Electrical Engineering and Cybersecurity.

(d) Credentialing: Seeking industry credentials is an important part of staying competitive within the Cyber CMF not only for documented continuing education but as a means to stay current with industry level technical skills and trends. Credentials to work towards include but are not limited to: GIAC Certified Enterprise Defender (GCED), GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Penetration Tester (GPEN), (GIAC) Web Application Penetration Tester (GWAPT), GIAC Certified Unix Security Administrator (GCUX), Cisco Certified Network Analyst (CCNA) Wireless, Cisco Certified Network Analyst (CCNA) Data Center, Cisco Certified Network Analyst (CCNA) Service Provider, Certified Information Systems Security Professional (CISSP)and Microsoft Certified Solutions Associate (MCSA): Windows 10

(e) Operational assignments. Assignment focus should not only be in an operational level in a joint environment but also include generating and broadening assignments. Leadership assignments should be a primary focus for Staff Sergeants.

(f) Self-development. SSD/DLC 3. Participate in at least one Work Role Working Group (WRWG), Assessor tasking, or TH Working Group (THWG). Focus on self-development in one of the functions at this level:

(1) Analyst: Demonstrate the ability to conduct low to moderate level malware analysis. Principle tasks: conduct database queries, understand advanced protocol analysis, programming fundamentals, and produce reports. Assist Operational Planners with developing overarching strategies and advise on courses of action for creating effects that meet operational requirements.

(2) Operator: The Senior Operator is tasked with training and testing of personnel and capabilities. They are also responsible for mitigating risk while leveraging tools, techniques, and procedures to secure new accesses in support of military operations beyond that of the Basic level. The Senior Cyber Operator will lead tactically oriented cyber support teams and aid in the integration of cyberspace support capabilities in the supported unit's MDMP.

(3) Planner: Senior Planners perform the same functions as Basic Planners, but also demonstrate higher levels of operational understanding. They are not only able to interface with tactical elements, but also with higher echelons of command to translate tactical and strategic objectives into long term National strategies.

(4) Engineer: A Senior Engineer specializes in a focus area and is responsible for the direction of a project within this specialty. The specialty areas are: UNIX access; Windows access; RF access; network architecture and applications; UNIX persistence; Windows persistence; embedded; and other (e.g., data science and machine learning). The access specialties involve reverse engineering hardware and software in order to identify vulnerabilities and crafting exploits for those vulnerabilities. Thus these specialties make use of platform-specific reverse engineering and low-level programming. The persistence specialties aim to use provided access to install software which allows operators persistent and convenient control of a targeted system. These specialties involve a deep understanding of a platform along with technical stealth and tradecraft. The UNIX specialties might further specialize in iOS or Android.

(g) Additional training: Exploitation Analyst (EA), Remote Interactive Operator Training (RIOT). Drill Sergeant Course, Instructors Course

(h) Special assignments. Adjunct Faculty, Defense Information Systems Agency (DISA), Special Mission Unit (SMU), Training with Industry (TWI), Special Operations Forces (SOF), expeditionary cyberspace support, Joint, Interagency, Intergovernmental, and Multinational (JIMM), Interactive On-net Operator (ION), and Tool Developer

(4) Sergeant First Class.

(i) Institutional training: Appropriate PME course as outlined in the Select, Train, Educate, And Promote (STEP) program. Suggested training for career progression includes but is not limited to: Joint Targeting Staff Course and Malware Analysis Course. Successful graduation with honors from these courses could be a significant promotion factor.

(j) Organizational Training: Organizational training for this level should align with designated work role. Sergeants First Class should be master level certified in a work role. Organizational training is determined by the unit and includes: Master Joint Qualifications Requirements (JQR), Master Gunnery I-IV.

(k) Civilian Education: Sergeants First Class should be working towards a Bachelor's Degree in any area of interest. It should also be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM, Computer Information Systems Management, Computer Science, Computer Networks and Security, Data Science, Basic Malware Analyst, Essential C programming, Electrical Engineering and Cybersecurity.

