MILPER Message Number
24-420

Proponent
AHRC-EPF-R

Title
Fiscal Year (FY) 25 Reserve Component Branch Transfer Procedures for AOC 170A (Cyber Warfare Technician)

_____

A. AR 600-9, The Army Body Composition Program, 28 Jun 19 13.B. AR 621-1, Training of Military Personnel at Civilian Institutions, 08 May 24.

B. DA PAM 611-21 (Military Occupational Classification and Structure), 20 Dec 22

C. DA PAM 611-21 Notification of Future Change (NOFC), O-1710-16, W-1710-04.

D. AR 600-20, Army Command Policy, 24 Jul 20.

E. Department of the Army Pamphlet (DA PAM) 600-3, Officer Talent Management, 14 Apr 23.

1. This message is effective upon release and will expire no later than 30 September 2025.

2. The United States Army Reserve (USAR) and Army National Guard (ARNG) are seeking qualified Warrant Officer(s) (WO) to become Cyber Warfare Technicians (170A). A Cyber Warfare Technician performs as the Subject Matter Expert and advisor to the Commander and staff regarding the employment of Offensive and Defensive cyber operations assets and personnel. Directs, plans, administers, manages, integrates, and assesses cyberspace technical capabilities. Provides technical recommendations and guidance regarding the operation and management of Army, Joint, intergovernmental, interagency, and multi-national cyberspace assets, and personnel. Integrates cyberspace capabilities into warfighting functions to optimize combat effectiveness. Defends the Department of Defense Information Network against foreign and domestic threat vectors to maintain network integrity and functionality. Maneuvers through the Cyber Domain to impose costs on adversarial threats both Offensively and Defensively. Leads, trains, and mentor's Cyber personnel through

individual and group instruction, as well as the establishment, direction, and evaluation of Joint Qualification Requirements (JQRs), Joint Qualification Standards (JQSs), and Joint Cyberspace Training and Certification Standards (JCT&CS).

3. This message applies to all United States Army Reserve (USAR) and Army National Guard (ARNG) Warrant Officers (Active Guard Reserve (AGR) and Troop Program Unit (TPU)).

(a) Individual Mobilization Augmentation (IMA) and Individual Ready Reserve (IRR) Servicemembers need to contact HRC for reclassification opportunities and position slotting before submitting a packet: (https://www.hrc.army.mil/content/Reserve%20Component%20Command%20Managem ent or usarmy.knox.hrc.mbx.rpmd-usar-cmd-mgmt@army.mil). ARNG IMA & IRR need to contact their State Warrant Officer Strength Manager (WOSM) for branch transfer opportunities and position slotting before submitting a packet.

(b) Active Component (AC) Servicemembers who are interested in transferring to USAR or ARNG Cyber ranks may participate in 170A branch transfer panels. AC WOs who are within a three-year window of their Mandatory Removal Date (MRD) are ineligible. For the ARNG, the AC Servicemember must be in contact with their State WOSM. For the USAR, the AC Servicemember must contact their local USAR unit Career Counselor (79V): https://www.usar.army.mil/ARCG/ARCG-Units/.

4. The Office Chief of Cyber (OCC) is accepting voluntary branch transfer requests into Area of Concentration (AOC) 170A from WOs meeting the prerequisites for the Cyber Branch. The dates of the FY25 Branch Transfer Eligibility Panels are:

(a) 170A Branch Transfer Panel #1
07 Oct 24 – 24 Jan 25: window to submit applications.
27 – 31 Jan 25: panel convenes.
07 Feb 25: results released (tentative).

(b) 170A Branch Transfer Panel #2
06 Jan 25 – 09 May 25: window to submit applications.
12 – 16 May 25: panel convenes.
22 May 25: results released (tentative).

4. Eligibility: To participate in the 170A Branch Transfer Eligibility Panel applicants must meet the following criteria:

a. Must be a U.S. Citizen.

b. Must be a Warrant Officer in the grade of Warrant Officer-2 (WO2) – Chief Warrant Officer-4 (CW4).

d. Must meet the physical demand standards per AR 40-501, Chapter 2 and DA PAM 611-21. All Soldiers must meet the Army Height and Weight Standards per AR 600-9. If applicable, a DA Form 5500/5501 must be submitted.

e. Request for waivers must be included in the application packet.

5. Warrant Officers who are not eligible include:

a. Warrant Officers controlled by the Judge Adjutant General's Corps, Chaplain Corps, AMEDD, or Medical Service Corps are not eligible for this program. Warrant Officers in these categories should contact their respective Warrant Officer/Career Manager for information regarding the branch transfer process.

b. Warrant Officers who have received or are pending unfavorable action are not eligible for this program. Unfavorable actions include but are not limited to the following: receiving or having been found guilty under any form of Uniform Code Military Justice as an Officer/Warrant Officer, receiving a General Officer letter or memorandum of reprimand, being selected for a separation board, or failing to meet Army Physical Fitness or Army Body Composition Standards in accordance with AR 600-9.

c. Warrant Officers who have received a Referred Officer Evaluation Report (OER) or Referred Academic Evaluation Report (AER) are ineligible.

d. Warrant Officers who are within a three-year window of their Mandatory Removal Date (MRD) are ineligible.

