



# ALASKA NATIONAL GUARD

ACTIVE GUARD RESERVE (AGR)

Announcement Number: AKANG 25-040

<b>POSITION TITLE:</b> Fixed Cyber Operations Crew, NCOIC	<b>AFSC</b> 1D771Q	<b>OPEN DATE:</b> 16 Dec 2024	<b>CLOSE DATE:</b> 15 Jan 2025
--	-----------------------	----------------------------------	-----------------------------------

<b>UNIT OF ACTIVITY/DUTY LOCATION:</b> 176th Communications Squadron, Joint Base Elmendorf Richardson, Alaska	<b>GRADE REQUIREMENT:</b> <b>Min:</b> E-5 <b>Max:</b> E-6
--	--

<b>SELECTING SUPERVISOR:</b> TSgt Ferss A. Corbett	<b>Position Number</b> 1097519
---	-----------------------------------

### AREAS OF CONSIDERATION

- On-board AK ANG AGR (Any AFSC)
- Alaska Air National Guard members (Must hold advertised AFSC)
- Alaska Army National Guard members (Must Hold Advertised MOS)
- Nationwide military members eligible for membership in the AKANG (Must Hold advertised AFSC or Equivalent)

### MAJOR DUTIES

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: E: 60
  - PULHES: 3 3 3 2 3 2
  - Strength requirement: Demonstrated ability to lift 40 lbs

### PREFERRED QUALIFICATIONS

The 176 CS Fixed Cyber Operations Crew NCOIC will be responsible for managing a team of 5 Airmen in providing enterprise IT services to the 176 WG, including CST support and network infrastructure installations. In accordance with AKNGI 1320.14 (26 Jun 2020) & ANGI 36-101, the following documents have been requested by the Selection Official. Applications received that do not contain these requested items will not be screened-out by HRO; but it may adversely affect the selection.

1. Resume
  2. Cover Letter
  3. Last three (3) EPBs/EPRs
  4. At least 1 letter of Recommendation
- Current Security + Certification attached to application
  - IT Customer service experience
  - Prior Information Technology experience or related skills
  - Strong administrative and organization skills
  - Supervisory experience
  - Personal initiative
  - Detail oriented
  - Effective organization skills

## ACTIVE GUARD AND RESERVE REQUIREMENTS

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 24 months prior to the start date of the AGR tour. Enlisted Airmen who are voluntarily assigned to a position which would cause an overgrade must indicate such in writing; a voluntary demotion letter must be included with the application 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 Administrative Demotion statement. 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 applicant. Any further questions regarding the AGR program may be answered in AKNGI 1320.14 (26 Jul 2020) & ANGI 36-101.

## SPECIAL ANNOUNCEMENT CRITERIA

- Selection into [ E8 / E9 / O4 / O5 ] positions is contingent on availability/state allocation of controlled grades.
- Selection into higher graded positions IS NOT a promise of promotion
- Upon selection additional medical verification will be required prior to start of AGR tour
- Any Individual(s) selected for this position must meet EFMP requirements for the duty location at time of assignment.
- Members that do not meet EFMP standards for the duty location may be subject to a rescinded offer of employment.
- Continuation beyond initial tour may be subject to evaluation based on AGR Continuation Board

## APPLICATION PROCEDURES

Applications must be signed and dated. Applications received with an unsigned NGB 34-1 will not be forwarded for consideration. Per ANGI 36-101, the application package must include at a minimum items 1-3 listed below. 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/ang-employment/>)
2. CURRENT full Records Review RIP from Virtual MPF <https://vmpf.us.af.mil/vMPF/Hub/Pages/Hub.asp>
3. CURRENT PASSING Report of Individual Fitness from MyFSS/MyFitness <(must not show a "fitness due date" that is in the past) (or) a signed letter from the UFPM. If exempt, please include Form 469 with application)
4. Items requested in the "PREFERRED QUALIFICATIONS" section above.

