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

***TRADITIONAL VACANCY ANNOUNCEMENT***

**Announcement Number:** 23-8ANA1-23811 **Closing Date:** Open Until Filled

**Position Title & Unit:** Incident Responder, Defense Cyber Operations Element **Location:** Lincoln, NE

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

**Military Requirements:** Designated CPMOS for this position 25D. 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. ****Non-DMOSQ applicants should pay close attention to specific requirements by grade IAW the attached excerpt from DA Pam 611-21.**

**Area of Consideration:** All eligible and available members of 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.
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:** Uses defensive measures and information collected from a variety of sources (including intrusion detection system alerts, firewall logs, network traffic logs, and host system logs) to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Provides detailed analysis reports as necessary to support mission requirements. Predominantly, serves in AN positions and in IS positions within limited organizations. Performs CND and IAT Level II-III functions as required by skill level, AR 25-2 and DoD 8570.01M. Serves as COMSEC Account Manager, when unit has a documented CAM position.

**Other Unit Unique Considerations/Requirements**: None

**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 23-8ANA1-23811**” 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.

**10-25D. MOS 25D-- Cyber Network Defender, CMF 25 (Effective 201910)**

a. *Major duties. P*erforms the duties associated with the five Computer Network Defense (CND) specialties (i.e., Infrastructure Support (IS), Analyst (AN), Incident Responder (IR), Auditor (AU) and Manager (MGR)), Information Assurance Technical (IAT) Levels I-III functions, Information Assurance Management (IAM) Levels II-III functions, as required by skill level IAW AR 25-2 and DoD 8570.01-M. CND protects against, monitors for, performs analysis of, responds to and detects unauthorized activity in the cyberspace domain, which includes deployment and administration of the CND infrastructure; performs deliberate actions to modify information systems or network configurations in response to CND alert or threat information; collects data gathered from a variety of CND tools to analyze events and warn of attacks that occur within the environment; plans response activities to contain and eradicate cyber incidents within the network environment or enclave; responds by validating incidents, performs incident correlation and trending, conducts network damage assessments, and develops response actions; performs assessments of threats and vulnerabilities within the network environment or enclave and identifies deviations from acceptable configurations, enclave policy, or local policy:

(1) *MOSC 25D3O.* Tests, implements, deploy, maintain and administer CND infrastructure hardware and software required to provide defense-in-depth to the network and resources. CND tools may include, but is not limited to routers, firewalls, intrusion detection systems and/or intrusion prevention systems, and other CND tools as deployed within the computing environment (CE) or network environment (NE). Responds to crisis or urgent situations within the network to mitigate immediate and potential cyber threats. Predominantly, serves in IS positions and in AN positions within limited organizations. Performs CND and IAT Level II functions in accordance with AR 25-2 and DoD 8570-01M. 25D3O will not perform duties as a Drill Sergeant or Recruiter.

(2) *MOSC 25D4O.* Uses defensive measures and information collected from a variety of sources (including intrusion detection system alerts, firewall logs, network traffic logs, and host system logs) to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Provides detailed analysis reports as necessary to support mission requirements. Predominantly, serves in AN positions and in IS positions within limited organizations. Performs CND and IAT Level II-III functions as required by skill level, AR 25-2 and DoD 8570.01M. 25D4O will not perform duties as a Platoon Sergeant, Drill Sergeant, or Recruiter.

(3) *MOSC 25D5O.* Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize network and information system confidentiality, integrity, and availability. These tasks include, but are not limited to creating and maintaining incident tracking information; planning, coordinating, and directing recovery activities; and incidents analysis tasks, including examining all available information and supporting evidence of artifacts related to an incident or event. Conducts assessments of threats and vulnerabilities (through such tasks as authorized penetration testing, compliance audits and risk assessments) to determine deviations from acceptable configurations and enterprise or local policies; and develops and/or recommends appropriate mitigation countermeasures. Respond to crisis or urgent situations within the network to mitigate immediate and potential cyber threats. Conducts assessments of threats and vulnerabilities (through such tasks as authorized penetration testing, compliance audits and risk assessments) to determine deviations from acceptable configurations and enterprise or local policies; and develops and/or recommends appropriate mitigation countermeasures. Develops and provides training to command and staff on CND matters. Predominantly, serves in IR positions and in AU and MGR positions within limited organizations. Performs CND functions, IAT Level III functions and IAM Level II-III functions as required by skill level, AR 25-2 and DoD 8570.01M. 25D5O will not perform duties as a First Sergeant.

(4) *MOSC 25D6O.* Supervises, plans, coordinates and directs CND operations within their organization. Serves as the senior enlisted CND advisor and provides senior level CND technical and tactical advice to command and staff on CND matters. Leads the establishment of command level CND tactics, techniques, procedures (TTP), and policies. Assists in the development of organizational Continuity of Operations Plan (COOP). Responsible for system lifecycle management, technology integration, and DoD Information Assurance Certification and Accreditation Process (DIACAP) as it relates to CND functions and mission. Serves in MGR positions above the Corps echelon. Performs CND IAM Level III functions as required by skill

level, AR 25-2 and DoD 8570.01-M. 25D6O will not preform duties as a Command Sergeants Major.

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

(1) Physical demands rating of Moderate (Gold).

(2) A physical profile of 212221.

(3) Normal color vision.

(4) Qualifying scores.

(a) A minimum score of 105 in aptitude area GT and ST on Armed Services Vocational Aptitude Battery (ASVAB) test.

(b) A minimum OPAT score of Long Jump (LJ) - 0120 cm, seated Power Throw (PT) - 0350 cm, Strength Deadlift (SD) - 0120 lbs., and Interval Aerobic Run (IR) - 0036 shuttles in Physical Demand Category of “Moderate” (Gold).

(5) A SSG, MOS immaterial, with at least 4 years of experience in IA and IT. This experience must be verified by the Office Chief of Signal (OCOS) Enlisted Division.

(6) All candidates for this MOS will process a selection packet through their local Command, who will forward to the OCOS for conditional acceptance and approval to take the 25D In-Service Screening Test (ISST).

(7) All candidates for this MOS will take and pass the 25D ISST for enrollment into the MOS producing course.

(8) A SSG must have Advanced Leader Course (ALC) common core (CC) or Structured Self Development (SSD) II completed with at least 8 years time in service (TIS) but no more than 15 years TIS.

(9) SSG waiver may be granted to SGT(P) with ALC CC or SSD II completed who meets all other requirements by the Commandant, U.S. Army Signal School, ATTN: ATSO-CD, Ft. Gordon, GA 30905-5735.

(10) A security clearance of TOP SECRET is required for the initial award of MOS. Must remain eligible to receive security access of TOP SECRET with SCI to maintain MOS.

(11) Must hold a current certification under either IAT Level II or IAM Level I IAW DoD 8570.01-M.

(12) Ability to read, comprehend, and clearly enunciate English.

(13) A U.S. citizen.

(14) Formal Training (successful completion of 25D Cyber Network Defender Course, conducted under the auspices of the USA Signal School) is mandatory. Waiver may be granted by Commandant, U.S. Army Signal School, ATTN: ATZH-CD, Ft Gordon, GA 30905-5735.

(15) Meet service remaining requirement per AR 614-200.

(16) Point of contact for verifications of qualifications is OCOS Enlisted Division – usarmy.gordon.cyber-coe.mbx.sigcoeocosed-mailbox@mail.mil

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

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

(1) *Table 10-25D-1.* Physical requirements.

(2) *Table 10-25D-2.* Standards of grade TOE/MTOE.

(3) *Table 10-25D-3.* Standards of grade TDA.