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

ATSR-PO 21 November 2023

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 (TASS), dated 1 May 2018

c. DA Pamphlet 600-3, Officer Professional Development and Career Management, dated 14 April 2023

d. DA Pamphlet 600-25, U.S. Army Noncommissioned Officer Professional Development Guide, dated 11 September 2023

e. DA Pamphlet 611-21, Military Occupational Classification and Structure, dated 20 December 2022

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 received, processed, evaluated, and completed. Additionally, it defines criteria for eligible personnel to request credit for courses for which the U.S. Army Cyber School is the proponent.

3. Applicability.

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

b. U.S. Army Cyber Corps officers, warrant officers, and enlisted personnel in all Components, as well as personnel from other branches of service (e.g., USN, USMC, USAF, etc.), 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 Force training or qualification credit to meet initial or full operational capability requirements nor job qualification requirements and standards. This program solely applies to credit for courses for which the U.S. Army Cyber School is the proponent, primarily including Cyber Corps MOS/AOC producing courses.

d. Partial course credit granted under this program may be revoked by the Cyber School Commandant/Chief of Cyber when changes are made to relevant course curriculum or Cyber career field MOS/AOCs. Cyber course credit revocation may also occur for other reasons deemed appropriate by the Commandant/Chief of Cyber. Full course credit granted prior to course curriculum or career field changes will generally be honored, particularly since it will likely already be documented in personnel records.

4. Objective. The Cyber Course Credit Program evaluates Cyber Corps officer, warrant officer, and enlisted personnel packet submissions, as well as those from other branches of service for credit for select Cyber School courses to avoid duplication of training and allow minimal disruption to the operational force under prescribed circumstances. The intent of the Commandant/Chief of Cyber in providing a course credit program is to satisfy the operational needs of the Army for qualified Cyber professionals while ensuring standardized knowledge, skills, and abilities within the entirety of the force. The Cyber Course Credit Program will primarily be used to ensure training standards are achieved for Cyber MOSs and AOCs. Receiving course credit (full or partial) through this program in lieu of fulfilling course requirements is the exception and not the rule.

5. General.

a. The Cyber School Commandant/Chief of Cyber awards course credit only for specified Cyber School governed courses and modules through this program. The Commandant/Chief of Cyber delegates management of the Cyber Course Credit Program to the Director, Office Chief of Cyber (OCC), and the validation, verification, and adjudication of course credit criteria to the Director, Cyber Training and Education Directorate (CTED). Full or partial course credit may be awarded to Cyber Corps Soldiers toward MOS/AOC qualification for select courses. The standard by which packets are evaluated is the program of instruction and learning objectives of the relevant Cyber School MOS/AOC producing courses and/or functional courses. Per regulatory references, course credit for all common core modules must be granted by Director of Training, U.S. Army Training and Doctrine Command (TRADOC) G-37, and as such, is not governed by this SOP.

b. Course credit for Cyber School governed training and education may be awarded using a combination of constructive, equivalent, and/or operational credit IAW AR 350-1 and Annex A of this SOP.

(1) Cyber School may grant constructive credit to individuals in lieu of course attendance based on previous leadership experience and/or past academic/training

experiences. 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) Equivalent credit may be granted to individuals in lieu of course attendance based on courses possessing comparable terminal learning objectives/learning outcomes. Terminal learning objective/outcome assessments are performed by TRADOC or the respective proponent school. Individuals must possess the same skills and qualifications as course graduates.

(3) Operational credit may be granted to individuals in lieu of course attendance based on operational experiences.

6. Cyber Course Credit Review Board (CCRB).

a. The Cyber School will convene the Cyber CCRB, generally monthly but not less than quarterly, to review applicant packets for Cyber course credit consideration. The board is facilitated by the OCC Cyber Course Credit Program Manager with voting board members consisting of designated representatives from CTED (e.g., College Directors, Course Managers, Senior Instructors, etc.).

b. To conduct a valid CCRB, a minimum of one subject matter expert for each Cyber School course or module for which credit is requested must be present and serving as a voting board member, with no less than three voting board members present; one member may be the expert for more than one course.

c. All CCRBs are considered closed boards due to Personally Identifiable Information concerns and to ensure the integrity of the proceedings. Visitors seeking to observe a board must request in writing with valid justification at least one week prior to the board convening and be approved by the Director, OCC.

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 in the service member's personnel records, proof of acceptance into the Cyber Corps 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 and course for which credit is being requested. See Annexes B and C for the packet worksheet and DA Form 4187 example.

(3) Submit completed packet to OCC no later than one week prior to the next CCRB convening date (which is typically the third Friday of every month, meaning packets would be due on the second Friday of the month). If applicants need to submit classified documentation, contact the appropriate POC to obtain a SIPR or JWICS email address.