### EMAILING REQUIREMENTS:

Ensure all requirements are consolidated into ONE single PDF (adobe portfolio is not recommended) (consider printing signed documents to PDF prior to combining files)-Signatures may be stripped once they are saved. PDF File Name should be: Position Announcement Number, Last name, First name, Grade

Example: ANG 25-XX Doe, Jane E1

Email Subject should be: Announcement Number

Example: ANG 25-XX

Email Application Package to: [ng.ak.akarng.mbx.hro-agr@ARMY.mil](mailto:ng.ak.akarng.mbx.hro-agr@ARMY.mil)

\*\* Applications will be accepted through DoD SAFE if standard email procedures do not work\*\*

- DoD SAFE <https://safe.apps.mil/>

IF A PASSPHRASE IS CREATED, YOU MUST ENSURE TO INCLUDE THAT IN THE NOTE SECTION PRIOR TO SUBMISSION.

\*\*All application documents must be consolidated into a single .pdf file. (Do not put in a PDF Portfolio format)

QUESTIONS: Applicants may call HRO for initial review of application and to verify receipt prior to closeout date. DSN 317-384-4467 or Commercial 907-428-6467 or DSN 317-384-4247 or Commercial 907-428-6247. Assistance will be rendered in the order the request was received.

**INSTRUCTIONS TO COMMANDERS/SUPERVISORS:** 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 the Hiring Official who will in turn notify all applicants of their selection/non-selection. The selection of an applicant is not final until the Hiring Official has been notified by of approval by the HRO-AGR Manager.

### 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, color, religion, gender, national origin, or any other non-merit factor. Due to restrictions in assignment to certain units and AFSC/MOS some positions may have gender restrictions.

AFSC 1D771, Craftsman  
 AFSC 1D751, Journeyman  
 AFSC 1D731, Apprentice  
 AFSC 1D711, Helper

## ★CYBER SYSTEMS OPERATIONS

(Changed 31 Oct 24)

1. ★**Specialty Summary.** Manages and performs Cyber Systems Operations and other cyber functions (DoDIN operations) in garrison and in deployed environments. Surveys, secures, protects, defends, preserves, designs, builds, operates, and extends data, networks, net-centric capabilities, and other designated systems. This Air Force Specialty Code incorporates the use of DoD Cyber Workforce Framework (DCWF) Codes to tie this specialty to the framework. The DCWF was developed by the National Institute of Standards and Technology (NIST) and the DoD to establish a common lexicon and model for all cyber work. The DCWF will universalize training and education between academia, industry, and military. It will also enable talent management by ensuring the right Airmen, for the right assignment, at the right time. Cyber, communications and Information Technology capabilities critically underpin all Air and Space Force core missions. The delivery of operationally focused governance and investment to drive sustainability and reliability for this domain is a warfighting necessity. This drives the Department of the Air Force (DAF) forward with real actions which enables modernizing and achieving the cyber posture required to meet pacing challenges. This fully mission capable model develops Airmen that can complement multiple work roles and build technical experts by using the advanced competency levels.

### 2. ★**Duties and Responsibilities:**

2.1. The available duties and responsibilities can encompass:

2.2. Enterprise Operations delivers enduring cyber mission capabilities. Enterprise Operations includes all applicable statutes, but specifically the designing, building, provisioning, maintaining, and sustaining information systems, including warfighter communications, within the Department of the Air Force (DAF). The Department of Defense Information Network (DoDIN) operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DoD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DoDIN's digital terrain and physical infrastructure.

2.3. ★**Cybersecurity** secures, defends, and preserves data, network, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions to protect DoDIN systems to execute DAF operations. Enforces national, DoD and Air Force security policies and directives to ensure Confidentiality, Integrity, and Availability (CIA) of Information Systems (IS) resources. Operations include identifying, locating, and eliminating identified vulnerabilities that compromise the security of the communications, information, electromagnetic environment, or industrial systems through protective measures. Oversees and governs the overall cybersecurity program to include Information Security (INFOSEC), TEMPEST, Communications Security (COMSEC), Emissions Security (EMSEC), and Computer Security (COMPUSEC) programs. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities.

2.4. Data Operations enables data driven decisions through delivering the employment of information operations and software development methodologies. Operations modernizes and enhances warfighter and weapon system/platform capabilities through the rapid design, development, testing, delivery, and integration of reliable, secure mission-enabling systems. Operates and maintains automated data solutions designed to aggregate, secure and display mission relevant data to facilitate rapid data driven decisions.