6. Applicants requesting to the Cyber Branch must adhere to the following qualifications:

a. Must obtain and maintain a TOP SECRET (TS) clearance. A favorable special background investigation (SBI) with eligibility for access to sensitive compartmented

information (SCI) is required. Selectees must initiate procedures to obtain proper level of clearance immediately upon initial notification of eligibility for the MOS 170A designation.

b. Must be able to successfully pass a counterintelligence (CI) scope polygraph based on specific unit assignment requirements.

c. Cyber community of interest training and experience should be documented as part of the Cyber questionnaire and should include specific work role qualification, a description of cyber work utilization, and cortication records. Cyber experience, by itself, is helpful but not required. Programming and software development experience are not required, but are preferred, and should be specifically highlighted in the Cyber questionnaire. The Cyber questionnaire must be requested by contacting the Office Chief of Cyber Reserve Component Division (usarmy.eisenhower.cyber-coe.mbx.rcao-cyber@army.mil)

d. Relevant education includes Computer Science/Engineering/Information Systems; Electrical Engineering; Mechanical Engineering; Cyber Security/Ops; Systems Engineering; Data Science; Mathematics; Physics; Chemistry; Information Technology/Systems/Security.

e. The panel will consider the applicant's strength and technical expertise and/or significant cyber-related accomplishments; significant operational experience derived from diverse backgrounds or educational paths indicative of creativity, intellectual curiosity, problem solving, and/or academic excellence. Common to all grades is a deep interest in and passion for the cyber domain, propensity for self-development and improvement, and proven ability to work as a contributing team leader or a team member.

f. AGR Warrant Officers electing to participate in the proponent branch transfer panel must first apply for consideration and be accepted by proponent before submitting an AGR Branch Transfer request via HRC Voluntary Transfer Incentive Program (VTIP) procedure. Upon acceptance, HRC will process VTIP packet review. ARNG AGR Warrant Officers should contact their State WOSM.

7. Application procedures: The guidelines for all applicants are listed at https://www.milsuite.mil/book/community/spaces/army-cyber-net/cyber-regiment/reserve-component. Letters to the president of the panel can be included if needed to address concerns within the application.

a. All applicants must understand and meet requirements for Cyber Warrant Officer Standards outlined in DA PAM 611-21 and DA PAM 600-25: (https://www.milsuite.mil/book/groups/smartbookdapam611-21) (https://www.milsuite.mil/book/docs/DOC-915605). Waiver requests for DA PAM 611-21 requirements must be included in the application packet.

b. Applicants must submit their branch transfer packet in a single Adobe .pdf file. Packets created with embedded attachments or as a portfolio will not be accepted and will be returned for corrections. Submissions must be in the order of the checklist provided at the location referenced in paragraph 7. Applications will not be accepted in any other format.

c. ARNG WOs will submit the application packet to their State WOSM for review. State WOSM will send packets to ARNG Multi-Domain Activities Division (ARNG-MDAD): ng.ncr.ngb-arng.list.cyber@army.mil. ARNG-MDAD will review all packets, consolidate and forward to the Cyber Proponent for adjudication. Packets submitted directly by applicants will not be accepted for consideration.

b. USAR WOs will submit the application packet to their unit / command for review. Commands will contact the Army Reserve Cyber Protection Brigade (ARCPB) for packet review and possible position placement (usarmy.usarc.arcpb.mbx.npe-s3-cmd@army.mil). ARCPB will review all packets, consolidate and forward to the Cyber Proponent for adjudication. Packets submitted directly by applicants will not be accepted for consideration.

8. Based on performance and technical review, applicants will receive an eligibility status in one of the following criteria:

a. Eligible for branch transfer. Warrant Officers must initiate procedures to obtain a TS/SCI clearance immediately upon notification eligibility for 170A AOC; must obtain and maintain a TOP SECRET (TS) clearance. A favorable special background investigation (SBI) with eligibility for access to sensitive compartmented information (SCI) is required.

b. Eligible for branch transfer with additional caveats. The panel results will state the required administrative or training requirement needed to obtain the Cyber Branch designation. Once the applicant meets the stated caveats, which may include an individual training plan, the applicant must re-submit a new signed DA Form 4187 with

the original qualification memo and proof of training or certification that meets the stated caveats. If all caveats have been met, the Office Chief of Cyber will generate a new eligibility status memo stating the applicant is eligible to be awarded the 170A AOC.

c. Commands will process the documentation through appropriate channels for the award of 170A AOC. Applicants who are unable to complete the required training or obtain the appropriate clearance will be involuntarily returned to the previous branch.

9. Warrant Officers approved for transfer will:

a. Receive a memorandum of selection from the Office Chief of Cyber outlining the transfer eligibility determination and any additional professional military education (PME) requirements.

(1) Warrant Officers who require training but are unable to complete the required training within 36 months may submit an Exception to Policy Memorandum to the Cyber Proponent justifying reason for additional time needed for required training.

b. Be considered for immediate assignment into a unit that has a corresponding Cyber (170A) billet.

c. Have the option to accept or decline their transfer. Warrant Officers electing to decline transfer will remain in their current branch and must wait one year before submitting another request.

d. Be required to accept or decline their transfer by replying through their command NLT 30 working days from notification.

10. Warrant Officers with questions concerning branch transfer opportunities should contact their Senior Warrant / WOSM or access the Cyber Reserve Component milSuite: https://www.milsuite.mil/book/community/spaces/army-cyber-net/cyber-regiment/reserve-component.

11. Address questions or concerns about the Cyber Branch Transfer process to:

a. Army National Guard Cyber Division at: ng.ncr.ngb-arng.list.cyber@army.mil

b. ARCPB BDE S3: usarmy.usarc.arcpb.mesg.bde-s3@army.mil

c. ARCPB BDE S1: usarmy.usarc.arcpb.mesg.bde-s1@army.mil

d. The Office Chief of Cyber, Reserve Component Division (Cyber Proponent): usarmy.eisenhower.cyber-coe.mbx.rcao-cyber@army.mil