

MILPER Number: 26-384

**Proponent
AHRC-EPF-R**

**Title
Fiscal Year (FY) 27 Reserve Components Reclassification Procedures for MOS 170A
(Cyber Warfare Technician)**

...Issued:[08 Oct 2026]...

-
- A. Army Regulation (AR) 600-9, The Army Body Composition Program, 16 Jul 19.
 - B. Department of the Army Pamphlet (DA PAM) 611-21 (Military Occupational Classification and Structure), 20 Dec 22 (RAR 6 Dec 2019).
 - C. DA PAM 611-21 Notification of Future Change (NOFC), O-1710-16, W-1710-04.
 - D. AR 600-20, Army Command Policy, 15 Apr 26.
 - E. DA PAM 600-3, Officer Talent Management, 19 Feb 25.
 - F. National Guard Regulation (NGR) 600-100 (Officer Federal Recognition and Related Personnel Actions), 22 Nov 22.
 - G. National Guard Regulation (NGR) 600-101 (Warrant Officer Federal Recognition and Related Personnel Actions), 27 Apr 26.
 - H. USAR G1 Personnel Action Guide (PAG) T-2-O-1 Request for Reclassification/Branch Transfer (Non-Army Medical Department (AMEDD))
1. This message is effective upon release and will expire no later than 30 September 2027.
 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 War 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 Job Qualification Record (JQRs), Joint Qualification Standards (JQSs), and Job 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), Mobilization Day (M-Day), 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/Individual%20Ready%20Reserve%20\(IRR\)%20Homepage](https://www.hrc.army.mil/content/Individual%20Ready%20Reserve%20(IRR)%20Homepage) or usarmy.knox.hrc.mbx.rpmd-ima-irr-branch@army.mil). ARNG IMA, and IRR need to contact their State Office of Personnel Management (OPM) for reclassification 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 reclassification 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 reclassification requests into MOS 170A from WOs meeting the prerequisites for the Cyber Branch. The dates of the FY27 reclassification eligibility panels are:

170A Reclassification Panel

04 Jan 27 – 31 Mar 27: window to submit applications.

19 Apr 27 – 23 Apr 27: panel convenes.

14 May 27: results released (tentative).

5. Eligibility: To participate in the 170A reclassification eligibility panel applicants must meet the following criteria:

- a. Must be a U.S. Citizen.
- b. Must not be a dual citizen of any foreign country.
- c. Must be a Warrant Officer in the grade of Chief Warrant Officer-2 (CW2) – Chief Warrant Officer-4 (CW4).
- d. (ARNG Only) Must have a Letter of Recommendation from their State Command Chief Warrant Officer (CCWO).
- e. (USAR Only) For Warrant Officer reclassification requests, Warrant Officers should coordinate with their career manager or Army Reserve Proponent Adviser (ARPA) for assistance with gaining/losing branch proponent for approval. Memorandum for record must be included in packet with explicit approval/concurrence for reclassification from losing career manager or ARPA.
- f. Must meet the physical demand standards per AR 40-501, Chapter 2 and DA PAM 611-21. All Soldiers must meet the Army Waist-to-Height ratio standards per AR 600-9 and AD 2026-13. If applicable, a DA Form 5500 must be submitted.
- g. Personnel with immediate family members who are citizens, dual citizens, or reside in a country on the U.S. Army High-Risk Country List, maintained by HQDA G-2, are ineligible for service as a Cyber Warrant Officer. Immediate family members include parents, stepparents, spouse, children, stepchildren, siblings, stepsiblings, cohabitants, only living blood relatives, and persons in loco parentis, per AR 600-8-10.
- h. Must ensure the required Soldier Talent Profile (STP) checklist is redacted of sex, race, and photos, or the packet will be returned.
- i. Request for waivers must be included in the application packet.

6. Warrant Officers who are not eligible include:

- a. Warrant Officers controlled by the Judge Advocate 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 reclassification 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 of 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 of current ABCP standards.
 - 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.
7. Applicants requesting reclassification 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. Must submit all supporting documentation pertaining to relevant Cyber experience, including NCOERs demonstrating performance as a 17C, Cyber-related Job Qualification Record (JQR) memos, and records of completed Cyber missions at the unclassified level.
 - d. 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 certification 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.gordon.cyber-coe.mbx.rcao-cyber@army.mil). Experience in roles such as helpdesk

operations, desktop support, cable installation, and similar support functions do not qualify as Cyber experience.

e. 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.

f. 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.

g. Participation in key exercises such as Cyber Shield, Cyber Fortress, Cyber Yankee, and others shows Cyber-related experience. Applicant must show active participation through official documentation such as certificate of participation, memo signed by Commander, orders, etc. Visiting or observing is not considered participation.

h. USAR AGR Warrant Officers electing to participate in the proponent reclassification panel must first apply for consideration and be accepted by proponent before submitting an AGR reclassification request via HRC Voluntary Transfer Incentive Program (VTIP) procedure. Upon acceptance, HRC will process VTIP packet review. T32 ARNG AGR Warrant Officers should contact their State OPM. T10 ARNG AGR Warrant Officers should contact TARC-HQ.

i. A Cyber Proponent 17A or 17C acceptance memo alone does not qualify Soldiers for the 17-Series or 170A Cyber Warrant Officer position. Applicants must provide proof of current 17C qualification or completion of 17A or 17C course credit with their 170A Pre-Determination Packet submission.

