NEBRASKA NATIONAL GUARD
HUMAN RESOURCES OFFICE
2433 NW 24TH STREET
LINCOLN, NEBRASKA 68524

ACTIVE GUARD RESERVE VACANCY ANNOUNCEMENT

Announcement Number: AGR-AF-22-033

Closing Date: 22 July 2022

Position Title: IT Specialist (CustSpt)
(Concurrent with Technician position
NE-11546560-AF-22-048, IT SPECIALIST)

Location: 155th CF, Lincoln, NE

Military Grade Range: Minimum A1C/E-3 - Maximum MSgt/E-7

Military Requirements: On board AGRs only**.** Designated AFSC for this position is any Comm 1D or 3D. Must be a U.S. Citizen and have or be able to obtain a Secret security clearance. The applicant must meet the DoD 8570 and AFSC requirements within one year of appointment. As mandated by the Secretary of Defense, employees are required to be fully vaccinated against COVID-19 regardless of the employee's duty location or work arrangement (e.g., telework, remote work, etc.), subject to such exceptions as required by law. If selected, you will be required to meet the COVID-19 vaccine requirements established by your military component. **Applicants will review the qualifications for the award of this AFSC in the AFECD. Failure to review these qualifications may result in the applicant not being eligible for the position.**

Area of Consideration: All on board AGR members of the Nebraska Air National Guard in the grade of A1C/E-3 –MSgt/E-7 may apply for this position. There are two vacancies.

Area 1 – AFSC Qualified
Area 2 – AFSC Not Qualified

1. Specialty Summary. Installs, supports, and maintains server operating systems or other computer systems and the software applications pertinent to its operation, while also ensuring current defensive mechanisms are in place. Responds to service outages and interruptions to network operations. Administers server-based networked systems, distributed applications, network storage, messaging, and application monitoring required to provision, sustain, operate, and integrate cyber networked systems and applications in garrison and at deployed locations. Core competencies include: server operating systems, database administration, web technologies, systems- related project management, and supervising cyber systems. Supports identification and remediation of vulnerabilities while enhancing capabilities within cyber environments to achieve desired affects. Related DoD Occupational Subgroup: 153100.

2. Duties and Responsibilities:
2.1. Defends, protects, and secures mission networking environments and devices. Provides networked application resources by designing, configuring, installing, and managing data services, operating system, and server applications. Provides directory services utilizing dynamically-assigned internet protocol (IP) addresses, domain name server (DNS), network storage devices, and electronic messaging resources. Manages secure authentication methods utilizing public key infrastructure (PKI) technologies and procedures. Standardizes user privileges and system settings using

automated deployment tools such as Group Policy Management Console (GMPC) and System Management Server (SMS). Manage accounts, network rights, and access to systems and equipment according to standards, business rules, and needs. Implements server and special mission system security fixes, operating system patches, and antivirus software. Develops, tests, and implements local restoral and contingency operations plans. Processes and reviews C4 systems requirement documentation, telecommunication service requests, status of acquisition messages, and telecommunication service orders. Performs strategic and budget planning for networks. [DCWF Code - 441, 451]
2.2. Performs user accounts management and standardizes systems settings using automated deployment tools. Manages physical, virtual, and cloud-based server/client hardware. Performs system-wide backups and data recovery. Ensures continuing systems operability by providing ongoing optimization and problem solving support. [DCWF Code - 441, 451]
2.3. Performs system resource management, to include load and capacity planning and balance. Creates, administers, and audits system accounts. Performs system-wide backups and data recovery. Ensures continuing systems operability by providing ongoing optimization and problem solving support. Applies computer security policies to safeguard systems and information. Categorizes, isolates, and resolves system problems. Performs fault recovery by validating, isolating, correcting faults, and verifying service restoral with customers. Processes, documents, and coordinates resolution of trouble calls from lower support echelons. Processes scheduled and authorized outages. Submits outage reports in response to unscheduled outages. [DCWF Code - 441, 451]
2.4. Utilizes enterprise patching tools to implement security updates and patches to include: Information Assurance Vulnerability Assessments, C4 Notice to Airman, Time Compliance Network Orders, Time Compliance Technical Order, operating system patches, and antivirus software updates. Implements and enforces national, DoD, and Air Force security policies and directives. Performs proactive security functions to deter, detect, isolate, contain, and recover from information system and network security intrusions. Performs system sanitation resulting from classified message incidents and classified file incidents. [DCWF Code - 441, 451, 461]
2.5. Supports information warfare operations within strictly controlled parameters and provides real-time intrusion detection and firewall protection for all networked resources. Researches latest system threats to develop and test tactics, techniques, and procedures (TTPs) for defensive information operations. Employs TTPs on Air Force and DoD computer networks to defend against hostile information operations. Analyzes risks and/or vulnerabilities and takes corrective action to mitigate or remove them. [DCWF Code - 511, 521, 541]
2.6. Reviews and implements C4 systems requirements. Performs strategic and budget planning for systems hardware and software. Coordinates and implements system service level agreements and memoranda of understanding with user agencies.
2.7. As part of the Cyberspace Support career field family, performs IT project management duties to include; manage, supervise, and perform planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings for facility design, military construction programs and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, wartime, support, contingency and exercise plans to determine impact on manpower, equipment, and systems. [DCWF Code - 802]