2.5. Expeditionary Communications delivers cyber capabilities in austere and mobile environments. Expeditionary Communications includes all applicable statutes, but specifically datalinks, the building, operating, maintaining, securing, and sustaining of tactical and communications networks when needed to support warfighter requirements, systems employed in austere, mobile, and/or expeditionary environments, to provide command and control in support of Air and Space Force missions.

### 3. ★**Specialty Qualifications:**

3.1. ★**Knowledge.** Knowledge is mandatory: of principles, technologies, capabilities, limitations, and cyber threat vectors of servers, clients, operating systems, databases, networks and related hardware and software. Cybersecurity principles include; national and international laws, policies, and ethics related to operational cybersecurity; operational risk management processes; and specific operational impacts of lapses in cybersecurity. Radio propagation factors along with understanding regulations governing use of the electromagnetic spectrum. The installation and maintenance management functions include; wire transmission principles; electrical and light wave communications; antenna fundamentals, and cable testing procedures.

3.2. **Education.** For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses in Science, Technology, Engineering, and Mathematics (STEM) are desirable. Associate degree or higher in related fields and/or Information Technology (IT) certification is desirable.

3.3. **Training.** For award of the 1D731X, completion of the suffix-specific course is mandatory.

3.4. **Experience.** The following experience is mandatory for award of the AFSC indicated:

3.4.1. There are no specific upgrade requirements for the slick AFSC 1D7X1 not already defined in the training AFI.

3.4.2. ★For award of the 1D751X, qualification in and possession of 1D731X, or 1D733X and experience in suffix specific functions.

3.4.3. For award of the 1D771X, qualification in and possession of 1D751X and experience in suffix specific functions.

- 3.4.4. ★For award of the 1D791, qualification in and possession of 1D77XX and experience managing and directing cyber activities.
  - 3.5. Other. The following are mandatory as indicated:
    - 3.5.1. For entry into this specialty:
      - 3.5.1.1. See attachment 4 for additional entry requirements.
      - 3.5.1.2. Prior qualification of attaining and maintaining an Information Assurance Technical Level II or Information Assurance Manager Level I cybersecurity certification IAW DAFMAN 17-1303, *Cybersecurity Workforce Improvement Program* for retraining can waive minimum ASVAB requirements.
    - 3.5.2. For award and retention of these AFSCs:
      - 3.5.2.1. Must attain and maintain a minimum cybersecurity baseline certification based on position requirements IAW DAFMAN 17-1303, *Cybersecurity Workforce Improvement* as specified by AFSC shred and/or work role SEI:
      - 3.5.2.2. For 1D7X1X, a minimum certification level is based on position requirements, or a minimum of an Information Assurance Technical Level II certification or Information Assurance Manager Level I certification.
      - 3.5.2.3. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security*.
    - 3.5.3. Specialty requires routine access to classified information, systems, missions, and environments to include but not limited to Sensitive Compartmented Information Facilities (SCIF), Airborne platforms, Agile Combat Employment, Nuclear Command Control & Communications (NC3), and a multitude of emerging mission requirements in a highly contested domain IAW DoDM 5200.01-DAFMAN 16-1405.
      - 3.5.3.1. Must maintain & sustain highest security clearance level received up to Top Secret (Tier 5) or based on current position requirements.
      - 3.5.3.2. Completion of a background investigation according to DoDM 5200.01 - DAFMAN 16-1405, *Personnel Security Program Management*, is mandatory.
- NOTE:** Award of the 3-skill level without a completed investigation is authorized provided minimum of interim Tier 5 (Top-Secret) clearance has been granted according to DoDM 5200.01 - AFMAN 16-1405.

