DEPARTMENT OF THE ARMY
UNITED STATES ARMY CYBER SCHOOL
633 BARNES AVENUE
FORT GORDON, GEORGIA 30905-5441

ATSR-ZA 22 January 2021

MEMORANDUM FOR RECORD

SUBJECT: Cyber Course Credit Program Standard Operating Procedures (SOP)

1. References.

a. Army Regulation 350-1, Army Training and Leader Development, dated 10 December 2017

b. TRADOC Regulation 350-18, The Army School System, dated 1 May 2018

c. DA Pamphlet 600-3, Officer Professional Development and Career Management, dated 30 September 2019

d. DA Pamphlet 611-21, Military Occupational Classification and Structure, dated 13 January 2020

e. Army Regulation 25-50, Preparing and Managing Correspondence, dated 10 October 2020

2. Purpose. This SOP assigns responsibilities to Cyber School directorates for managing the Cyber Course Credit Program to ensure Cyber Corps Soldiers' applications for course credit are properly processed, evaluated, and completed.

3. Applicability.

a. This SOP applies to all U.S. Army Cyber Career Field personnel engaged in the participation, management, coordination, and execution of the Cyber Course Credit Program across the force.

b. Cyber Corps officers, warrant officers, enlisted personnel, and select personnel from other military service branches, may utilize the Cyber Course Credit Program in accordance with (IAW) all applicable regulations and policies pertaining to each cohort.

c. Credit granted to personnel under the Cyber Course Credit Program does not guarantee U.S. Cyber Command or Cyber Mission Forces training or qualification credit to meet initial or full operational capability requirements. This program applies to course credit primarily for Military Occupational Specialty (MOS), Area of Concentration (AOC), or Skill Identifier (SI) / Additional Skill Identifier (ASI) qualification, and Certificate of Completion producing courses for which the U.S. Army Cyber School is the proponent.

4. Objective. The Cyber Course Credit Program efficiently and effectively evaluates Cyber officers, warrant officers, and enlisted personnel (and select personnel in other military service branches) who possess comparable skills, knowledge, and abilities in order to avoid duplication of training and allow minimal disruption to the operational force. The intent of the Commandant/Chief of Cyber in providing a comprehensive course credit program involves satisfying the operational needs of the Army for qualified Cyber professionals while ensuring standardized skills and qualifications throughout the entirety of the force. The Cyber Course Credit Program will primarily be used to ensure training and qualifications standards are achieved for Cyber MOSs and AOCs. IMPORTANT NOTE: Receiving approved course credit (full or partial) in lieu of course attendance is the exception, not the rule.

5. General. The Cyber School Commandant/Chief of Cyber awards course credit only for Cyber School governed courses and modules under the Cyber Course Credit Program. Furthermore, the Commandant/Chief of Cyber delegates management of the Cyber Course Credit Program to the Director, Office of the Chief of Cyber (OCC) and validation/verification of course credit criteria to the Director, Cyber Training and Education Directorate (CTED). Full or partial credit may be awarded to Cyber Corps Soldiers toward MOS/AOC qualification. The standard with which packets are compared against is the courseware of the relevant Cyber School MOS/AOC producing courses and/or functional courses. Course credit for Cyber School governed training and education may be awarded using a combination of constructive, equivalent, and/or operational credit, as per Annex A. Per regulatory references, course credit for all Primary Military Education course modules (e.g., common core) must be granted by Director of Training, U.S. Army Training and Doctrine Command (TRADOC) G-37.

a. Constructive credit may be granted to individuals in lieu of full or partial course attendance based on previous leadership/operational experience and/or past academic/training experiences.

(1) In all cases, TRADOC or the proponent school will assess the individual’s past comprehensive military or civilian experience against established course terminal learning objectives/learning objectives. Individuals must possess the same skills and qualifications as course graduates.

(2) The Commandant/Chief of Cyber considers “similar courses,” or a combination of “similar course modules,” that provide students the same or similar learning objectives in order to produce graduates with the same skills and qualifications as Cyber School courses and modules as eligible for constructive credit upon individual review.

b. Equivalent credit may be granted to individuals in lieu of course attendance based on courses possessing comparable terminal learning objectives and enabling learning objectives.