(4) Receive course credit determination from OCC following the conclusion of the CCRB, and if approved for course credit, coordinate with the appropriate agency or department (i.e., HRC, S1/G1, S3/G3) to schedule required training and/or update personnel records.

(5) Applicants who are submitting for course credit in conjunction with MOS reclassification or branch transfer must first receive a favorable determination through that process and then submit a separate course credit packet for review. Personnel should not submit their reclassification packet into the CCRB process; only submit documents relevant to receiving course credit.

(6) Following approval of Cyber course credit, all applicants must still attend their entire course unless receiving full course credit from the CCRB. In the case of phased courses, all applicants must attend each phase unless receiving full credit for an entire phase from the CCRB. All personnel receiving partial course credit (or partial credit for a phase) are required to submit an alternate study plan (ASP) for the modules for which they have approved course credit at least two weeks prior to the start of the module. Without an approved ASP, the individual must be present for class even if granted course credit. The ASP approval must be granted by the course manager in coordination with the appropriate commander within the 401st Cyber Battalion.

(7) Task Force Echo (TFE) applicants only: For applicants to receive course credit for the Cyberspace Response Assessment (CsRA), TFE applicants must submit signed memorandum for record (MFR) from the 91st Cyber Brigade Commander attesting to their completion of each terminal learning objective, enabling learning objective, and learning support activities. See Annex D.

b. OCC will:

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

(2) Facilitate the monthly Cyber CCRB consisting of designated CTED representatives appointed by the CTED Director to adjudicate course credit approval / disapproval determinations. The Cyber CCRB will generally be held monthly on the third Friday, but not less than once per quarter.

(3) Generate approval/disapproval determination memorandum, which are signed by the OCC Director. In the absence of the OCC Director, the determination memorandum may be signed by the CTED Director.

(4) Provide applicant with course credit approval/disapproval memorandum, listing which modules or courses for which credit is awarded. 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 applicants, or directly to the applicants.

(5) Maintain and revise the SOP when programmatic changes occur. The OCC Director, as the authorized delegate of the Commandant/Chief of Cyber is the signatory for this SOP.

(6) Publish the SOP updates on the Cyber Course Credit Program milSuite site: https://www.milsuite.mil/book/docs/DOC-748306. While Cyber School may publish the SOP and its annexes elsewhere, this is the primary online repository and information source.

c. CTED will:

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

(2) Develop and publish course credit criteria (Annex A) per Cyber School course/module to inform the course credit application process and the Cyber CCRB.

(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 TFE and Cyber Warfare Company service, course credit will be evaluated using the crosswalk provided in Annex E.

(4) 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 a total of three voting board members. 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.

(5) CTED Course Managers in coordination with commanders within the 401st Cyber Battalion grant approval/disapproval of ASPs, as necessary.

8. Eligibility.

a. All applicants must be current members of the Cyber Career Field 17 (i.e., already assessed and selected into 17-series Cyber Corps career field) in any Component of the 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 personnel in other military service branches.

b. An applicant may not receive course credit if doing so will result in initial military training (IMT) of less than the minimum training time required by applicable laws, regulations, or policies. For instance, AR 350-1, Section III, Paragraph 3-27a states: “In accordance with 10 USC 671, a Soldier may not be assigned to active duty on land outside the United States and its territories and possessions until the Soldier has completed IMT within the Army. In time of war or a national emergency declared by Congress or the President, the period of required IMT may not be less than 12 weeks.”

c. At the time of application, individuals must meet all Cyber Corps MOS or AOC requirements outlined in DA PAM 611-21, including but not limited to security clearance level, height, weight, and medical readiness. Applicants will provide verification of meeting these requirements as part of their application packet as outlined in this SOP and its annexes.

d. Eligibility by cohort (see Annex A for more details):

(1) Enlisted Soldiers. MOS 17C or 17E Advanced Individual Training (AIT) course credit is only available to 17C or 17E MOS-T (reclassification) Soldiers; MOS-I (IET) Soldiers are not eligible to apply. Also, no course credit may be awarded for the 17C or 17E Advanced Leaders Courses and Senior Leaders Courses.

(2) Warrant Officers. Credit may be awarded for the CCTC module of 170A Warrant Officer Basic Course (WOBC) if the applicant has previously completed CCTC; no other credit may be awarded for 170A WOBC. Additionally, no credit may be awarded for the following Cyber warrant officer courses: 170A Warrant Officer Advanced Course (WOAC), 170B WOBC, 170B WOAC, and 170D WOAC. For 170D WOBC, a separate process exists for requesting technical equivalency outside of the program governed by this SOP, as follows:

(a) If the warrant officer holds current Army qualification as a basic developer or higher, a request for technical equivalency for the technical modules of 170D WOBC may be sent to CTED. The warrant officer must send copies of their Army developer qualification memorandum and signed JQR document to the 170D Course Manager. If validated, the course manager drafts a memorandum for technical equivalency and sends it to the Department of the Army (DA) G-3/5/7 for approval.