(l) Credentialing: Seeking industry credentials is an important part of staying competitive within the Cyber CMF not only for documented continuing education but as a means to stay current with industry level technical skills and trends. Credentials to work towards include but are not limited to: GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), GIAC Reverse Engineering Malware (GREM), GIAC Python Coder (GPYC), Certified Wireless Analysis Professional (CWAP), Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE), Microsoft Certified Solutions Associate (MCSA): Windows Server, Microsoft Certified Solutions Associate (MCSA): Productivity, Microsoft Certified Solutions Associate (MCSA): Mobility, Red Hat OpenStack Administrator, Linux Professional Institute Certified Level 2 (LPIC-2), and Red Hat Certified System Administrator (RHCSA)

(m) Operational assignments. Leadership assignments should be a primary focus for Sergeant First Class. Sergeants First Class should be looking to fill staff positions that will help them better understand how the organization works from a higher level. Assignment focus should not only be operational level but also generating and broadening assignments.

(n) Self-development. SSD/DLC 4. Participate in at least one Work Role Working Group (WRWG), Assessor tasking, or TH Working Group (THWG). Focus on self-development in one

of the functions at this level:
(1) Analyst: Demonstrates the ability to provide strategic guidance on emerging threats across different mission sets. Sergeants First Class demonstrate their capability in advanced queries, validate draft network signatures, quality control of implemented network signatures for efficiency, multiple programming languages, and conduct moderate to high level malware analysis. Identifies access and collection gaps across multiple infrastructures at various echelons and recommends or develops analytical and initial access strategies for the successful execution of offensive and defensive cyberspace operations
(2) Operator: The Master Operator will oversee cyber operations and advise the cyber planner on team and unit requirements. Master level operators will develop training requirements and operational tactics, techniques and procedures. A Master level Operator will also be required to invest knowledge and time into building and sustaining the work role through mentoring junior operators, conducting formal training and advising the command on capabilities and limitations. The Master Operator is trained in multiple operational disciplines. They are expected to bring significant expertise, problem solving, and mentorship to bear on highly challenging problem sets and interface with personnel across various domains and echelons.
(3) Planner: Master Planners continue to operate with higher echelons of command, but they have additionally set themselves apart from their peers as technical experts who are intimately familiar with networking fundamentals and cyber weapons/capabilities pairing
(4) Engineer: A Master Cyberspace Capability Engineer has mastered the specialty and is responsible for providing guidance and technical direction over multiple projects in the specialty. Master Cyberspace Capability Engineers mentor senior cyberspace capability engineers as they progress to the Master level. Master Cyberspace Capability Engineers provide the highest level of technical insight during the design of new capabilities.
(o) Additional training: Exploitation Analyst (EA), Remote Interactive Operator Training (RIOT)
(p) Special assignments. Adjunct Faculty, Defense Information Systems Agency (DISA), Special Mission Unit (SMU), Training with Industry (TWI), Special Operations Forces (SOF), expeditionary cyberspace support, Joint, Interagency, Intergovernmental, and Multinational (JIMM), Interactive On-net Operator (ION), Human Resources Command (HRC) Enlisted Assignments NCO/ Professional Development NCO (PDNCO), and Career Manager NCO
(5) Master Sergeant/First Sergeant.
(a) Institutional training: Appropriate PME course as outlined in the Select, Train, Educate, And Promote (STEP) program.
(b) Organizational Training: Organizational training for this level should align with designated work role. Master Sergeants should be master level certified in a work role. Organizational training is determined by the unit and include: Master Joint Qualifications Requirements (JQR), Master Gunnery I-IV.
(c) Civilian Education: Master Sergeants should be completing a Bachelor's Degree in any area of interest. It should also be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM, Computer Information Systems Management, Computer Science, Computer Networks and Security, Data Science, Basic Malware Analyst, Essential C programming, Electrical Engineering and Cybersecurity.
(d) Credentialing: Work on Continuing Education (CE) hours which will help to renew current certifications. CE hours can come from: Obtaining higher level certifications, college courses where at least 50% of the course content is directly related to certification, authorized webinars, authorized conferences, documented work experience, participation in IT industry activities, publication of a relevant article, white paper, blog post or book. See certification's vendor for more details.
(e) Operational assignments. Master Sergeants are assigned as Subject Matter Experts (SME) in the technical integration of cyberspace attack; defense; Intelligence, Surveillance, and Reconnaissanceand Operational Preparation of the Environment in support of unified land operations. Master Sergeants are also assigned as First Sergeants and Operations Sergeants. These assignments rely heavily on leadership experience and technical expertise in order to synchronize effects within the Joint operational and targeting planning process and operational framework. Leadership assignments should be a primary focus for Master Sergeants. Master

