NEBRASKA ARMY NATIONAL GUARD
DIRECTORATE OF PERSONNEL ADMINISTRATION
ENLISTED PROMOTION SECTION
2433 NW 24TH STREET
LINCOLN, NEBRASKA 68524

TRADITIONAL VACANCY ANNOUNCEMENT

Announcement Number: 24-97NAA-003B3 **Closing Date:** Open Until Filled

Position Title & Unit: Host NCO, 179th Cyber Protection Team **Location:** Lincoln, NE

Military Grade Range: Minimum SGT/E5 - Maximum SFC/E7

Military Requirements: Designated CPMOS for this position 17C. Must meet the physical demands requirements of DA Pam 611-21. MOS qualification, if required, must be completed IAW current policy and training guidance. Selected individual may incur additional training requirements for SQI and/or ASI requirements for the duty position (see unit specific requirements below). The qualifications for the award of this MOS can be found in DA Pam 611-21.

Area of Consideration: All eligible and available members of the Nebraska Army National Guard or eligible personnel available for transfer into the Nebraska Army National Guard serving in the grade range listed above. In order to be promoted in this position, the selected Soldier must be fully qualified for promotion IAW AR 600-8-19.

General Requirements:
1. Currently assigned SGT/E5 – SFC/E7 in the Nebraska Army National Guard or any personnel eligible for transfer into the Nebraska Army National Guard.
2. Not currently "Flagged from Favorable Personnel Actions" or under a "Bar to Reenlistment", or defined as “Stagnant”.
3. Meet other requirements as stated in **Military Requirements** above.

Summary of Duties: Serves as the team HOST NCO for 179th CPT; 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.

Other Unit Unique Considerations/Requirements: Selected individual must be willing to put in a 17C reclassification packet within 90 days. Must be willing to attend 17C MOS at the earliest available course upon 17C packet acceptance. Selected individual must have at least 3 years’ time remaining on the current contract from graduation of 17C MOSQ, and if not be willing to extend to a minimum 3 years. Must have a mixture of hands on Signal and Cyber experience, to include but not limited to servers, clients, threat hunting, and virtualization to support a diverse and dynamic mission. Must have experience in managing projects and Soldiers with different technical disciplines.

Application Instructions: Submit a completed Traditional NCO Vacancy Application by e-mail to **ng.ne.nearng.list.g1-epm@army.mil** with a subject line of "**Vacancy Application 23-97NAA-003B3**” or in hard copy to the G1 office no later than 1600 hours on the closing date. Electronic applications must be in PDF format on one single attachment. The use of official mail to forward employment applications is prohibited. Applications or attachments which are unreadable or cannot be opened will not be accepted or considered. G1 is not responsible for any malfunctions when using electronic means to transmit job applications. Applicants may verify receipt of their application telephonically by calling (402)309-8152.

10-17C. MOS 17C—Cyber Operations Specialist, CMF 17 (eff 202210)

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 113 in aptitude area ST on Armed Services Vocational Aptitude Battery (ASVAB) test administered prior to 1 July 2004.

(b) A minimum score of 110 in aptitude area GT and a minimum score of 112 in aptitude area ST on ASVAB tests administered on and after 1 July 2004..

(c) 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.

(d) 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 Gordon, 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) E6 – Interactive On-net Operator

(3) 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.