MISSOURI NATIONAL GUARD
JOINT FORCE HEADQUARTERS
IKE SKELTON TRAINING SITE
2302 MILITIA DRIVE
JEFFERSON CITY, MISSOURI 65101-1203

S: **20 Mar 26**
S: **31 Jan 27**

NGMO-PER-AB (600-8-19D) 18 February 2026

MEMORANDUM FOR DISTRIBUTION A & I

SUBJECT: Statewide Vacancy Announcement (**SWVA #26-0048**)

1. The vacancy has been verified against the UMR and AUVS and the following position is open statewide for best select interviews:

a.	Unit Name / UIC:	DCOE-JFHQ / W8AJAA
b.	MOS / Duty Title:	17C / Cyber Operations Specialist
c.	Position # / Grade:	09189659 / E5
d.	Location:	Jefferson Barracks, MO

2. Applicability: MOS specific duties and qualification requirements are listed in the enclosed.

3. Interested, qualified candidates may apply by emailing a completed application and all other required documentation to CW3 Katie Herrell at kathleen.d.herrell.mil@army.mil. Reference the SWVA number located in the above subject line on all documents.

4. Soldiers holding a Select Reserve Incentive Program bonus are recommended to consult with the Education & Incentives office to determine compatibility.

5. All units will post this announcement on their unit bulletin board and in their monthly newsletter through the suspense date. For additional information, see the Memorandum of Instruction (MOI) for the 2026 Enlisted Promotion System (EPS), dated 1 May 2025.

FOR THE MILPO:

Digitally signed by
OSIIER.TABITHA.DAWN.125786
7290
Date: 2026.02.17 14:15:39 -06'00'

TABITHA D. OSIIER
MAJ, MS, MOARNG
Chief, Military Personnel Services Division

MISSOURI NATIONAL GUARD
VACANCY ANNOUNCEMENT

Opening Date: 18 February 2026
Closing Date: 20 March 2026
Position: 17C Cyber Operations Specialist
Grade/Rank: E-5/SGT
DMOS: 17C2O
PARA/LINE: 238/17
Location: Defensive Cyber Operations Element (DCOE), Jefferson Barracks, MO. 63125
APPOINTMENT FACTORS: The vacancy is a **TRADITIONAL GUARD** position.

M-DAY APPLICANTS MUST:

1. Meet physical standards IAW Chapter 3, AR 10-501 (Retention Standards). Meet height and weight standards of AR 600-9.

2. Must be able to pass the Army Fitness Test (AFT).

3. Minimum Military Grade: E-3/PFC
   Maximum Military Grade: E-5/SGT

WHO MAY APPLY: All qualified Missouri Guard members and those eligible for enlistment or transfer into the Missouri Army National Guard in the rank of Private First Class to Sergeant.

MAJOR DUTIES: The DCOE is the State of Missouri’s Cyber incident response capability. Members can be called upon by the Adjutant General and/or the Governor of Missouri to defend the Department of Defense Information Network (DoDIN) as well as critical infrastructure within the State of Missouri. Soldiers will be expected to be called upon as an incident responder and maintain both the DCWF Host Analyst (Work Role ID: 463) and Network Analyst (Work Role ID: 443) Roles. The ability to work more than one two-week Annual Training period per year is also expected.

PHYSICAL DEMANDS AND QUALIFICATIONS:

1. Have a minimum of 36 months TIS remaining after completion of the functional training.
2. Must possess, at a minimum, a Secret clearance at the time of application with the ability to meet TS/SCI access eligibly if selected for the position.
3. Due to the nature of training and assignments, temporary restrictions may be placed on foreign travel, both during and after, the term of service.
4. Be qualified or able to be qualified 17C within at least one year of branch transfer approval.