Sergeants should be looking to fill staff positions that help them with a better understanding of how the organization works from a higher level. Assignment focus should not only be operational level but also generating and broadening assignments.

(f) Self-development. At this level a Master Sergeant will continue to master their skill set. They should stay current with the latest cyber issues and read documents that are published from all echelons of the cyber mission force for a greater understanding of the community's posture within the joint community. These documents can be found on the ACT CMF 17 community.

(g) Additional training: Master Instructor Certification

(h) Special assignments. Adjunct Faculty, Defense Information Systems Agency (DISA), Special Mission Unit (SMU), Training with Industry (TWI), Special Operations Forces (SOF), Joint, Interagency, Intergovernmental, and Multinational (JIMM), Interactive On-net Operator (ION), Human Resources Command (HRC) Enlisted Assignments NCO/ Professional Development NCO (PDNCO), Army Cyber Institute (ACI), and Senior Career Manager NCO

(6) Sergeant Major/Command Sergeant Major.

(a) Institutional training. Appropriate PME course as outlined in the Select, Train, Educate, And Promote (STEP) program.

(b) Operational assignments. Sergents Major are assigned to serve as the senior enlisted advisor, providing senior level technical and tactical advice to command and staff on all aspects of offensive and defensive cyberspace operations matters (i.e. Operations SGM). These assignments have significant influence on Joint, theater, ASCC, and inter-agency level operations. This is accomplished through the development, prioritization, allocation, and coordination of cyberspace operations. In addition, Sergents Major provide expertise in the development of strategic concepts and operations through direct involvement with HQDA, FORSCOM, TRADOC, CCMDs, Army Commands, and other National and Strategic level US Government and DOD organizations.

(c) Civilian Education: Sergeants Major should be working towards or completing a Master's Degree in any area of interest. It should also be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM, Computer Information Systems Management, Computer Science, Computer Networks and Security, Data Science, Basic Malware Analyst, Essential C programming, Electrical Engineering and Cybersecurity.

(d) Credentialing: Work on Continuing Education (CE) hours which will help to renew current certifications. CE hours can come from: higher level certifications, college courses where at least 50% of the course content is directly related to certification, authorized webinars, authorized conferences, documented work experience, participation in IT industry activities, publication of a relevant article, white paper, blog post or book. See certification's vendor for more details.

(e) Self-development. SSD/DLC 5. Read all books recommended on the SMA's Professional Reading List for this grade as well as regular reading of professional military and current events publications and journals to expand the knowledge base and organizational leadership skills needed to coach, teach, train, and mentor Soldiers. (See chapter 3f for further information.)

(f) Additional training. BN/BDE Pre-Command Course; Senior Executive Level-How the Army Runs; CSM/SGM Legal Orientation Course; Senior Leader Seminar; Army Strategic Leader Development Program (ASLDP)-Basic; ASLDP-Intermediate; ASLDP-Advanced; Army NCO Senior Leader Development Program-Executive; Army NCO Senior Leader Development Program-Strategic.

(g) Special assignments. Proponent SGM, Operations SGM, DAMO Cyber SGM, Chief Career Management NCO, Joint Agency Senior Enlisted Leader (SEL), Training and Education Division SGM, DISA and ACI.