(b) If approved, the 170D Course Manager drafts an early graduation memorandum and sends to Cyber School Commandant for approval, along with the DA G-3/5/7 approval memorandum. Upon Commandant approval, the course manager sends the memorandums to the 170D Career Manager at HRC to amend the warrant officer’s orders for 170D WOBC. At that point, the warrant officer will only be required to attend the 170D WOBC common core modules and may receive TDY orders instead of PCS orders, depending on their next assignment.

(3) Officers. The Cyber officer courses available for credit are 17A Cyber Warfare Officer Course (previously, Cyber Operations Officer Course), 17B Cyber

Electromagnetic Warfare Officer Course (previously, Cyber Electromagnetic Operations Officer Course), and 17D Basic Officer Leaders Course (BOLC). For 17D BOLC, credit may only be awarded for the technical modules for prior service Soldiers who hold current Army basic developer qualification or higher. Officer courses not eligible for course credit are the 17A BOLC, 17A/B Captains Career Course (CCC), and 17D CCC.

9. Application Procedures. Complete a Cyber Course Credit Program packet as outlined in this SOP and its annexes. 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 for consideration at another board) no later than a week prior to the board.

a. Applicant course credit packets must include the following items:

(1) DA Form 4187 signed by the applicant and their commander. The commander should select "Recommend Approval" or "Recommend Disapproval" in block 11; provide name and rank in block 12; and sign/date in blocks 13-14.

(2) Completed Course Credit Worksheet: one per course required, signed by the applicant, detailing the modules for which credit is requested and the supporting documentation provided to verify/validate course credit.

(3) Current/valid DA Form 705-TEST, Army Combat Fitness Test Scorecard, along with DA Form 5500, Body Fat Content Worksheet (Male), or DA Form 5501, Body Fat Content Worksheet (Female), as applicable, to verify the applicant is compliant with Army physical readiness and height/weight requirements.

(4) Copy of current Soldier Talent Profile or similar personnel record documenting status as a Cyber Corps 17-series officer, warrant officer, or enlisted Soldier. If not yet documented on the Soldier Record Brief, valid proof of acceptance into the Cyber Branch must be included in the packet to determine eligibility.

b. Applicant packets may also include one or more of the following items, particularly those documents which provide evidence for constructive, equivalent, or operational course credit validation:

(1) College/university transcripts with relevant coursework highlighted/annotated. Include copies of course syllabi and/or other materials that show what was covered in the course since college courses vary widely in their coverage. The submission must clearly demonstrate how the college course covered the terminal learning objectives/learning objectives for each course/module for which credit is sought.

(2) Officer Evaluation Report(s) or NCO Evaluation Report(s) for all time periods the applicant is requesting operational credit. In limited cases, civilian evaluation reports may be considered if they are detailed and relevant for operational credit.

(3) DA Form 1059, Academic Evaluation Reports

(4) National Cryptologic School transcript with relevant coursework highlighted

(5) Training course completion certificates/documents

(6) Industry certification documents

(7) Recent sample of non-proprietary, unclassified programming work performed by the applicant and verified by the supervisor

(8) Army Basic Developer (or higher) qualification document

(9) Memorandum for Record from the commander detailing specific operational experience to be considered for course credit validation

c. Applicants who are requesting course credit as part of an MOS reclassification or branch transfer packet must submit a separate complete Cyber Course Credit Program packet, as detailed 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 (using the below listed mailbox) detailing what they believe is inaccurate or incomplete and 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 available board.

10. Suggested Improvements. Users of this SOP are invited to send feedback or suggestions for improvement to the below listed mailbox.

11. For programmatic or process related questions or concerns, contact the Program Manager using the below listed mailbox.

12. The mailbox for all unclassified packet submissions is: usarmy.eisenhower.cyber-coe.mbx.cyber-course-credit-packets@army.mil. The title of the email subject line should read: “CCRB Packet – [applicants rank and name].”

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

BOVA.SHAWN.DALLAS.1026973712
Digitally signed by BOVA.SHAWN.DALLAS.1026973712
Date: 2023.11.21 13:28:58 -05'00'

SHAWN D. BOVA
Director, Office Chief of Cyber

5 Encls
Annex A: Course Credit Criteria
Annex B: Course Credit Worksheet
Annex C: Example DA Form 4187
Annex D: Sample CsRA MFR for TFE
Annex E: TFE to CyS Crosswalk