Alaska National Guard
Active Guard Reserve (AGR)
Position Announcement
AKANG 18-20

https://dmva.alaska.gov/employment/

POSITION TITLE:	AFSC or MOS	OPEN DATE:	CLOSE DATE:
Cyber Surety Manager	3D053 or 3D073	03 Jan 2018	01 Feb 2018

UNIT OF ACTIVITY/DUTY LOCATION:	GRADE REQUIREMENT:
176th Communications Flight, Joint Base Elmendorf-Richardson, Alaska	**Min:** E5 **Max:** E7

SELECTING SUPERVISOR:	Position Number	PHYSICAL PROFILE:
SMSgt Brandy Thanos	959760	PULHES – 333233

AREAS OF CONSIDERATION

On-board AK ANG AGR (Must hold advertised AFSC)

Alaska Air National Guard members (Must hold advertised AFSC)

Nationwide military members eligible for membership in the AKANG (Must hold advertised AFSC)

MAJOR DUTIES MAY INCLUDE

AIR GUARD: Please refer to attached pages for more info on the major duties and initial qualifications for this position for this AFSC or go to: https://www.my.af.mil to review the AFECD

INITIAL ELIGIBILITY CRITERIA

In addition to criteria listed on attached pages
- Security Clearance - Must be able to obtain: Secret
- Aptitude Requirement: General: 64; or General: 54 and Cyber-Test 60
- Strength requirement: Demonstrated by weight lift of 40lbs

PREFERED QUALIFICATIONS

In addition to the initial eligibility criteria and required forms listed application procedures, the following are preferred qualifications:
- Resume
- Cover Letter
- Last 3 Enlisted/Officer Performance Evaluations
- Letters of Recommendation will be accepted

COMSEC Account Management Experience
Key Management Infrastructure (KMI) Experience

SPECIAL ANNOUNCEMENT CRITERIA

Upon selection additional medical verification will be required prior to start of AGR tour
Continuation beyond initial tour may be subject to evaluation based on AGR Continuation Board

INSTRUCTIONS FOR APPLICANTS

Applicants must not be entitled to receive Federal military retired or retainer pay or Federal civil service annuities and not be eligible for immediate Federal civil service annuities
Individuals who have been separated from other military services for cause, unsuitability, or unfitness for military service are not eligible to enter the AGR program
IAW ANGI 36-101 “Initial tours may not exceed 6 years…”
AGR tours may not extend beyond an Enlisted member’s ETS or an Officer’s MSD
Airmen 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.
For members with a documented Duty Limitation Code (DLC) which prohibits them from performing one or more components of the Fitness Assessment, an overall "Pass" rating is required
Individuals selected for AGR tours must meet the Preventative Health Assessment (PHA)/physical qualifications outlined in AFI 48-123, Medical Examination and Standards. They 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 an HIV test must be completed not more than six months prior to the start date of the AGR tour.
Individuals transferring from Title 10 (Regular Air Force or Reserve Component Title 10 Statutory Tour) are not required to have a new physical unless the previous physical is over 12 months old at time of entry into AGR status
An applicant’s military grade cannot exceed the maximum military authorized grade on the UMD for the AGR position.
Enlisted Airmen who are voluntarily assigned to a position which would cause an overgrade must indicate in writing a willingness to be administratively reduced in grade in accordance with ANGI 36-2503, Administrative Demotion of Airmen, when assigned to the position. Acceptance of demotion must be in writing and included in the assignment application package. Application Package will not be forwarded without statement
ANGI 36-101 “applicant must be able to complete 20 years of active federal service prior to MSD for officers and age 60 for enlisted members. Exceptions may be considered….”
If a selectee does not possess the advertised AFSC, he/she must complete the required training/assignment criteria within 12 months of being assigned to the position. Failure to do so may result in immediate termination. Extension past 12-months will only be considered if the delay is through no fault of the selectee
Members currently on occational tours exceeding 180 consecutive days may be considered as full-time AGR (members currently on occasional tours 179 days or less are not considered AGR). Any further questions regarding the AGR program may be answered in ANGI 36-101