Chapter 5. MOS 17C Professional Development Model

Access to the career map is located on the Army Career Tracker (ACT) website. ACT is the Army's first comprehensive leadership development tool to integrate training, assignment history, and formal/informal education activities in one location. ACT is accessed from the Soldier's AKO homepage by selecting "My Training" from the "Self Service" dropdown, then selecting “Visit ACT” from the “ACT” gadget. It may be accessed at the following web address: https://actnow.army.mil/. The Sergeants Major professional development model and talent management overview may be accessed from the Sergeants Major Management Directorate at the following web address (CAC required for access): https://www.hrc.army.mil/Site/Protect/Assets/Directorate/EPMD/5%20pdf%20WG%20SGM-CSM_Talent_Management_Brief.pdf

Chapter 6. MOS 17C Reserve Component (RC)

All Soldiers, regardless of component, are essential to the successful accomplishment of military operations. The RC provides a substantial percentage of the structure and capability of the Army’s operational force. RC 17C Soldiers must possess the same qualifications and capabilities as AC personnel and the quality of training of 17C RC Soldiers will be the same as their AC counterparts. Duty assignments and professional development steps for career progression parallel those of the AC. Geographic limitations and varying TDA authorizations, respectively, will restrict the types of units and availability of 17C assignments.

Chapter 7. MOS 17E Electronic Warfare Specialist

a. *Major duties.* Electronic Warfare Specialists are subject matter experts on the manipulation, control, and dominance of the electromagnetic spectrum. They advise and assist the commander or command Electronic Warfare Officer (EWO), as applicable, to defeat the enemy through planning, coordination, integration, and execution of Electronic Attack (EA); protect and harden friendly systems, processes, and personnel by developing, training, and executing Electronic Protection (EP); and support current and future operations by planning and performing Electronic Warfare Support (ES). Electronic Warfare Specialists plan for and coordinate the integration of electronic warfare into military operations through every step of the Military Decision Making Process (MDMP).

b. *Prerequisites.*

(1) Security Clearance: Soldier must maintain TOP SECRET (TS) Sensitive Compartmented Information (SCI) access eligibility requirements to be awarded and maintain this MOS (TS/SCI granted or open T5 investigation reflected in JPAS). The clearance requirement to begin training is SECRET with T5 investigation initiated and reflected in JPAS.

(2) Based on specific unit of assignment requirements, Soldiers in this MOS must be capable of passing a counterintelligence scope polygraph (CSP).

(3) Physical demands: Rating and qualifications for initial award of MOS. Electronic Warfare Specialist must possess the following qualifications:

(b) A physical demands rating of Moderate (Gold).

(c) A minimum OPAT score of Standing Long Jump (LJ) – 0120 cm, seated Power Throw (PT) 0350 cm, Strength Deadlift (SD) – 0120 lbs., and Interval Aerobic Run (IR) – 0036 shuttles

(d) A physical profile of 222221.

(e) Normal Color vision

(4) Qualifying scores: A minimum score of 105 in aptitude area SC, ST and EL in Armed Services Vocational Aptitude Battery (ASVAB) test.

(5) Civilian Education: (a) A high school graduate or equivalent prior to entry on active duty (b) Credit for successful completion of 1 year of high school algebra or equivalent.

(6) Formal Training: Successful completion of MOS 17E Course conducted under the auspices of the US Army Cyber School is mandatory. Waiver may be granted by Commandant, US Army Cyber School, Fort Gordon, GA 30905-5300.

(7) Additional information for Prerequisites are found in DA PAM 611-21 Chapters 9-14

c. *Goals for development.* NCOs should serve in varying assignments from the tactical to the strategic in TOE and TDA units. The EW NCO must strive to seek additional broadening and leadership opportunities at all levels such as recruiting NCO, drill sergeant, instructor, and supervisory positions when given the opportunity.

(1) *Private-Specialist/Corporal*.

(a) *Institutional training.* Advanced Individual Training (AIT), and Basic Leaders Course for Specialists/Corporals.

