HAWAII AIR NATIONAL GUARD

ACTIVE GUARD RESERVE FULL TIME Job ANNOUNCEMENT

Application Opening Date:	Application Closing Date:	Position Number
21 DEC 2018	**14 JAN 2019**	**FY 19-018**
Duty Position:	Grade Min. / Max.:	Duty AFSC:
SUPV IT SPEC (NETWORK)	**MSgt (E7) / MSgt (E7)**	**3D072**

Duty Location:
154 CS
360 Harbor Dr.
Hickam AFB, HI 96853

Selecting Official: Maj Mariko M. Boone
Point of Contact: MSgt Shane Gaines
Comm: 808-672-1235
Who May Apply: **1st Area of Consideration: Open to on-board technician within the (154 CS) Hawaii Air National Guard that has a duty AFSC 3D072.**

2nd Area of Consideration: Open to military members within the Hawaii Air National Guard that has a duty AFSC 3D072.

3rd Area of Consideration: Open to Air Force military members located in the State of Hawaii that has a duty AFSC 3D072.

4th Area of Consideration: Open Nationwide to Air Force military members that has a duty AFSC 3D072 and must be able to become a member of the Hawaii Air National Guard.

Qualifications, Duties and Responsibilities:
Classification Directory AFECD & AFOCD - (accessed from a .mil computer)
https://mypers.af.mil/app/categories/c/1363/p/13
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. 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.
2.2. 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.
2.3. 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.
2.4. 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.
2.5. 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.
2.6. As part of the Cyberspace Support career field family, manages, supervises, and performs 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 status 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.
2.7. Conducts defense 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.
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, must maintain local network access IAW AFI 17-130, Cybersecurity Program Management and AFMAN 17-1301, Computer Security.
3.5.2.1. Specialty routinely requires work in the networking environment.
3.5.2.2. Must attain and maintain a minimum Information Assurance Technical Level II certification according to DoD 8570.01-M, Information Assurance Workforce Improvement Program.
3.5.2.3. Specialty requires routine access to Top Secret material or similar environment.
3.5.2.4. Completion of a current Single Scope Background Investigation (SSBI) according to AFI 31-501, Personnel Security Program Management, is mandatory.
NOTE: Award of the 3-skill level without a completed SSBI is authorized provided an interim Top Secret clearance has been granted according to AFI 31-501.

Additional Duties and Responsibilities:

As directed.

FAILURE TO SUBMIT REQUIRED DOCUMENTS WILL RESULT IN THE APPLICATION BEING RETURNED WITHOUT ACTION.

REQUIRED DOCUMENTS:

1. NGB Form 34-1, dated November 2013, Signed, dated and annotated with job number and title.
***YOU MUST USE THE FOLLOWING LINK TO OBTAIN THE CORRECT VERSION OF NGB FORM 34-1: http://www.ngbpdc.ngb.army.mil/forms/Adobe/ngbf34-1.pdf**

*ALL APPLICANTS Must FULLY complete SECTION IV - PERSONAL BACKGROUND QUESTIONAIRE of the NGB FORM 34-1. Any "YES" answers to the questions (except 9 & 10) require a separate sheet fully explaining the "YES" response. A current passing Fit Test will suffice for a "YES" response to question 17. FAILURE to provide this documentation will result in the application being returned without action. **** Application must be signed ****

2. Current & complete Report on Individual Personnel (RIP) printout from virtual MPF
3. Most recent copy of current passing fitness assessment

Forward application and attachments to:

Inquiries Call: (808) 672-1235

Applications are required to emailed to: NG.HI.HIARNG.MBX.NGHI-HRO-AGR@mail.mil

Applications must submit through a DOD government computer and any applications received after 24:00 of close date are returned without action.

NOTE: Due to software constraints, we only accept applications in the following formats by email: MS Word (.docx) or other MS Office products (Outlook file, Excel, PowerPoint) Adobe File (.pdf) Rich Text File (.rtf) Text File (.txt) Tagged Image File

Format (.tif or .tiff) Graphics Interchange Format (.gif) Joint Photographic Expert Group Image (.jpg or .jpeg) and PureEdge Forms

Equal Opportunity/ Basic Eligibility Requirements:

- Application screening will be made without regard to race, religion, color, gender, or national origin.

- Applicants are subject, but not required, to a personal interview, before a military board upon notification of time and place. Necessary travel will be at the expense of the individual. Inquiries concerning specific aspects of the duty position should be directed to the Selecting Official.

- Selection will be made from those applicants determined best qualified in terms of experience, training and demonstrated performance ability.

- All interested members may apply by submitting a completed NGB Form 34-1 and a recent RIP, which can be obtained from the virtual MPF. Due to manning restrictions, positions will not be filled if funding/resource are not available.

- Pregnant females are eligible to apply for AGR tours. Individuals selected for AGR tours must meet all applicable medical and physical requirements in accordance with AFI 48-123 prior to entering or initiating the tour. If selected, they cannot be appointed and entered on active duty until the pregnancy period has expired.

- Must meet the Preventative Health Assessment (PHA)/physical qualifications outlined in AFI 48-123, Medical Examination and Standards. Must also be current in all Individual Medical Readiness (IMR) requirements to include immunizations. RCPHA/PHA and dental must be conducted not more than 12 months prior to entry on AGR duty and HIV test must be completed not more than six months prior to the start date of the AGR tour. The State Air Surgeon will review all medical examinations and determine if a member is physically qualified to enter on AGR duty.

- Grade inversion is detrimental to the military nature of the ANG and is not authorized.

- Must meet the minimum requirements for each fitness component in addition to scoring an overall composite of 75 or higher for entry into the AGR program. Any member in the Fitness Improvement Program (FIP) is ineligible for entry into any type of AGR tour program.

- Should be able to complete 20 years of total active federal military service (TAFMS) prior to reaching mandatory separation - - 28 years commissioned service date for officers; age 60 for enlisted members. Waiver authority of this requirement is The Adjutant General. Individuals selected for AGR tours that cannot attain 20 years of active federal service prior to reaching mandatory separation, must complete a Statement of Understanding. The HING, HRO AGR Branch will maintain the completed and signed Statement of Understanding.

- Must not have been separated “for cause” from active duty or a previous Reserve Component AGR tour.