AGR VACANCY ANNOUNCEMENT
ENLISTED

THE ADJUTANT GENERAL
NEW MEXICO AIR NATIONAL GUARD
ATT: NMANG-HR-AD
47 BATAAN BLVD
SANTA FE, NM 87508

ANNOUNCEMENT NO:
NME 25-010

OPENING DATE
5-June-25

CLOSING DATE
26-June-25

POC: MSgt. Alejandro Unale
COMM: (505) 846-1290
DSN: 246-1290
Alejandro.unale@us.af.mil

OPEN FOR FILL

X	STATE	X	NMANG
	NATIONWIDE		NMARNG

POSITION TITLE: Policy and Evaluation.

LOCATION OF POSITION: Joint Force Headquarters, New Mexico Air National Guard, Kirtland Air Force Base, New Mexico 87117.

AREA OF CONSIDERATION: Open to all members of the New Mexico Air National Guard. In the grade of E-5 to E-7. Willing to cross train into 3F0X1 AFSC Immediatley.

DATE VACANCY EXISTS: Currently with a projected start date of 7 July 2025 TBD by Commander.

ELIGIBILITY REQUIREMENTS TO QUALIFY FOR AGR TOUR:

Enlisted must meet AFSC, requirements as outlined in AFECD. If medical exam is older than 30 days, applicant must submit an AF Form 895. Submit applications on NGB Form 34-1. Must meet the physical examination qualification outlined in Chapter 12, ANGI 36-101, and IAW AFI 48-123 Medical Examination and Standards. Examination must have been conducted within 18 months before the date of entry on military duty. Must meet and comply with weight standards at the time of entry into AGR duty. Should be able to acquire 20 years of active duty prior to mandatory separation date. Should be able to serve at least five (5) consecutive years in the AGR program prior to becoming eligible to receive military non-disability retirement or retainer pay. Must not be eligible for, or receiving an immediate Federal (military or civilian) retirement annuity.

SPECIAL INFORMATION: As a condition of employment, **selected** agrees to attend all Unit Training Assemblies and Annual Training deployments, special projects, and exercises when required, with his/her unit of assignment; applicant must be assigned to a Military UMD in the unit they support and UMD compatible AFSC prior to Active Duty Tour. The military uniform will be worn in accordance with AFI 36-2903.

INSTRUCTIONS FOR APPLYING: Submit application using a NGB Form 34-1, which is on the internet at https://usaf.dps.mil/sites/34163/150SOW/JOBS/SitePages/Home.aspx. Completed applications will be scanned into one PDF file and emailed to alejandro.unale@us.af.mil **no later than** the closing date. You must submit a separate PDF file for each job you are applying for.

REQUIRED DOCUMENTS: All applications must include the following documents:
Completed NGB 34-1
Current Record Review RIP (not more than one (1) year old)
Current copy of your Official Air Force Fitness Assessment Scorecard.

EQUAL OPPORTUNITY: The New Mexico Air National Guard is an Equal Opportunity Organization. Selection for this position will be made without regards to race, color, religion, sex, age, or national origin.

CLOSING DATE: Applications will be forwarded to the HRO office, to arrive **no later than** the business day on the closing date specified on the vacancy announcement.

CYBER SYSTEMS OPERATIONS

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 industrials 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.

Performs additional duties as assigned.
Note: Incomplete packages will not be considered.