(b) *Civilian Education.* College courses that work towards an Associate Degree in any area of interest should be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM and Electrical, Computer, or Communications Engineering Technology Degrees.

(c) *Credentialing.* Seeking industry credentials is an important part of staying competitive within the Cyber CMF not only for documented continuing education and promotion points but as a means to stay current with industry level technical skills and trends. Credentials to work towards include but are not limited to: Associate Electronics Technician (CETa), Electronics Associate AC (EM2), Certified Electronics Technician - Journeyman-Level – Computer, Electromagnetic Compatibility (EMC) Technician, and RADAR Electronics Technician (RAD)

(d) *Operational assignments*. Primary assignment focus should remain at the tactical level. During the early years of a career, focus on building a strong base of technical and tactical expertise, basic MOS skills, and common Soldier tasks. Soldiers should seek responsibility and take advantage of opportunities to display their leadership skills, initiative, and motivation.

(e) *Self-development*. SSD/DLC 1. Soldiers should have a basic understanding of military radios like SINCGARS, HF Radios, and Harris 117G radios. They should be familiar with the electromagnetic spectrum, military symbols and graphics, Algebra and Introductory Physics. Soldier should also be familiar with radio frequency communications, wi-fi networks and electro-optics, CREW systems, and electronic warfare principles.

(f) *Additional training*. N/A.

(g) *Special assignments*. N/A.

(2) Sergeant.

(a) Institutional training. Suggested training for career progression include but are not limited to: Battle Staff, Critical Thinking and Structured Analysis (CTSA), and Tactical Information Operations Planner.

(b) Civilian Education. College courses that work towards an Associate's Degree in any area of interest should be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM and Electrical, Computer, or Communications Engineering Technology Degrees.

(c) Credentialing: Seeking industry credentials is an important part of staying competitive within the Cyber CMF not only for documented continuing education and promotion points but as a means to stay current with industry level technical skills and trends. Credentials to work towards include but are not limited to: Associate Electronics Technician (CETa), Electronics Associate Analog (EM3), Certified Electronics Technician - Journeyman-Level – Computer, Electromagnetic Compatibility (EMC) Technician, and RADAR Electronics Technician (RAD)

(d) Operational assignments. Sergeants are assigned to maneuver battalions, Brigade Combat Team CEMA Sections, and EW Platoons. At maneuver battalions they are the EW subject matter experts at that echelon. Sergeants participate in the operations planning process, coordinate EW efforts among staff functions, serve as primary trainers in Electronic Protect measures, and if applicable serve as the Counter Radio Control Improvised Explosive Device Electronic Warfare (CREW) system technical expert, responsible for training and supervising company CREW Specialists as required to ensure an effective CREW Electronic Counter-Measure Force Protection (ECM-FP) program,with oversight of Company-level CREW programs to include troubleshooting, accountability, maintenance, installation and update of associated firmware and threat loads, and will ensure dissemination of same from higher. Sergeants ensure relevant EW training is included in Annual Training Plans; EW information within TAC/TOC SOPs is current and accurate and includes procedures for monitoring and reporting suspected jamming of friendly systems; Sergeants develop and implement EP and jamming TTPs and drills; and prepare and process requests for Electronic Attack support for higher echelon or joint EW assets in support of ground force maneuver. At the BCT CEMA Section, Sergeants assist the CEMA NCOIC and CEMA Sergeant in all aspects of the Brigade EW program and focus on honing technical and operational skill sets in preparation for follow-on assignments and oversee and mentor junior EW Specialists within the CEMA Section. This position is ideal for early development/mentorship of 17E2x soldiers preparing to move to Maneuver BN EWNCO positions. Within the EW PLT, 17E2x serve as EW Team Chiefs, technically and tactically proficient, responsible for the correct deployment, employment, and daily operations of an EW team to include equipment and/or vehicle maintenance, guidance,

mentorship, and sustainment training of junior EW Specialists, and the accomplishment of any mission assigned to the Team from the EW PLT SGT or PL.

