|  |  |
| --- | --- |
| **ADVERTISEMENT TRADITIONAL GUARD ENLISTED VACANCY ANNOUNCEMENT** | |
| **NEW YORK AIR NATIONAL GUARD**  **174TH ATTACK WING**  **6001 EAST MOLLOY ROAD**  **SYRACUSE, NEW YORK 13211-7099** | **ANNOUNCEMENT #:** FY 22-39 |
| **DATE: 7 September 2022** |
| **CLOSING DATE: UNTIL FILLED** |
| **UNIT: 174th Communications Flight** | **AFSC:** 1D7X1B  **RANK:** SSgt |
| **POSITION TITLE:**  Systems Operations | **AREA OF CONSIDERATION: NATIONWIDE**  All members who meet the qualifications for these positions  **Anyone Eligible To Join The Air National Guard** |
| **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. | |
| **DUTIES AND RESPONSIBILITIES**   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 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. 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. 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. | |
| **CLEARANCE**  Top Secret, as a minimum.  (SEE REVERSED) | |
| **INQUIRIES ABOUT POSITIONS**  **Please Contact The Recruiting Office @ 315-427-9460 / 315-233-2159 For Qualification and Eligibility Questions.** | |