(1) Terminal and enabling learning objective/outcome assessments are performed by TRADOC or the respective proponent school. Individuals must possess the same skills and qualifications as course graduates.

(2) The Commandant/Chief of Cyber considers equivalent credit as "same course, different vendor/provider" that provides students with the same learning objectives in order to produce graduates with the same skills and qualifications as Cyber School courses and modules. This approach may also include individual course modules completed through the Cyber School for requesting overall MOS or AOC qualification.

(3) Possession of certifications that demonstrate module or course mastery would be considered equivalent. While current certifications are encouraged, they are not required. This SOP supports the assumption that an applicant received all necessary training to pass the certification test elsewhere.

c. Operational credit may be granted to individuals in lieu of course attendance based on operational experiences. The Commandant/Chief of Cyber considers operational credit as "on the job training or experience" that provides Cyber Career Field personnel the same skills and qualifications as those provided in Cyber School courses and modules controlled by CTED. Since operational experience of this kind is difficult to measure and evaluate, detailed and well-documented supporting evidence must be provided to establish credit. Evidence that may best validate this experience includes evaluation reports, awards, and letters of recommendation/attestation from commanders/supervisors.

6. Cyber Course Credit Review Board (CCRB). The Cyber School will convene the Cyber CCRB, generally on a monthly basis but not less than quarterly, to review applicant packets for Cyber course credit. The board is facilitated by the OCC Cyber Course Credit Program Manager; board members consist of designated representatives from CTED (e.g., College Directors, Course Managers, Senior Instructors, etc.). A minimum of one subject matter expert for each Cyber course or module for which credit is requested must be present and serving as a board member, with no less than three voting board members present; one member may be the expert for more than one course. All CCRBs are considered closed boards due to Personally Identifiable Information concerns and to ensure the integrity of the proceedings. Visitors requesting to attend a board must be individually approved by the OCC Director at least one week prior to the board convening.

7. Responsibilities.

a. The Course Credit Applicant will:

(1) Already be assessed and selected into the Cyber Corps in any component of the Army, or be a designated member of another branch of service requiring Cyber School training. If not already evident on the service members (SM) Soldier Record

Brief (SRB), proof of acceptance into the Cyber Branch must be included in the packet to determine eligibility.

(2) Build a complete individual course credit packet highlighting equivalent constructive, and/or operational experience per module (unit or block) for the AOC, MOS, SI/ASI, or Certificate of Completion producing course for which credit is being applied. See Annex B.

(3) Submit completed packet to OCC (see Annex C) no later than one week prior to the next Cyber Course Credit Review Board convening date (which is typically the third Friday of every month).

(4) Receive course credit determination from OCC at the conclusion of the approval/disapproval cycle and coordinate with their unit S1/G1 section and/or the HRC Information Dominance Branch to schedule required training and/or update personnel records, as appropriate.

(5) Applicants who are submitting for course credit in conjunction with MOS reclassification or branch transfer must include the course credit worksheet (Annex B) for the appropriate MOS, along with the course credit memorandum found in the sample packet (Annex C). These course credit packets are in addition to any vehicle used to reclassify/transfer into the Cyber Career Field. Therefore, do not submit your reclassification packet into the CCRB process; only submit documents relevant to receiving course credit.

(6) For Task Force Echo applicants only: In order for applicants to receive course credit for Cyber Operations Planner Course (COPC) and/or Cyberspace Response Assessment (CsRA), SMs must submit signed memoranda for record (MFRs) from the 91st Cyber Brigade Commander attesting to their completion of each courses terminal learning objectives, enabling learning objectives, and learning support activities. See Annex D and Annex E for example memoranda.

(7) If applicants need to submit documentation via a classified medium (e.g. SIPR / JWICS), email the above address and request a classified point of contact.

b. OCC will:

(1) Publish contact information for course credit packet submission. The contact email is: usarmy.gordon.cyber-coe.mbx.occ-officers@mail.mil.