(e) Self-development. SSD/DLC 2. Sergeants should be familiar with how to plan, coordinate, and conduct Electronic Attack (EA) in support of ground maneuver and tactical deception. Sergeants should be able to employ ES measures to locate threat systems; be able to support information operations using Electronic Protection (EP) activities to harden communications against intentional or unintentional electromagnetic interference, and have the ability to minimize emission signatures of friendly unit communication and non-communication emitters, and avoid spectrum interference by adjacent units.

(f) Additional training. Airborne; Air Assault; Pathfinder; Ranger.

(g) Special assignments. NCOs at this level may be eligible to apply for selected special assignments, however it is highly recommended to concentrate on successful completion of tactical level assignments.

(3) Staff Sergeant.

(a) Institutional training: Senior Leaders Course (SLC). Suggested training for career progression includes but is not limited to: Battle Staff, Tactical Information Operations Planner Course, Cyber Operations Planners Course, and the Joint Firepower Course.

(b) Civilian Education: Staff Sergeants should be working towards/completing an Associate Degree in any area of interest. This should be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM and Electrical and Computer Engineering Technology Degrees.

(c) Credentialing: Seeking industry credentials is an important part of staying competitive within the Cyber CMF not only for documented continuing education but as a means to stay current with industry level technical skills and trends. Credentials to work towards include but are not limited to: CompTIA A+ ce, CompTIA IT Fundamentals, CompTIA Network+ ce, CompTIA Security+ ce, Microsoft Certification, LINUX Certification, and FCC General Radio Operator License

(d) Operational assignments. Staff Sergeants will primarily be assigned to either BCT or Division CEMA sections as the CEMA Sergeant, or to EW PLTs to serve as the Senior Team Chief. Within the CEMA sections, the CEMA Sergeant will assist the CEMA NCOIC and CEWO in accomplishment of all BCT CEMA planning, integration, and execution into operations; coordinate efforts between subordinate battalion EW operations and the EW PLT; prepare and maintain SOPs and TTPs for dissemination to same; prepare and maintain EW staff estimates; consolidate, review, and process requests for EW support from subordinate battalions to BCT or higher organic and external supporting agencies; train and mentor CEMA section EW Sergeant and Specialists, and assist in the management of the BCT CEMA cell in the Tactical Operations Center (TOC) or Tactical Action Center (TAC). In the EW PLT, the Staff Sergeant will serve as the Senior Team Chief, responsible for accomplishment of the highest priority, most difficult, and most complex EW missions of the PLT. Staff Sergeants will be responsible for the correct deployment, employment, and daily operations of an EW team to include equipment and/or vehicle maintenance, guidance, mentorship, and sustainment training of junior EW Specialists, and the accomplishment of any mission assigned to the Team from the EW PLT SGT or PL. Varied EW assignments are highly desired.

(e) Self-development. SSD/DLC 3. Staff Sergeants should be well versed in Electronic Warfare support (ES) in support of an information collection plan to answer PIR. Staff Sergeants should be able to provide early warning to ground maneuver units, or to assist in the assessment of unit electronic protection (EP) measures.

(f) Additional training. Master Fitness Trainer, Master Resilience Trainer; Common Faculty Development-Instructor Course.

(g) Special assignments. NATO, Combat Training Centers (CTCs); US Army Cyber Command (ARCYBER); Special Missions Units; drill sergeant; recruiter; institutional school instructor.

(4) Sergeant First Class.

(a) Institutional training. Master Leaders Course (MLC). Suggested training for career progression include but are not limited to: Army Basic Space Cadre Course, Joint Electronic Warfare Theater Operations Course (JEWTOC), Joint Network Attack Course (JNAC).

(b) Civilian Education: Sergeants First Class should be working towards/completing a Bachelor's Degree in any area of interest. This should be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM and Electrical and Computer Engineering Technology Degrees.

(c) Credentialing: Seeking industry credentials is an important part of staying competitive within the Cyber CMF not only for documented continuing education but as a means to stay current with industry level technical skills and trends. Credentials to work towards include but are not limited to: Cisco Certified Network Assistant (CCNA), Certified Ethical Hacker (CEH), General Communications Technician (GCT1).