5. Must display high moral character as determined by the following criteria:
   (a) No pattern of undesirable behavior as evidenced by civil and military records
   (b) No record of convictions by court martial
   (c) No record of civilian conviction within the last two years other than minor traffic offenses
6. Must be a U.S. citizen.
7. Must be able to meet DoDI 8140.03 Qualifications for the Host and Network Analyst Roles within one year of acceptance:
   (a) System Administration (i.e. Security+, CySA+, GSEC)
   (b) Analyst and/or Incident Responder Roles (i.e. CEH, CySA+, GCIH)
8. Must be able to maintain Joint Qualification Requirements (JQR) for both Host and Network Analyst Roles according to the DoD Cyber Workforce (DCWF)
9. Complete the Incident Response Handler Course within one year of acceptance of position.
10. Complete the Cyber Operational Training Experience within one year of acceptance of position
11. 17C qualified or Branch Transfer Acceptance Memo holders preferred
12. If not currently 17C Branch Transfer Approved or MOS qualified at time of application, Servicemember must submit branch reclassification application packet within 90 days of acceptance of position or be reassigned to another unit. Please refer to MILPER Number: 25-287 (FY 26 Reserve Component Reclassification Procedures for MOS 17C).
13. 17C Reclassification applicants that are not eligible for branch transfer will be reassigned to another unit after results of Eligibility panel is received.

HOW TO APPLY: Packet should consist of the following required items**:**

1) Copy of Soldier Talent Profile from IPPS-A

2) Copy of most recent ASVAB Scores on a REDD Report or page 1 of DD 1966 series

3) E5 and above - Copies of last three NCOERS. If three NCOERs are not available, supplement with a recommendation memo from Platoon Sergeant, 1SG, or Commander

4) E3 & E4 - Recommendation memo from Platoon Sergeant, 1SG, or Commander

5) Copy of DA Form 705 (Army Physical Fitness Test Card). The latest 'RECORD' test must be within 12 months

6) Copy of DA Form 3349 (Physical Profile) and MMRB results (if applicable)

7) Copy of DA Form 5500-R or 5501-R (Body Fat Worksheet) (if applicable)

8) Memorandum from unit stating whether unfavorable actions or flags are pending

9) Security Clearance Verification (type/date) (if applicable)

10) Copy of most recent MEDPROS IMR Report reflecting most recent PHA and PULHES

11) NGB Form 23 (RPAS Statement) with copies of all DD Form 214 and NGB Form 22

12) DA Form 1059 (Service School Academic Evaluation Report) for all NCOES attended and for the PMOS

13) Cover letter addressing your reason for transfer to this position, to include contact phone and email information

14) Letters of recommendation are suggested but not required

15) Copies of any professional certifications and/or certificates of training applicable to the position (if any)

CAUTION: If your packet does not provide all the information requested on the forms and documents listed above, you may lose consideration for the job and not be interviewed. ONLY complete packets will be considered for interview. Incomplete packets will be returned to the applicant without further communication. If you are unable to provide any of the documents above, a memorandum must be submitted explaining why that document is not available.

FORWARD COMPLETED PACKETS TO:

MONG Cyber Operations
ATTN: CW3 Katie Herrell
44 Johnson Rd. (BLDG 44)
Jefferson Barracks, MO. 63125

Or scan completed packets to kathleen.d.herrell.mil@army.mil

ALL APPLICANTS ARE CONSIDERED WITHOUT REGARD TO RACE, RELIGION, COLOR, NATIONAL ORIGIN, SEX, POLITICAL AFFILIATION, AGE (WITH AUTHORIZED EXCEPTIONS) OR ANY OTHER NONMERIT FACTOR.

THIS ANNOUNCEMENT WILL BE CALLED TO THE ATTENTION OF ALL ASSIGNED PERSONNEL AND POSTED IN A TIMELY MANNER ON ALL BULLETIN BOARDS

For more information, call CW3 Katie Herrell at 314.416.6699

10-17C. MOS 17C—Cyber Operations Specialist, CMF 17

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 produces 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: Planner, Analyst, Operator, and Engineer. Duties for MOS 17C at each level of skill are:

(1) *MOSC 17C1O*. Perform cyber-attack; cyber defense; cyber operational preparation of the environment; and cyber intelligence, surveillance, and reconnaissance actions on specified systems and networks. Conduct network terrain audits, penetration testing, basic digital forensics data analysis, and software threat analysis. React to cyberspace events, employ cyberspace defense infrastructure capabilities, collect basic digital forensics data, provide incident response impact assessments, and produce network security posture assessments. Analyze computer system and network architectures, as well as determine and implement exploitation methods.

(2) *MOSC 17C2O.* Perform duties in preceding skill level and provide guidance to subordinate Soldiers. Lead Soldiers in performing activities in support of offensive and defensive cyberspace operations. Validate critical infrastructure configurations, network alerts, and network security posture assessments. Review, write, edit, evaluate and publish both offensive and defensive cyberspace operations products and reports.