2.8. As part of the Cyberspace Support career field family, conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]
2.9. Performs risk management framework security determinations of fixed, deployed, and mobile information systems (IS) and telecommunications resources to monitor, evaluate, and maintain systems, policy, and procedures to protect clients, networks, data/voice systems, and databases from unauthorized activity. Identifies potential threats, administers, and manages resolution of Communications Security (COMSEC) incidents. [DCWF Code - 461, 722]
2.10. Develops and writes new or modifies existing specialized utility programs (scripts) following software assurance best practices. Tests specialized utility programs (scripts) to ensure they meet intended performance targets. Deploys specialized utility programs (scripts) to automate the deployment of software packages or simplify the collection of systems/software data. [DCWF Code – 621]
3. Specialty Qualifications:
3.1. Knowledge. Knowledge is mandatory of cyber systems elements: capabilities, functions, and technical methods for system operations.
3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses or certifications in computer and information systems technology are desirable. Any network or computing commercial certification is desirable.
3.3 Training. For award of AFSC, completion of Cyber System s Operations initial skills course is mandatory.
3.3. Experience. The following experience is mandatory for award of the AFSC indicated:
3.3.1. 3D052. Qualification in and possession of AFSC 3D032. Experience in functions such as system operations, multi-user technical support, system restoral, resource counting, or security.
3.3.2. 3D072. Qualification in and possession of AFSC 3D052. Experience supervising one of the following functions: analysis of system failure and restoral, operations, command and control systems support, system administration, or resource and project management.
3.5. Other. The following are mandatory as indicated:
3.5.1. For entry into this specialty, see attachment 4 for entry requirements.
3.5.2. For award and retention of this AFSC:
3.5.2.1. Must maintain local network access IAW AFI 17-130, Cybersecurity Program Management and AFMAN 17-1301, Computer Security.
3.5.3. Specialty routinely requires work in the networking environment.
3.5.3.1. Must attain and maintain a minimum Information Assurance Technical Level II certification IAW AFMAN 17-1303, Cybersecurity Workforce Improvement Program and DoD 8570.01-M, Information Assurance Workforce Improvement Program.
3.5.2.4. Completion of a current Tier 5 (T5) background investigation according to AFMAN 16-1405, Personnel Security Program Management, is mandatory.
3.5.2.5. Must maintain a T5 clearance for retention of this AFSC.
NOTE: Award of entry level without a completed T5 Investigation is authorized provided an interim Top Secret clearance has been granted according to AFMAN 16-1405.

Application Instructions:

Please read the application instructions as there have been changes to the application and process for applying.
!!! IMPORTANT NOTICE!!!

Applications will be screened after the job closing date, not prior. Please review your application for accuracy before you submit it to HRO. Nothing will be added to the application after 1600 hrs on the closing date.

E-mail may be sent to ng.ne.nearng.list.hro-agr-job-apps@mail.mil with a subject line of "Job Application AGR-AF-__-___ (list job announcement number)". Electronic applications will be submitted as one attachment. Applications submitted in multiple attachments will not be accepted. Applications submitted in binders or document protectors will not be accepted. Applications or attachments which are unreachable or cannot be opened will not be accepted or considered.

Packets without the appropriate documents or a written explanation will not be processed for interviews. Applicants will use the following checklist to ensure proper documentation is submitted.

____ **Yes** ____ **No** 1. **Application for Active Guard/Reserve (AGR) Position, NGB Form 34-1, dated 20131111. This form can be downloaded from the Nebraska National Guard Opportunities webpage. Previous versions of the form will not be accepted.** Application must be signed and written explanations for YES answers must be provided within the application packet. ____(Initials)

____ **Yes** ____ **No** 2. **Records review RIP or SURF Sheet** ____(Initials)

____ **Yes** ____ **No** 3. **Last 3 Officer / Enlisted Performance Reports (OPR / EPR),** or Statement addressing missing reports. Does not apply to traditional, enlisted Airmen or if you have not required 3 OPR/EPR's. ____(Initials)

____ **Yes** ____ **No** 4. **Current Point Credit Summary -** Applies to Reserve Component/ANG Only ___(Initials)

____ **Yes** ____ **No** 5. **Current Flying History Report** (if applicable) ____(Initials)

____ **Yes** ____ **No** 6. **AF 422 or DD 2992** (showing current physical PULHES) and PHA within 12 months ____(Initials)

____ **Yes** ____ **No** 7. **AF Fitness Assessment with current Fit Test Score and Fit Test History** Member must provide current documentation **from their fitness monitor** showing they meet the **fitness standard score of 75 or higher** IAW NGB/AIPOF Memorandum dated, 1 Oct 08, Subject: Interim Guidance Implementation of Standard Fitness Score for Purposes of Promotion and Reenlistment, Effective 1 October 2008, AWGI 10-248, and ANGI 36-101. ____(Initials)

The use of official mail to forward employment applications is prohibited. Applications submitted using government postage will not be considered.

Mail applications to: *NE National Guard*
Human Resource – AGR Branch
2433 NW 24th Street
Lincoln, NE 68524

The HRO is not responsible for any malfunctions when using electronic means to transmit job applications. Applicants may request to verify receipt of their application through e-mail or telephonically.

The Nebraska National Guard is an equal opportunity employer; we do not discriminate on the basis of race, gender, sexual orientation, religion, national origin or ethnicity.