(d) Operational assignments. Sergeants First Class are primarily assigned to EW PLTs and CEMA Sections at Division and above. At the EW PLT they are the PLT SGT. They are tasked by the BCT Operations Section, with input and guidance from the BCT CEMA Section, to execute EW operations in support of ground force maneuver. Sergeants First Class are responsible for tasking EW teams within the PLT, the guidance and mentorship of Team Chiefs and Senior Team Chiefs, talent management of the teams, assisting the Platoon Leader with coordination of EW efforts with the BCT CEMA Section, preparing and maintaining staff estimates of EW Team equipment and personnel, and responsible for the maintenance and upkeep of organic EW assets. At the CEMA Section, Sergeants First Class are the primary planner of CEMA Operations, responsible for CEMA inputs into staff estimates, contingency plans and Operations Orders, responsible for the direction, integration, coordination, and de-confliction of CEMA functions and capabilities, and consolidate, prioritize, and process requests for EW support from external agencies. Additionally, Sergeants First Class develop CEMA training and maintenance programs for dissemination and implementation to subordinate units. Varied EW assignments from the tactical to the strategic level in MTOE and TDA units look favorable for promotion to MSG.

(e) Self-development. SSD/DLC 4. EW Sergeants First Class must possess a thorough understanding of staff functions and processes and the targeting process.

(f) Additional training. Small Group Leader; Pathfinder; Jump Master; SHARP Sexual Assault Response Coordinator (SARC)and Equal Opportunity Leaders Course (EOLC).

(g) Special assignments. US Army Research Labs; Combined Training Centers (CTC); Joint Electromagnetic Preparedness for Advanced Combat (JEPAC); Training With Industry (TWI); senior drill sergeant; recruiter; NCOES small group leader; senior small group leader; equal opportunity advisor; Career Management NCO; Special Mission Units; ARCYBER Staff; USAE Space Command; Cyber Training Battalion.

(5) Master Sergeant/First Sergeant.

(a) Institutional training. Distributed Leaders Course 5 (DLC 5), Special Technical Operations Course (STOPC), and the Electronic Warfare Coordinators Course (EWCC), Information Operations Capabilities (IOCAP). Selected MSGs will attend the Sergeant Major Course at the U.S. Army Sergeants Major Academy.

(b) Civilian Education. Master Sergeants should be working towards/completing a Master's Degree in any area of interest. This should be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM and Electrical and Computer Engineering Technology Degrees.

(c) Credentialing. Seeking industry credentials is an important part of staying competitive within the Cyber CMF not only for documented continuing education but as a means to stay current with industry level technical skills and trends. Credentials to work towards include technical certifications such as General Communications Technician (GCT2).

(d) Operational assignments. Master Sergeants are assigned to BCT and above CEMA Sections to serve primarily as CEMA section NCOICs. Master Sergeants develop and assess robust mentorship and training programs for subordinate EW organizations and NCOs, integrate joint CEMA functions and capabilities in support of ULO at the Division and JTF level focusing on: Special Technical Operations (STO); Offensive and Defensive Cyberspace Operations; Electromagnetic Spectrum Operations (EMSO); and prioritization, de- confliction, and allocation of CEMA resources. When serving as a Cyberspace operations planner Master Sergeants assist in the planning, coordinating, synchronizing, and integrating of offensive and defensive cyberspace operations.