(3) *MOSC 17C3O.* Perform duties shown in preceding skill levels and provide guidance to subordinate Soldiers. Lead operational teams in support of offensive and defensive cyberspace operations. Conduct cyberspace operations risk assessments, post-incident analysis and intermediate software analysis. Collect and analyze intermediate forensics data. Validate architectural analysis, administer penetration testing, and coordinate response actions.

(4) *MOSC 17C4O.* Perform duties shown in preceding skill levels and provide guidance to subordinate Soldiers. Supervise operational teams in support of offensive and defensive cyberspace operations. Direct network terrain audits, digital forensics processes, and exploitation missions. Evaluate cyber defense requirements and participate in the joint targeting process.

(5) *MOSC 17C5O.* Perform duties shown in preceding skill levels and provide guidance to subordinate Soldiers. Perform mission management functions for cyberspace operations. Develop crisis plans to directly support cyberspace operations planning and targeting. Serve as Subject Matter Experts (SME) of the technical integration of cyberspace attack; defense; Intelligence, Surveillance, and Reconnaissance; Operation Preparation of the Environment in support of unified land operations. MSGs 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.

b. *Physical demands rating and qualifications for initial award of MOS.* Cyber Operations Specialist must possess the following qualifications:

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

(2) A physical profile of 222221.

(3) Qualifying scores.

(a) A minimum score of 110 in aptitude area GT and a minimum score of 112 in aptitude area ST.

(b) 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.

(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 Physical Demand Category in “Moderate” (Gold).

(4) A high school graduate or equivalent prior to entry on active duty.

(5) Never been a member of the U.S. Peace Corps, except as specified in AR 614-200(para 3-2).

(6) No information in military personnel, Provost Marshal, intelligence, or medical records that would prevent the granting of a security eligibility under AR 380-67 (para 3.401.a).

(7) No record of conviction by court-martial.

(8) No record of conviction by a civil court for any offense other than minor traffic violations.

(9) Must be a U.S. citizen.

(10) The Soldier must meet TOP SECRET (TS) Sensitive Compartmented Information (SCI) access eligibility requirements to be awarded and maintain the MOS. The clearance requirement to begin 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.

(11) Recruits or Soldiers cannot hold this MOS if they have immediate family members (includes both blood and step: spouse, parents, siblings, children, any sole living blood relative, cohabitant of the individual, or a person in loco parentis per AR 600-8-10) who are citizens or dual-citizens, or reside in one of the countries on the U.S. Army Tiered Country List. Waiver requests must be coordinated with the Cyber Center of Excellence, Personnel Security Office.

(12)Have neither commercial nor vested interest in a country within whose boundaries physical or mental coercion is known to be a common practice against persons acting in the interest of the U.S. This requirement applies to the Soldier's spouse as well.

(13) Due to the nature of training and assignments, temporary restrictions may be placed on foreign travel both during and after the term of service.

(14) 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.

(15) Formal Training (successful completion of 17C Cyber Operations Specialist Course, conducted under the auspices of the US Army Cyber School) is mandatory. Constructive credit for formal training and/or operational experience may be granted by Commandant, US Army Cyber School, Fort Eisenhower, GA 30905-5300.

(16) IET Soldiers incur a 5 year term of service, beginning upon completion of 17C Cyber Operations Specialist Course.

(17) The Service Remaining Requirement (SRR) for reclassification into MOS 17C under the provisions of AR 614-200, Chapter 4 is 3 years, which will begin upon completion of all required training. If no training is required the SRR will begin upon effective date of reclassification. If ASI “Y2” is utilized, the SRR will begin upon completion of training and “Y2” will be removed.

c. *Additional skill identifiers.* (Note: Refer to table 12-8 (Listing of universal ASI’s associated with all enlisted MOS)).

(1) 5C – Mission Command Digital Master Gunner

(2) Q6--Protection Cell Operations (skill level 4 through 6 for personnel only) (Effective 202410).

(3) E6 – Interactive On-net Operator.

(4) Y2 – Transition (personnel only).

d. *Physical requirements and standards of grade.* Physical requirements and SG relating to each skill level are listed in the following tables:

(1) *Table 10-17C-1.* Physical requirements.

(2) *Table 10-17C-3.* Standards of grade TDA.