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 19-013**
Duty Position:	Grade Min. / Max.:	Duty AFSC:
SUPV IT SPEC (NETWORK)	**MSgt (E7) / MSgt (E7)**	**3D0X3**

Duty Location:
154th CS
360 Mamala Bay
JBPHH, 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 3D0X3.**

2nd Area of Consideration: Open to military members within the Hawaii Air National Guard that has a duty AFSC 3D0X3.

3rd Area of Consideration: Open to Air Force military members located in the State of Hawaii that has a duty AFSC 3D0X3.

4th Area of Consideration: Open Nationwide to Air Force military members that has a duty AFSC 3D0X3 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. 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 and manages resolution of communications security incidents. Enforces national, DoD, and Air Force security policies and directives to ensure Confidentiality, Integrity, and Availability (CIA) of IS resources. Administers and manages the overall cybersecurity program to include Communications Security (COMSEC), Emissions Security (EMSEC), and Computer Security (COMPUSEC) programs. Related DoD Occupational Subgroup: 153000.

2. Duties and Responsibilities:

2.1. Conducts cybersecurity risk management framework assessments; ensures enterprise cybersecurity policies fully support all legal and regulatory requirements and ensures cybersecurity policies are applied in new and existing IS resources. Identifies cybersecurity weaknesses and provides recommendations for improvement. Monitors enterprise cybersecurity policy compliance and provides recommendations for effective implementation of IS security controls. 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.

2.2. Evaluates and assists IS risk management activities. Makes periodic evaluation and assistance visits, notes discrepancies, and recommends corrective actions. Audits and enforces the compliance of cybersecurity procedures and investigates security-related incidents to include COMSEC incidents, classified message incidents, classified file incidents, classified data spillage, unauthorized device connections, and unauthorized network access. Develops and manages the cybersecurity program and monitors emerging security technologies and industry best practices while providing guidance to unit-level Information Assurance (IA) Officers. Employ countermeasures designed for the

protection of confidentiality, integrity, availability, authentication, and non-repudiation of government information processed by AF IS's.
2.3. Responsible for cybersecurity risk management of national security systems during all phases of the IS life cycle through remanence security.
2.4. Integrates risk management framework tools with other IS functions to protect and defend IS resources. Advises cyber systems operations personnel and system administrators on known vulnerabilities and assists in developing mitigation and remediation strategies. Provides CIA by verifying cybersecurity controls are implemented in accordance with DoD and Air Force standards. Ensures appropriate administrative, physical, and technical safeguards are incorporated into all new and existing IS resources and protects IS resources from malicious activity.
2.5. Performs COMSEC management duties in accordance with national and DoD directives. Maintains accounting for all required physical and electronic cryptographic material. Issues cryptographic material to units COMSEC Responsible Officer (CRO). Provides guidance and training to appointed primary/alternate CRO. Conducts inspections to ensure COMSEC material is properly maintained and investigates and reports all COMSEC related incidents.
2.6. Performs TEMPEST duties in accordance with national and DoD TEMPEST standards. Denies unauthorized access to classified, and in some instances, unclassified information via compromising emanations within a controlled space through effective countermeasure application. Ensures all systems and devices comply with national and DoD EMSEC standards. Inspects classified work areas, provides guidelines and training, maintains area certifications, determines countermeasures; advises commanders on vulnerabilities, threats, and risks; and recommends practical courses of action.
2.7. Performs Combat Crew Communications (CCC) functions in support of flying operations. Trains and equips airlift, bomber, early warning, reconnaissance, and tanker aircrews with appropriate COMSEC, Flight Information Publications, Identification, Friend or Foe/Selective Identification Feature publications, Combat Mission Folders, High Frequency, MILSTAR, Very Low Frequency/Low Frequency, aircrew training, and programming communications equipment.
2.8. Responsible for oversight or management of installation cybersecurity awareness programs. Promotes cybersecurity awareness through periodic training, visual aids, newsletters, or other dissemination methods in accordance with organizational requirements.
2.9. 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.
2.10. 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, AFECD, 31 October 2018 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: IS resources; capabilities, functions and technical methods for IS operations; organization and functions of networked IS resources; communications-computer flows, operations and logic of electromechanical and electronics IS and their components, techniques for solving IS operations problems; and IS resources security procedures and programs including Internet Protocols.
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 3D033, completion of Cyber Surety initial skills course is mandatory.
3.4. Experience. The following experience is mandatory for award of the AFSC indicated:

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.