APPLICATION PROCEDURES

Interested applicants who meet the eligibility criteria listed in this announcement may apply by submitting the below listed documents to ng.ak.akarng.mbx.hro-agr@mail.mil. Hard copy applications will NOT be accepted. All applications must be typed or printed in legible dark ink and must be signed and dated with original signature. Applications received with an unsigned NGB 34-1 will not be forwarded for consideration. Applicants may include copies of training certificates or any documentation that may be applicable to the position they are applying for. Per ANGI 36-101, the application package must include at minimum the signed NGB 34-1, current Report of Individual Person (RIP), and current Report of Individual Fitness. Items 1-3 are required by the Human Resource Office to determine initial qualifications. If the required documents are not submitted, a letter of explanation must be included. Incomplete packages will not be considered for the position vacancy.

1. Signed NGB Form 34-1 Application Form for Active Guard/Reserve (AGR) Position dated 20131111 (http://dmva.alaska.gov/employment.htm) (Cannot use outdated NGB 34-1)
2. CURRENT Records Review RIP available on vMPF (http://www.afpc.randolph.af.mil/vs) (Must be a full RIP)
3. CURRENT PASSING Report of Individual Fitness from Air Force Fitness Management Systems (AFFMS) or AF Fitness Assessment Scorecard or a signed letter from the Unit Fitness Monitor.
4. Items requested in the "PREFERED QUALIFICATIONS" section above.
   - Resume
   - Cover Letter
   - Last 3 EPR's/NCOER's
   - Letter of Recommendation

EMAILING REQUIREMENTS:
Ensure all requirements are consolidated into ONE single PDF (adobe portfolio is not recomended)
PDF File Name should be: Position Announcement Number, Last name, First name, Grade
Example: ANG 18-XX Doe, Jane E1
Email Subject should be: Position Announcement Number
Example: ANG 18-XX
Email Application Package to ng.ak.akarng.mbx.hro-agr@mail.mil

** Applications will not be accepted through AMRDEC**

QUESTIONS:
To verify receipt of application or have issues, you may call DSN 317-384-4467 or Commercial 907-428-6467 and/or DSN 317-384-4242 or Commercial
907-428-6242

INSTRUCTIONS TO COMMANDERS/SUPERVISORS: This position vacancy announcement will be given the broadest possible dissemination. A copy of this announcement will be posted on your unit/activity bulletin board. Selecting supervisor will contact qualified applicants for interviews. After the Human Resources Officer (HRO) approves the selection package, the HRO office will send a notification letter to all applicants of their selection/non-selection. The selection of an applicant is not final until the individual has been notified by the HRO-AGR. After the selecting supervisor makes a selection, the “routing” of the selection package begins and ends with HRO.

THE ALASKA NATIONAL GUARD IS AN EQUAL OPPORTUNITY EMPLOYER
All applicants will be protected under Title VI of the Civil Rights Act of 1964. Eligible applicants will be considered without regard to race, age, religion, marital status, national origin, political affiliation or any other non-merit factor. Due to restrictions in assignment to certain units and AFSC/MOS some positions may have gender restrictions.

AFSC 3D073, Craftsman
AFSC 3D053, Journeyman
AFSC 3D033, Apprentice
AFSC 3D013, Helper

★CYBER SURETY
★ (Changed 31 Oct 17)

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.
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.

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:

3.4.1. 3D053. Qualification in and possession of AFSC 3D033. Experience performing cybersecurity functions and/or activities.

3.4.2. 3D073. Qualification and possession of AFSC 3D053. Experience supervising cybersecurity functions and/or activities 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, individual must maintain local network access IAW AFMANs 17-1201, *User Responsibilities and Guidance for Information Systems* and 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 Management Level I 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 security clearance has been granted according to AFI 31-501.