(2) Receive and review individual course credit packets for completeness.

(3) Facilitate the monthly Cyber CCRB, consisting of designated CTED representatives appointed by the CTED Director, in order to analyze and recommend approval/disapproval determinations to the OCC Director, which are validated by the

Deputy Commandant on behalf of the Commandant/Chief of Cyber. The Cyber CCRB will generally be held monthly on the third Friday, but not less than once per quarter.

(4) Generate approval/disapproval determination memoranda and submit to the OCC Director for approval/signature, and route through the Deputy Commandant for validation on behalf of the Commandant/Chief of Cyber.

(5) Provide applicant with course credit approval/disapproval memorandum, along with specific units, blocks, modules, and/or courses for which credit is awarded or still needed, as applicable. The memorandum will be provided by the Cyber Course Credit Program Manager to the appropriate OCC Division (Enlisted, Warrant Officer, Officer, or Reserve Component) for transmission to the applicant.

(6) If full course credit is awarded through this program that fully qualifies the applicant for an MOS, AOC, SI/ASI, or Certificate of Completion course, OCC will provide the qualification memorandum to the applicant and HRC Information Dominance Branch in order to facilitate the appropriate personnel records update.

(7) Provide interim SOP updates via the CCRB MilSuite page which reflect changes in course content and management. The MilSuite site is located at: https://www.milsuite.mil/book/docs/DOC-748306.

c. CTED will:

(1) Serve as the Cyber Career Field prescribed assessor for Cyber Program of Instruction (POI) courses and modules IAW TRADOC Regulation (TR) 350-18.

(2) Develop and publish course credit criteria (see Annex A) per Cyber School course, module, unit, or block to advise Cyber Corps personnel during the course credit application process on applying equivalent credit.

(3) Evaluate all Cyber course credit packets according to the applicable courseware on a “by course or module” basis for constructive, equivalent, and/or operational credit. For documented Task Force Echo and Cyber Warfare Company service, course credit will be evaluated and awarded as documented in Annex I.

(4) If full course credit is awarded for MOS/AOC-producing courses that require a DA Form 1059 AER, CTED will generate the DA Form 1059 IAW AR 623-3 and DA PAM 623-3 for submittal to HRC through Army Training Requirements and Resources System (ATRRS) or by email, as appropriate.

(5) Support the Cyber CCRB, generally held monthly but not less than quarterly, with at least one subject matter expert board member for each course or module being considered, and with no less than three voting board members total. Board members will be appointed by the CTED Director, with names provided to the OCC Cyber Course Credit Program Manager NLT one week prior to the board convening.

(6) Provide Virtual Hacking Lab (VHL) and Pen-Testing With Kali (PWK) vouchers for students enrolled through ATRRS. Soldiers not enrolled in Phase 3 of Cyber Operations Officers Course (CyOOC) or Cyber Basic Officer Leader Course (CyBOLC) must receive funding for vouchers through their command.

8. Eligibility.

a. All applicants must be current members of the Cyber Career Field (i.e. already assessed and selected into the Cyber Corps) in any component of the U.S. Army. This SOP is not a branch transfer or reclassification mechanism for officers, warrant officers, or enlisted personnel to bypass the regular transfer process for the Army and Cyber Career Field. In some cases, it may be used to award course credit to select personnel in other military service branches.

(1) Only Warrant Officers who have successfully completed a WOBC or Commissioned Officers who completed any BOLC and have been approved to transition to Warrant Officer are eligible to request WOBC equivalency. WOBC is a requirement for the commissioning of Warrant Officers and must be completed by all Warrant Officers who have not completed any WOBC or BOLC.

(2) An applicant may not receive course credit if doing so would result in initial military training of less than 12 weeks for all Army personnel as outlined in AR 350-1.

b. At the time of application, individuals must meet all MOS or AOC requirements outlined in DA PAM 611-21, including but not limited to security clearance level, height, weight, and medical readiness.

