

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

TRADITIONAL VACANCY ANNOUNCEMENT

Announcement Number: 24-P4MAA-125/09 25D40

Closing Date: Open Until Filled

Position Title & Unit: Senior Infrastructure Support

Location: Lincoln, NE

HSC, 67th MEB

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

Military Requirements: Designated CPMOS for this position 25D. A security eligibility of Top Secret with SCI is required for initial award and to maintain this MOS. 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 serving in the grade range listed above. In order to be promoted in this position, the Soldier must be fully qualified for promotion IAW AR 600-8-19.

General Requirements:

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

Summary of Duties: Performs 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.

MOSC 25D40. 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. 25D40 will not perform duties as a Platoon Sergeant, Drill Sergeant, or Recruiter.

Other Unit Unique Considerations/Requirements: Student must complete the 25D application process to receive approval (Final 25D Acceptance memo) from Office Chief of Signal, Fort Gordon, GA. prior to class seat reservation. Student MUST bring a copy of their TS/SCI clearance for in-processing and evidence from losing or home station unit S2 Security Manager that a TS/SCI investigation has been initiated and no derogations exist that would jeopardize the awarding of the TS/SCI. MOS immaterial, physical demands rating of medium, physical profile of 212221, normal color vision, and have a minimum score of 105 on both GT and ST on the ASVAB. Only Soldiers, regardless of rank, vetted by the Office Chief of Signal and approved by Human Resources Command, Reclassification Branch for the purpose of reclassification can attend (i.e., be enrolled), this MOS producing course. SGT (P), SSG, SFC, MSG, and SGM can attend providing they meet the prerequisites provided for their rank below:

SGT (P)/SSG: AT LEAST 4 YEARS OF EXPERIENCE IN INFORMATION ASSURANCE (IA) and INFORMATION TECHNOLOGY (IT); ADVANCED LEADER COURSE (ALC) COMMON CORE OR SSD II COMPLETED WITH AT LEAST 8 YEARS TIME IN SERVICE (TIS). MUST HOLD A CURRENT CERTIFICATION UNDER EITHER INFORMATION ASSURANCE TECHNICIAN (IAT) LEVEL II OR INFORMATION ASSURANCE MANAGEMENT (IAM) LEVEL I IAW DOD 8570.01-M. SERGEANTS FIRST CLASS (SFC): AT LEAST 7 YEARS OF EXPERIENCE IN IA AND IT. ALC GRADUATE WITH AT LEAST 9 YEARS TIS BUT NO MORE THAN 20 YEARS TIS. SOLDIERS DOES NOT NEED TO BE A SENIOR LEADER COURSE (SLC) GRADUATE. MUST HOLD A CURRENT CERTIFICATION UNDER EITHER IAT LEVEL II OR IAM LEVEL I IAW DOD 8570.01-M. MASTER SERGEANT (MSG): AT LEAST 9 YEARS OF EXPERIENCE IN IA AND IT. AT LEAST 11 YEARS TIS BUT NO MORE THAN 23 YEARS TIS. MUST HOLD A CURRENT CERTIFICATION UNDER IAM LEVEL II IAW DOD 8570.01-M. SGM: AT LEAST 11 YEARS OF EXPERIENCE IN INFORMATION ASSURANCE (IA) AND INFORMATION TECHNOLOGY (IT). AT LEAST 13 YEARS TIME IN SERVICE (TIS) BUT NO MORE THAN 27 YEARS TIS. MUST HOLD A CURRENT CERTIFICATION UNDER INFORMATION ASSURANCE INFORMATION ASSURANCE MANAGEMENT (IAM) LEVEL II IAW DOD 8570.01-M.

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 24-P4MAA-125/09-25D40**" 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 by calling (402)309-8152.