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 22-027

OPENING DATE
21-Dec-22

CLOSING DATE
20-Jan-23

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

OPEN FOR FILL

	STATE	**X**	**NMANG**
	NATIONWIDE		**NMARNG**

POSITION TITLE: Cyber Defense Ops

LOCATION OF POSITION: 250th Intelligence Squadron New Mexico Air National Guard, Kirtland Air Force Base, New Mexico 87117.

AREA OF CONSIDERATION: Open to all members of the 150th New Mexico Air National Guard. Eligible up to the rank of E-5. Must hold 1D751B or 1D751A AFSC.

DATE VACANCY EXISTS: Currently with a projected start date of TBD.

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 DEFENSE OPERATIONS

1. Specialty Summary. Manages and performs Defensive Cyber Operations (DCO) and cyber support functions (DoDIN operations) in- garrison and at deployed locations. Surveys, secures, protects, defends, preserves, designs, builds, operates, and extends data, networks, net-centric capabilities, and other designated systems. This Air Force Specialty Code description incorporates the use of DoD Cyber Workforce Framework (DCWF) Codes to tie this specialty description 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.

2. Duties and Responsibilities:
2.1. Responds to disruptions within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches to maximize survival of life, preservation of property, and information security. Investigates and analyzes relevant response activities and evaluates the effectiveness of and improvements to existing practices. [DCWF Code – 531]
2.2. Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware, software, and documentation that are required to effectively manage network defense resources. [DCWF Code – 521]

2.3. Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Uses data collected from a variety of cyber defense tools (e.g., Intrusion detection system alerts, firewalls, network traffic logs.) to analyze events that occur within their environments for the purposes of mitigating threats. [DCWF Code – 511]
2.4. Conducts threat and vulnerability assessments and determines deviations from acceptable configurations or policies. Assesses the level of risk and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. Performs assessments of systems and networks within the Network Environment (NE) or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. [DCFW Code – 541]
2.5. Collects, processes, preserves, analyzes, and presents computer-related artifacts in support of network vulnerability mitigation [DCWF Code – 211]
2.6. Performs and supports cyber mission Planning, Briefing, Execution, and Debriefing (PBED). Identifies, validates and synchronizes resources to enable integration during the execution of defensive cyber operations. [DCWF Code - 332]
2.7. Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include Communications Security (COMSEC), Emissions Security (EMSEC), Computer Security (COMPUSEC), personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources. Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives. [DCWF Code 612, 722, 723]
2.8. Installs, configures, troubleshoots, and maintains server and systems configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Administers server-based systems, security devices, distributed applications, network storage, messaging, and performs systems monitoring. Consults on network, application, and customer service issues to support computer systems' security and sustainability. [DCWF Code – 451]
2.9. Manages and administers integrated methods, enabling the organization to identify, capture, catalog, classify, retrieve, and share intellectual capital and information content. The methods may include utilizing processes and tools (e.g., databases, documents, policies, procedures) and expertise pertaining to the organization. [DCWF Code – 431]
2.10. Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices. Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results. Utilizes on the development process of the system development lifecycle. Makes daily product decisions, works on a collaborative team, pairs with team members, and helps ensure user satisfaction using Lean and Agile methodologies. Works with the project team, leadership, stakeholders, and other PMs to progress the goal of shipping the right product to users. Ensures that the product is successful in terms of user value, stakeholder value, and organizational business goals.
[DCWF Code – 621, 622, 632]

2.11. Consults with stakeholders to guide, gather, and evaluate functional and security requirements. Translates these requirements into guidance to stakeholders about the applicability of information systems to meet their needs. [DCWF Code - 641]
2.12. Develops, administers, and secures databases, data management systems, and/or data processes for the storage, query, and utilization of data. Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. Locates patterns in large data sets using computer science techniques to help team members with different levels of understanding and expertise to make data driven business decisions that increase effectiveness or efficiency of operational forces. [DCWF Code – 421/422]
2.13. Provides end users tiered-level customer support by coordinating software, hardware, and network configuration, troubleshooting, resolution, security, maintenance, and training. [DCWF Code – 411]
2.14. Deploys, sustains, troubleshoots and repairs standard radio frequency wireless, line-in-sight, wideband, and ground-based satellite and encryption transmission devices in a fixed and deployed environment. Included are multiple waveform systems. Establishes and maintains circuits, configures and manages system and network connectivity.

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 including; national and international laws, policies, and ethics related to operational cybersecurity; operational risk management processes; and specific operational impacts of lapses in cybersecurity.
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 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 defense activities.
3.5.4. Other. The following are mandatory as indicated: 3.5.4.1. For entry into this specialty:
3.5.4.1.1. See attachment 4 for additional entry requirements. 3.5.2. For award and retention of these AFSCs:
3.5.2.1 Must attain and maintain a minimum Information Assurance Technical Level II certification IAW AFMAN 17-1303, *Cybersecurity Workforce Improvement Program* and DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, as specified by AFSC shredout:
3.5.2.1.1. For 1D7X1, a minimum of position requirements.

3.5.2.1.2. For 1D7X1A, a minimum Information Assurance Technical Level II certification.
3.5.2.1.3. For 1D7X1B, a minimum Information Assurance Technical Level II certification.
3.5.2.1.4. For 1D7X1D, a minimum Information Assurance Management Level I certification.
3.5.2.1.5. For 1D7X1E, a minimum Information Assurance Technical Level II certification.
3.5.2.1.6. For 1D7X1K, a minimum of position requirements.
3.5.2.1.7. For 1D7X1R, a minimum of position requirements.
3.5.2.1.8. For 1D7X1Z, a minimum of position requirements.
3.5.2.2. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security*.
3.5.2.34. Completion of a background investigation according to AFMAN 16-1405, *Personnel Security Program Management*, is mandatory by AFSC shredout specified:
3.5.2.3.1. For 1D7X1,
3.5.2.3.2. For 1D7X1A, completion of a current Tier 5 (T5), Top Secret.
3.5.2.3.3. For 1D7X1B, completion of a current Tier 5 (T5), Top Secret.
3.5.2.3.4. For 1D7X1D, completion of a current Tier 5 (T5), Top Secret.
3.5.2.3.5. For 1D7X1E, completion of a current Tier 3 (T3), Secret.
3.5.2.3.6. For 1D7X1K, completion of a current Tier as specified by position requirements.
3.5.2.3.7. For 1D7X1R, completion of a current Tier 3 (T3), Secret.
3.5.2.3.8. For 1D7X1Z, completion of a current Tier 5 (T5), Top Secret.
NOTE: Award of the 3-skill level without a completed Tier 5 Investigation is authorized provided an interim Top Secret clearance has been granted according to AFMAN 16-1405.

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