



# District of Columbia Air National Guard

## AGR Announcement

### 14-357



<p><b>APPLICATION MUST BE FORWARDED TO:</b>          Human Resource Office          DC National Guard          2001 East Capitol Street          Washington, DC 20003-1719</p> <p><b>IN ORDER TO RECEIVE CONSIDERATION APPLICATION MUST BE RECEIVED BY 1530 EST ON CLOSING DATE OF THIS ANNOUNCEMENT</b></p>	<p><b>OPENING DATE:</b> 16 October 2014</p>	<p><b>CLOSING DATE:</b> 30 October 2014</p>
	<p><b>Position Title:</b> IT Specialist (INFOSEC)  <b>Applicant Max Grade:</b> E8  <b>Applicant Min Grade:</b> E7</p>	
	<p><b>Selectee will be assigned to a compatible military position of:</b> 3DXXX</p>	
<p><b>Position Location:</b>          113<sup>th</sup> Communications Flight          Joint Base Andrews, MD</p>	<p><b>Appointment Status</b>  <input checked="" type="checkbox"/> Enlisted    <input type="checkbox"/> Officer</p>	
<p><b>AREA OF CONSIDERATION:</b></p> <p style="text-align: center;"><b>GROUP I</b></p> <p style="text-align: center;">Individuals who are current employed full-time in the DCANG AGR program</p>		
<p><b>Special Remarks:</b> ****APPLICANTS MUST BE FULLY QUALIFIED****</p>		
<p><b>INSTRUCTION FOR APPLYING:</b> This office will not accept applications mailed at government expense. Electronic or fax applications will not be accepted. <b><u>Failure to submit all required documents as outlined below will result in your application not being considered for employment.</u></b></p> <p style="text-align: center;"><b>AGR REQUIRED DOCUMENTS (no binders please):</b></p> <ol style="list-style-type: none"> <li>1.) NGB 34-1 (<i>dated Nov 2013</i>) Application for AGR Position with original signature</li> <li>2.) Separate sheet of paper with email address and additional point of contact number(s)</li> <li>3.) Current RIP (Report of Individual Performance) from <u>vMPF</u>              *Please do not submit a Data Verification Brief (DVB)</li> <li>4.) Recent Fitness Test from AFFMS (Per AFI 36-2905 (<i>current within 12 months</i>))</li> <li>5.) Knowledge, Skills, and Ability (KSA) questions addressed by element on a separate paper.</li> <li>6.) Security Clearance verification memorandum (<i>do not submit a JPAS print out</i>)</li> <li>7.) Letter(s) of recommendation (<i>optional</i>)</li> </ol>		
<p><b>Conditions of Employment:</b></p> <p><u>National Guard Membership:</u> Prior to appointment to this position, selectee must be a member of the District of Columbia Air National Guard.</p> <p><u>Electronic Funds Transfer:</u> Selectee is required to participate in electronic funds transfer/direct deposit.</p>		
<p><b>Evaluation Process:</b> Applicants will be evaluated solely on information supplied in application documents outlined above. Interview responses will also be considered when applicable.</p>		
<p><b>Equal Employment Opportunity:</b> 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, in accordance with NGB Regulation 690-600 and ANGR 40-1614.</p>		

This announcement must be posted on unit bulletin boards until the day following the close date



# District of Columbia Air National Guard



Is an Equal Opportunity Affirmative Action Employer

**Announcement Number:** 14-357

**Position:** IT Specialist (INFOSEC)

**Brief Description of Duties:** Serves as the Wing Information Assurance Manager. Applies Information Technology (IT) security principles, methods, and security products to protect and maintain the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle. Establishes and publishes base-wide policy to manage the INFOSEC (also known as COMPUSEC) program and provides advice and guidance in its implementation and in procedures used in the development and operation of systems. Assists all base organizations in the development of their individual INFOSEC program. Disseminates information and ensures computer security practices are adhered to by all functional areas. Reviews, analyzes, and validates certification and accreditation (C&A) packages. Continuously identifies and analyzes threats and vulnerabilities to the information systems to maintain an appropriate level of protection. Ensures computer software designs address information system security requirements. Accomplishes risk analysis, security testing, and certification due to modifications or changes to computer systems. Evaluates, assesses, or locally tests and approves all hardware, software, and firmware products that provide security features prior to use on any accredited information system or network. Certifies all software prior to installation and use on communications and computer systems. Implements and advises on IT security policies and procedures to ensure protection of information transmitted to the installation, among organizations on the installation, and from the installation using Local Area Networks (LAN), Wide Area Networks (WAN), the World Wide Web, or other communications modes. Utilizes current and future multi-level security products collectively to provide data integrity, confidentiality, authentication, non-repudiation, and access control of the LAN. 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 authorize 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 IT information, equipment, or processes. Conducts the Information Assurance Awareness Program which uses computer-based training for both initial and recurring information protection training. 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. Maintains accountability for sensitive cryptographic materials and related COMSEC information. Oversees issuance of COMSEC materials. Performs other duties as assigned.

**Qualifications:**

1. Must have a SECRET security clearance or be able to obtain one within 6 months.
2. Must be AFSC qualified with minimum aptitude score of A: 47

**Specialized Experience:** Must demonstrate eighteen (18) months experience in which the following Knowledge, Skills and Abilities (KSA's) as described below have been attained.

**Knowledge, Skills and Abilities (KSA's) Statements:**

- A. Knowledge of a full range of IT security principles, methods, regulations, policies, products and services sufficient to develop specifications to ensure compliance with security requirements at the LAN level and to plan and coordinate the delivery of an IT security awareness training program for end users at all levels at the installation.
- B. Knowledge of a full range of IT security requirements for certification and accreditation; network operations and protocols.
- C. Skill to develop and evaluate program documentation to include mission needs statements, operational requirements documents and support plans, specifications.
- D. Ability to serve as the focal point for information security, providing authoritative advice and assistance on complex, technical, controversial, and precedent setting matters to improve the IT security program comprising many unique organizations and large, complex computer and communications security systems.

**Eligibility Requirements:**

1. Applicants who have been separated for cause from active duty or a previous AGR tour are ineligible.
2. Service members whose initial DCNG AGR order places them at 18 years or more of Total Active Federal Military Service (TAFMS) will require a signed and approved sanctuary waiver prior to beginning tour.  
\*This requirement is not applicable to service members with over 18 years TAFMS.
3. Prior to entry into the AGR Program, member must be medically cleared by the 113th, MDG.
4. Must meet all eligibility requirements in accordance with ANGI 36-101

**AGR Employment Points of Contact:**

HR Specialist: TSgt Angel Love-Shorter / angel.d.loveshorter.mil@mail.mil / 202-685-9778 (DSN 325-9778)

AGR Manager: CPT Ryan McBride / ryan.mcbride@us.army.mil / 202-685-9779 (DSN 325-9779) or follow us on  TWITTER @NGDCHRO.

This announcement must be posted on unit bulletin boards until the day following the close date