8. Application procedures: The guidelines for all applicants are listed at <https://armyeitaas.sharepoint-mil.us/:u:/r/sites/TR-CCoE-CYBERSCHL/SitePages/Cyber%20RC%20Division.aspx>. A memorandum of record 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.army.mil/G-1#org-g-1-resources> or <https://armyeitaas.sharepoint-mil.us/teams/usar-g1-pag/Lists/ActionsList/USARG1PAG.aspx>. Waiver requests for DA PAM 611-21 requirements must be included in the application packet.

- b. Applicants must submit their reclassification 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 SharePoint referenced in paragraph 8. Applications will not be accepted in any other format.
 - c. ARNG WOs must submit the application packet to their State WOSM for review. State WOSM will send packets to Army National Guard Strategic Operations (ARNG-SO) Division at: ng.va.ngb.mbx.arng-warrant-officer-170x-branch-transfer-requests@army.mil. ARNG-SO will review (QA/QC) all packets, consolidate and forward to the Cyber Proponent for adjudication. Packets submitted directly by applicants will not be accepted for consideration.
 - d. USAR WOs will submit the application packet to their unit / command for review. Commands will forward all eligible and complete packets to Reserve Component Division, Office Chief of Cyber (usarmy.gordon.cyber-coe.mbx.rcao-cyber@army.mil). RC will coordinate with Cyber Protection Brigade (ARCPB) for packet review and possible position placement (usarmy.usarc.arcpb.mbx.npe-s3-cmd@army.mil). Packets must be submitted through unit S-1, Commanders, or Commander's Designee. Packets submitted directly by applicants will not be accepted for consideration.
9. Based on performance and technical review, applicants will receive an eligibility status in one of the following categories:
- a. Eligible for reclassification. Warrant Officers will be informed of formal training required for MOS Designation. Warrant Officers must maintain a TS/Sensitive Compartmented Information (SCI) clearance immediately upon notification of MOS designation.
 - b. Eligible for reclassification with additional caveats. The panel results will state the required administrative or training requirement needed to obtain the Cyber Branch designation. Those who do not have a TS/SCI must obtain and maintain a TOP SECRET (TS) clearance before MOS designation. A favorable special background investigation (SBI) with eligibility for access to SCI is required. Once the applicant meets the stated caveats, and has completed formal training, they may be granted the MOS designation.
 - c. Not eligible for reclassification. Warrant Officers will be provided with panel recommendations for future submissions. Applicants may apply no earlier than (NET) 12 months from the date of published results.

d. Fully Qualified Not Selected (FQNS). Warrant Officers deemed qualified for the cyber branch but not selected due to Component authorized overstrength or insufficient cyber school quotas. Applicants may request to be reconsidered at next available 170A reclassification panel. Applicants who are FQNS do not need to resubmit a new packet unless there have been significant changes to submitted documents. Applicants are encouraged to reach out to RC Division, OCC, to inquire if any changes meet the “significant” threshold.

e. The accepted applicant can choose to submit to have a portion of the course waived based on previous training and experience by submitting a course credit review board packet to the Cyber Training, Education Directorate (CTED) (usarmy.gordon.cyber-coe.mbx.cyber-course-credit-packets@army.mil) who will review to determine eligibility training requirements and award constructive and equivalent credit.

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

10. 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. All Determination of Eligibility acceptance memos will state that the applicant is technically qualified to transfer into the MOS 170A, Cyber Warfare Technician, and is required to attend the 170A Cyber Warfare Technician Warrant Officer Basic Course (WOBC).

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.

11. (ARNG ONLY) Warrant Officers selected must complete all required training and be granted designated MOS NLT 18 months from published results.

12. (USAR ONLY) This eligibility to transfer will expire 18 months from the date of assignment to the Army Reserve Cyber Protection Brigade (ARCPB) or a cyber para/ln outside of ARCPB if transfer action is not completed. Warrant Officers listed as eligible to reclassify have 6 months from the date of their approval memorandum to execute a unit transfer to ARCPB or a cyber para/ln. Failure to do so may nullify reclassification eligibility

13. One (1) 12-month waiver may be granted by OCC, RC Division, NET 12 months from published results, NLT 18 months from published results. One (1) additional 6-month waiver may be granted by OCC, Director, NET 24 months from published results, NLT 30 months from published results. Warrant Officers who are not granted a waiver or have not completed all required training will not be granted designated MOS and must remain in their current MOS.

a. One (1) 12-month waiver can be submitted to the Office Chief of Cyber, Reserve Component Division (Cyber Proponent): usarmy.gordon.cyber-coe.mbx.rcao-cyber@army.mil. Waiver must have O-5 or higher concurrence.

b. One (1) 6-month waiver can be submitted to the Office Chief of Cyber, Reserve Component Division (Cyber Proponent): usarmy.gordon.cyber-coe.mbx.rcao-cyber@army.mil. Waiver must have O-6 or higher concurrence.

14. Warrant Officers with questions concerning reclassification opportunities should contact their Senior Warrant / WOSM or access the Cyber Reserve Component SharePoint: <https://armyeitaas.sharepoint-mil.us/:u:/r/sites/TR-CCoE-CYBERSCHL/SitePages/Cyber%20RC%20Division.aspx>.

15. Address questions or concerns about the cyber reclassification process to:

a. Army National Guard Strategic Operations Division at: ng.ncr.ngb-arng.list.cyber@army.mil; ng.va.ngb.mbx.arng-warrant-officer-170x-branch-transfer-requests@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.gordon.cyber-coe.mbx.rcao-cyber@army.mil