9. Application Procedures. Complete a Cyber Course Credit Program packet as outlined below and in Annex C. A complete application must be submitted for each board (e.g., if a Soldier applied during a previous board cycle, they must submit a new packet to be considered at another board) no later than one week prior to the board convening date.

a. Applicant course credit packets must include the following:

(1) DA Form 4187 signed by the applicant and their commander, when necessary. The Commander should select “Recommend Approval” in block 11.

(2) Completed Cyber Course Credit Program memorandum to the Commandant/Chief of Cyber detailing relevant training, education, or experience for constructive, equivalent, and/or operational credit. The memorandum must be THRU their higher headquarters and signed by the THRU authority IAW AR 25-50. Applicant will include the applicable table from Annex B, Course Credit Worksheets, in their memorandum to designate what education and experience they are allocating to which

module of training. The memorandum should specify which type(s) of course credit (constructive, equivalent, and/or operational) is/are being requested.

(3) Current/valid DA 705 Army Physical Fitness Test and DA 5500 (male) or DA 5501 (female), if applicable, which shows the applicant is compliant with Army physical readiness and height/weight requirements.

(4) Copy of Records Brief (ORB, ERB, or SRB).

(5) DA 67-9, Officer Evaluation Report, or DA 2166-8, NCO Evaluation Report, for all time periods the applicant is requesting operational credit. Service members may submit civilian evaluation reports if they are relevant for operational credit.

b. Applicant packets may include the following, if these documents provide evidence of constructive, equivalent, and/or operational credit:

(1) College transcripts

(2) Course completion certificates

(3) Industry certifications

(4) National Cryptologic School transcripts

(5) Approved U.S. Cyber Command Individual Training Equivalency Board results/reports

(6) DA 1059 Academic Evaluation Reports

(7) Letters of recommendation

(8) Memoranda from supervisors detailing cyber exercise participation

(9) Samples of non-proprietary, unclassified code written by the applicant

c. Applicants who are requesting course credit as part of a Reclassification or branch transfer packet must submit a separate complete Cyber Course Credit Program packet, as detailed above, in conjunction with their reclassification/transfer packet. Submit the CCRB packet separately from the reclassification packet to the email listed above.

d. Appeals and Resubmissions.

(1) If an applicant feels the determination of the Cyber CCRB is inaccurate or incomplete, the applicant may submit a Memorandum for Record to the Commandant,

U.S. Army Cyber School through OCC detailing what they believe is inaccurate or incomplete, and also add amplifying information to justify their appeal.

(2) Appeals are handled on a case by case basis, and all appeal decisions are final with no subsequent appeals authorized.

(3) If a packet is returned without action or if the Board requires amplifying information, the requester may resubmit a new packet for the next board.

10. Suggested Improvements. Users of this SOP are invited to send comments and suggestions to the points of contact listed below.

11. The publication of this SOP supersedes all previous Cyber Course Credit Program SOPs as of the signature date.

12. Points of Contact for Packet Submission.

a. Officer Division: usarmy.gordon.cyber-coe.mbx.occ-officers@mail.mil

b. Warrant Officer Division: usarmy.gordon.cyber-coe.mbx.occ-wo@mail.mil

c. Enlisted Division: usarmy.gordon.cyber-coe.mbx.occ-enlisted@mail.mil

CRAFT.PAUL.GRANT.1074760534 Digitally signed by CRAFT.PAUL.GRANT.1074760534 Date: 2021.01.28 16:20:02 -05'00'

PAUL G. CRAFT
Brigadier General, U.S. Army
Commandant

Attachments:
Annex A: Course Credit Criteria
Annex B: Course Credit Worksheets
Annex C: Course Credit Example Packet
Annex D: Sample COPC MFR TFE
Annex E: Sample CsRA MFR TFE
Annex F: Example Waiver Request – PWK for CsRA
Annex G: Example Waiver Request – VHL for JACWC
Annex H: Example Waiver Request – PWK for JACWC
Annex I: TFE_CCOE Crosswalk, dated 12 Dec 20