(e) Self-development. EW Master Sergeants should be familiar with Army and Joint Planning processes, Tactical and Joint Operations/Action Center operations, Air Tasking Orders, Offensive and Defensive Cyber Operations, and should remain up to date on EW capabilities and assets available both organically and through external agencies.
(f) Additional training. N/A NA
(g) Special assignments. Combat Training Centers; Human Resource Command (HRC); Training With Industry (TWI); Training Capabilities Management – Electronic Warfare (TCM-EW); Electronic Warfare Doctrine; Special Mission Units; ARCYBER Staff; Security Force Assistance Brigades (SFAB); Cyber Training Battalion.
(6) Sergeant Major/Command Sergeant Major.
(a) Institutional training. Institutional training. Appropriate PME course as outlined in the Select, Train, Educate, and Promote (STEP) program.
(b) Civilian Education. Sergeants Major should be working towards/completing a Master's Degree in any area of interest. This should be implemented as a short term goal for your Individual Development Plan (IDP). Suggested degree plans that help develop technical skills are: STEM and Electrical and Computer Engineering Technology Degrees.
(c) Credentialing. Seeking industry credentials is an important part of staying competitive within the Cyber CMF not only for documented continuing education but as a means to stay current with industry level technical skills and trends. Credentials to work towards are listed in the Army Credentialing Opportunities On-Line web site.
(d) Operational assignments. Sergeants Major are assigned at the Corps, ASCC, or higher echelons as the senior enlisted CEMA advisor to the echelon CEWO and Commander. Sergeants Major mentor command leadership and subordinate Electromagnetic Warfare personnel on CEMA functions and capabilities. Facilitate and synchronize joint CEMA functions and capabilities in support of ULO at the theater, ASCC, and inter-service level focusing on: decisional aspects; prioritization, allocation, and coordination of ground, air, sea, and space CEMA assets and operations; development and pass-down of strategic concepts and operations; direct involvement with HQDA, Army Commands and Army Service Component Commands. Negotiate, establish, and maintain liason within the Army, other services, national, allied, and coalition nations on all CEMA functions and capabilities. Serve on national strategic panels, committees, work groups, and advise international, national, military and civil organizations. Responsible for development, preparation and/or analysis of strategic CEMA guidance for use by subordinate commands through direct interaction with HQDA, ACOM, TRADOC and ASCC.
(e) Self-development. SSD/DLC 5. Read all books recommended on the SMA's Professional Reading List for this grade as well as regular reading of professional military and current events publications and journals to expand the knowledge base and organizational leadership skills needed to coach, teach, train, and mentor Soldiers. (See chapter 3e for additional resources.)
(f) Additional training. BN/BDE Pre-Command Course; Keystone Course; Senior Executive Level-How the Army Runs; CSM/SGM Legal Orientation Course; Senior Leader Seminar; Army Strategic Leader Development Program (ASLDP)-Basic; ASLDP-Intermediate; ASLDP-Advanced; Army NCO Senior Leader Development Program-Executive; Army NCO Senior Leader Development Program-Strategic.
(g) Special assignments. Proponent SGM; HRC Branch SGM; Cyber Training and Education SGM; SMC Instructor; nominative positions (00Z only).

Chapter 8. MOS 17E Professional Development Model

Access to the career map is located on the Army Career Tracker (ACT) website. ACT is the Army's first comprehensive leadership development tool to integrate training, assignment history, and formal/informal education activities in one location. ACT is accessed from the Soldier's AKO homepage by selecting "My Training" from the "Self Service" dropdown, then selecting "Visit ACT" from the "ACT" gadget. It may be accessed at the following web address: https://actnow.army.mil/.

The Sergeants Major professional development model and talent management overview may be accessed from the Sergeants Major Management Directorate at the following web address (CAC required for access):
https://www.hrc.army.mil/Site/Protect/Assets/Directorate/EPMD/5%20pdf%20WG%20SGM-CSM_Talent_Management_Brief.pdf

Chapter 9. MOS 17E Reserve Component

All Soldiers, regardless of component, are essential to the successful accomplishment of military OPS. The Reserve Component (RC) provides a substantial percentage of the structure and capability of the Army's operational force. RC 17E NCO must possess the same qualifications and capabilities as Active Component (AC) personnel and the quality and quantity of training of 17E RC Soldiers will be the same as their AC counterparts. Duty assignments and professional development steps for career progression parallel those of the AC. Geographic limitations and varying MTOE authorizations will restrict the types of units and availability of 17E assignments