District of Columbia Air National Guard

AGR Announcement

25-167

APPLICATION MUST BE FORWARDED TO: IN ORDER TO RECEIVE CONSIDERATION **113WG.DCANG.APPLICATIONS@US.AF.MIL**	**OPENING DATE:** 14 August 2025	**CLOSING DATE:** 28 August 2025
	Position Title: Security Operations **Max Grade:** MSgt (E7) **Min Grade:** SSgt (E5) **AFSC:** Any, must have score 60 in category "E" on ASVAB **Tour:** Permanent	
	Appointment Status [X] **Enlisted** [ ] **Officer**	
Position Location: 113th Communications Squadron Joint Base Andrews, MD 20762	**AREA OF CONSIDERATION: GROUP I** Current DCANG AGR members.	

INSTRUCTIONS FOR APPLYING:

This office will **NOT** accept mailed applications. You must send applications electronically. **Failure to submit all required documents as outlined below will result in your application not being considered for employment.**

AGR REQUIRED DOCUMENTS:

1.) NGB 34-1 (***dated Nov 2013***) Application for AGR Position. https://www.ngbpmc.ng.mil/Forms/NGB-Form/
2.) Copies of last three EPRs/EPBs.
3.) Resume *(any format).*
4.) 3 References on a separate sheet of paper with email address and additional point of contact number(s).
5.) Report of Individual Personnel (RIP) from vMPF only *(must be dated within 60 days).* If clearance is expired, you must obtain security memo from the Wing security manager.
6.) Current Fitness Test from myFitness *(Per DAFI 36-2905 – current within 12 months, handwritten scorecards are not accepted).*
7.) Letter(s) of recommendation *(optional).*
8.) If missing documents, memo to board president required stating reason why documents are missing.

****All documents must be consolidated into a single pdf file**. *DO NOT put in PDF Portfolio format. Save applications in the following format:* ***MVA number, Rank, Last name, First name, Middle Initial**. Ex: 20-300 – SSGT DOE, JOHN A*
Email subject will be in the same format.

Conditions of Employment:

Electronic Funds Transfer: Selectee is required to participate in electronic funds transfer/direct deposit.
If applying for an MVA at a lower rank, a voluntary demotion memorandum stating action must be submitted.

Evaluation Process: Applicants will be evaluated solely on information supplied in application documents outlined above. Interview responses will also be considered when applicable. Incomplete applications will not be considered. It is the responsibility of the applicant to contact the POC identified on this vacancy announcement prior to the vacancy closing date to verify all documents have been received. Failure to do so may result in disqualification. Complete and accurate data is essential to ensure fair evaluation of candidates.

Equal Employment Opportunity: All qualified applicants will receive consideration for this announcement without regard to race, color, gender, religion, national origin, or membership/non-membership in an employee organization. Reference: NGR AR 690-600 / NGR AF 40-1614. CNGBI 9601.01 and ANGI 36-7

The District of Columbia Air National Guard

DC is an Equal Opportunity Affirmative Action Employer
This announcement must be posted on unit bulletin boards until the day following the closing date.

Announcement Number: 25-167

Position: Security Operations

Position Description:

This position is located at an Air National Guard Communications Group or in the Base Communications Squadron. The purpose of this position is to serve as the unit Information Assurance Specialist during day-to-day in-garrison planning and execution of information assurance and to serve as planner for deployed operations requiring the same. The incumbent administers the communication-computer security and awareness training programs. The position performs duties necessary to accomplish information security functions in support of programs essential to Combat Communications Group or Squadron operations, training, and readiness missions.
Serves as the Computer Security (COMPUSEC) Manager. Protects and maintains the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle. Establishes and publishes squadron policy to manage the COMPUSEC program. Disseminates information and ensures computer security practices are adhered to by all functional areas in-garrison and in support of deployed war-fighting personnel. Reviews, analyzes, and validates, and provides guidance for certification and accreditation packages. Continuously identifies and analyzes threats and vulnerabilities to the information systems to maintain an appropriate level of protection. Accomplishes risk analysis and certification due to modifications or changes to computer systems. Certifies all software prior to installation and use on communications and computer systems. Executes computer security plans and enforces mandatory access control techniques such as trusted routers, gateways, firewalls, or other methods of information systems protection. Manages the Information Assurance Program. Implements procedures to ensure protection of information transmitted to the squadron, among units in the squadron, and from the squadron units using local or wide area networks, the worldwide web or other communications modes. Utilizes the most current multi-level security products available to provide data integrity, confidentiality, authentication, non-repudiation, and access control of the Local Area Network (LAN). Reports to Major Command (MAJCOM), Air Force Communications Agency (AFCA), National Security Agency (NSA), and Air Force Computer Emergency Response Team (AFCERT) all incidents involving viruses, tampering, or unauthorized system entry. Controls access to prevent unauthorized persons from using network facilities. Limits access to privileged programs (i.e., operating system, system parameter and configuration files, and databases), utilities, and security-relevant programs/data files to only authorized personnel. Implements methods to prevent or minimize direct access, electronic or other forms of eavesdropping, interpreting electro-mechanical emanations, electronic intercept, telemetry interpretation, and other techniques designed to gain unauthorized access to Automated Data Processing (ADP) information, equipment, or processes. Recognizes such potential, defines vulnerabilities and oversees the installation of physical and technical security barriers to prevent others from improperly obtaining such information. Serves as the Communications Security (COMSEC) Manager for all cryptographic activities including managing the Cryptographic Access Program (CAP). Formulates and develops communications security criteria and requirements for inclusion in mobility, contingency, and exercise plans. Responsible for ensuring the protection of COMSEC materials and to determine and enforce limited access of such materials to proper individuals based on training, clearance and a need to know. Implements procedures to ensure the safeguarding and accounting of all COMSEC materials received, distributed, shipped, stored, and destroyed; conducts inventories on all COMSEC materials including hardware, keying material, maintenance manuals and reports results to Central Office of Record; and maintains COMSEC accounting and related records. Briefs staff members requiring access to administrative COMSEC information and material. Prepares and evaluates written plans for emergency actions and ensures personnel are fully qualified in the execution of plans. Investigates security incidents to determine the possibility of compromise to COMSEC materials and ensures documentation and reporting to appropriate channels. Performs semi-annual functional reviews of all COMSEC user accounts, physically inspecting the user's COMSEC facilities, reviewing procedures, and audits all cryptographic holdings. Documents and forwards cryptographic access certificates and acts as liaison for scheduling polygraph examinations of personnel enrolled in the program. Implements and manages the electronic key management system program. This includes system configuration and operation of the Local Management Device/Key Processor (LMD/KP) to the Data Transfer Device (DTD) or Simple Key Loader (SKL). Initializes the system, performs

system backups, determines operator access, and control functions (privilege management), reloads and configures the operating system's parameters. Installs or oversees installation of local COMSEC account hardware and software, including training alternates in the electronic key management system operations. Serves as secure voice (such as STU-III/STE) representative and Emissions Security Program (EMSEC) administrator. Develops, implements, and monitors security systems for the protection of controlled cryptographic cards, documents, ciphers, devices, communications centers, and equipment. Validates strapping and configuration options of cryptographic units as required. Ensures Information Assurance (IA) awareness information is available to all information system users, including all tenants and geographically separated units. Provides technical training and instruction on Information Awareness training program procedures to supervisors, employees, and/or unit security representatives. Utilizes computer-based training for both initial and recurring information protection training. Conveys the degree of reliance on information systems, the potential consequences arising from the lack of secure information systems, the organization's commitment to secure information systems, and the means by which users can protect information systems. Conducts annual COMSEC training for unit COMSEC users. Uses a wide variety of formal training materials, such as outlines, handouts, publications, films, exhibits, protective devices, and visual aids to provide and/or reinforce information related to communications-computer systems security awareness practices. Promotes security campaigns through oral presentations at local security committee meetings; and extracts, compiles, and prepares security articles, bulletins, and pamphlets for local use by unit personnel. Maintains required course records. Develops, implements and maintains work center training programs. Plans and schedules tasks and training activities for drill status guard members. Oversees and conducts on-the-job training (OJT) for personnel. Creates and develops lesson plans. Ensures availability of facilities and training aids. Monitors the training status of personnel and ensures that supplemental and/or remedial training is accomplished. Responsible for documentation of accomplished training in a timely manner. Uses automated training documentation system as required. Assists unit personnel with duties involving a wide range of communications and information systems and communications programs consisting of tactical communications equipment, LAN systems, information resource management, and information protection programs. Perform other duties as assigned.

Minimum Qualification Requirements:

1. Must be current DCANG AGR member.
2. Must have Secret security clearance.
3. Must cross train into 1D7X5 within 12 months of starting position.

Eligibility Requirements:

1. Applicants who have been separated for cause from active duty or a previous AGR tour are ineligible.
2. Prior to entry into the AGR Program, member must be medically cleared by the 113th Medical Group.
3. Must meet all eligibility requirements in accordance with ANGI 36-101.

AGR Employment Points of Contact:

AGR NCOIC: MSgt Victoria McNamara, Victoria.McNamara@us.af.mil, 202-685-8813 (DSN 325-8813)