4. ★\*Specialty Shreds:

<i>Suffix</i>	<i>Portion of AFS to Which Related</i>	<i>Suffix</i>	<i>Portion of AFS to Which Related</i>
A	★Network Operations Specialist	P	Data Operations
B	★Systems Administration Specialist	Q	Enterprise Operations
D	★Cybersecurity Technician	R	RF Operations
E	★Technical Support Specialist	W	Expeditionary Communications
K	★Knowledge Management Specialist	Z	★Software Development Specialist
M	★Cybersecurity		

**NOTE:** Suffixes A, B, D, E, K, R sand Z are only applicable to the 3-skill level.

**MANDATORY AFSC ENTRY REQUIREMENTS**

Changed / Effective Date	AFSC	Note(s)	APTITUDE					PHYSICAL PROFILE						OTHER	
			M	A	G	E	X	P	U	L	H	E	S	M	N
31-Oct-18	1A1X2/X	3	60				K	1	1	1	1	2	1		X
31-Oct-19	1A1X3/X	3	60				K	1	1	1	1	2	1		X
31-Oct-24	1A1X4/X	3				65	K	1	1	1	1	2	1		X
31-Oct-18	1A1X8/X	2, 3	60	50			K	1	1	1	1	2	1		X
31-Oct-18	1A8X1/X				72		G	1	1	1	1	2	1	X	X
	1A8X2				72		G	1	1	1	1	2	1	X	X
30-Apr-21	1B4X1					70	G	3	3	3	2	3	1		X
30-Apr-19	1C0X2			50			G	3	3	3	2	3	3		X
31-Oct-16	1C1X1	3			55		G	1	1	1	1	1	1		X
30-Apr-24	1C3X1	2		50	50		G	2	2	2	1	2	1		X
1-Dec-09	1C5X1				55		G	1	1	1	1	1	1		X
31-Oct-21	1C6X1	3				60	G	2	2	2	2	2	1		X
31-Oct-23	1C7X1				50		G	3	3	3	2	3	3		X
30-Apr-23	1C8X3	2	50			65	G	3	3	3	2	3	2		X
30-Apr-23	1D7X1	2 & 4	45			60	G	3	3	3	2	3	2	X	X
30-Apr-23	1D7X2	2 & 4	45			60	G	3	3	3	2	3	3	X	X
30-Apr-23	1D7X3	2 & 4	45			60	L	3	3	1	2	3	1	X	X
30-Apr-22	1H0X1				50		J	1	1	1	1	2	1		X
30-Apr-24	1N0X1	4			G53/G55*		G	3	3	3	2	3	1		X
31-Oct-22	1N1X1A	4			50		G	3	3	3	2	3	1		X
30-Apr-23	1N2X1A	4		64			G	3	2	3	1	2	1		X
30-Apr-23	1N2X1C	1,4		68/64*	67/63*		G	3	2	3	1	2	1		X
31-Oct-22	1N3X1/X	4					G	3	3	3	1	2	1		X
31-Oct-21	1N4X1A	4			62		G	3	3	3	2	2	1		X
31-Oct-21	1N4X2				62		G	3	3	3	2	2	1		X
31-Oct-23	1N7X1	1,4			62/65*		G	3	3	3	2	2	1		X
31-Oct-24	1N8X1	4			67		G	3	3	3	2	3	1		X
31-Jan-11	1P0X1		40				K	2	2	2	2	2	1		X
30-Apr-18	1S0X1			57			G	3	2	2	2	2	1		
	1T0X1	3			55		K	1	1	1	1	2	1		X
31-Oct-19	1U1X1	1			64	54	K	1	1	1	1	2	1		X
	1W0X1	2			66	50	H	2	3	1	2	2	1	X	X
31-Oct-21	1Z1X1	3			49		K	1	1	1	1	1	1	X	X
31-Oct-21	1Z2X1	3			49		K	1	1	1	1	1	1	X	X
31-Oct-24	1Z3X1	3			49		K	1	1	1	1	1	1	X	X
31-Oct-21	1Z4X1	3			49		K	1	1	1	1	1	1	X	X
30-Apr-24	2A2X1					65	J	3	3	3	1	3	2	X	X
	2A3X3E		47				K	3	3	3	1	3	2		X
1-Aug-12	2A3X3L		47				K	3	3	3	1	3	2		X
1-Aug-12	2A3X3M		47				K	3	3	3	1	3	2		X
30-Apr-24	2A3X4A					65	K	3	3	3	2	3	2		X