DISTRICT OF COLUMBIA ARMY NATIONAL GUARD
AGR VACANCY ANNOUNCEMENT

OTOT - NTE 3 Years

ANNOUNCEMENT #: 25-020

All individuals eligible for entry into the DCARNG (Nationwide Announcement)

Position: Cybersecurity Branch NCO Para/Lin: 239A/ 02 Position #00055518		**Minimum Rank/Grade:** SGT/E5	**Maximum Rank/Grade:** SSG/E6
MOS/AOC: 25B	**Unit/Location:** Joint Force Headquarters (JFHQ) DC Armory 2001 E. Capitol St SE Washington, DC 20003	**Opening Date:** 30 May 2025	**Closing Date:** 30 June 2025

DUTIES AND RESPONSIBILITIES:

As a Cybersecurity Branch NCO, you will serve as a critical leader in safeguarding the unit’s information systems and ensuring compliance with Department of Defense (DOD) cybersecurity standards. Your responsibilities will include, but are not limited to:

1. Network Security Management: Monitor, analyze, and secure the unit’s network infrastructure to prevent unauthorized access, data breaches, and cyber-threats. Implement and maintain firewalls, intrusion detection/prevention systems, and other security tools to protect classified and unclassified systems. Conduct regular vulnerability assessments and penetration testing to identify and mitigate potential security weaknesses.

2. Information Assurance and Compliance: Ensure compliance with DOD cybersecurity policies, including the Risk Management Framework (RMF) and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). Maintain and update System Security Plans (SSPs), ensuring all systems are accredited and authorized to operate (ATO). Oversee the implementation of security patches, updates, and configurations to maintain system integrity.

3. Incident Response and Recovery: Lead the response to cybersecurity incidents, including identifying, containing, and eradicating threats in coordination with higher headquarters and external agencies. Conduct post-incident analysis to determine root causes, document lessons learned, and implement preventive measures. Develop and maintain the unit’s Continuity of Operations Plan (COOP) for IT systems in the event of a cyber-attack or system failure.

4. Training and Supervision: Train and mentor junior enlisted personnel in cybersecurity best practices, ensuring they are proficient in their roles as IT and cybersecurity specialists. Conduct regular security awareness training for all unit personnel to promote a culture of cybersecurity and reduce human-related risks (e.g., phishing, social engineering). Supervise daily operations of the cybersecurity team, ensuring tasks are completed efficiently and in alignment with mission objectives.

5. Classified Information Protection: Safeguard Top Secret and other classified information by enforcing strict access controls, encryption standards, and secure communication protocols. Manage the unit’s cryptographic equipment and key material, ensuring proper handling, storage, and accountability in accordance with NSA and DOD regulations. Coordinate with the unit’s Information Assurance Manager (IAM) to maintain compliance with clearance and access requirements for personnel.

6. Collaboration and Reporting: Liaise with higher headquarters, including the Army Cyber Command (ARCYBER) and Joint Force Headquarters (JFHQ), to report cyber-threats, incidents, and readiness status. Provide regular briefings to unit leadership on the state of cybersecurity, including risks, mitigation strategies, and resource requirements. Participate in joint exercises and operations to test and improve the unit’s cyber-defense capabilities.

7. System Administration Support: Assist in the administration of servers, workstations, and communication systems, ensuring they meet security and operational standards. Manage user accounts, permissions, and authentication systems to ensure secure access to resources. Troubleshoot and resolve IT-related issues that impact mission-critical operations.

8. Documentation and Policy Development: Develop and maintain standard operating procedures (SOPs) for cybersecurity operations within the unit. Document all security incidents, audits, and compliance activities for accountability and future reference. Recommend updates to unit policies and procedures to address emerging cyber-threats and technological advancements.

This announcement is for a One-Time Occasional Tour (OTOT) not-to-exceed 3 years.

Mandatory Requirements and Skills at Time of Application:

1. CompTIA Security+ (required for DoD 8570.01-M IAT Level II compliance).
2. Applicant must be able to complete the Military Educational requirements commensurate with their military grade.
3. Must meet the physical requirements of AR 350- 15, AR 600-9, and AR 40-501 and appointment criteria IAW NGR 601-1, NGR 600-100, NGR 600-101, NGR 600-5, and AR 135-18.
4. All applicants grade E-6 must possess the required grade and MOS level authorized for the AGR duty position or take a voluntary reduction in grade to accept the position, if selected and offered and become MOS qualified in the first 12 months or be released from active duty/FTNGD. All applicants grade E-5 must have the potential to become MOS qualified in the first 12 months or be released from active duty/FTNGD.

Documents from Applicant in Addition to AGR Application Checklist (Page 4):

1. None

PREFERRED APPLICANTS WILL POSSESS THE FOLLOWING SKILLS/ATTRIBUTES:

1. Experience with incident response and forensic analysis tools (e.g., Wireshark, Splunk, Nessus) (desired).
2. Proficiency in network security, system administration, and cyber-security operations (firewalls, intrusion detection systems, vulnerability assessment tools).
3. Familiarity with DoD cyber-security frameworks (Risk Management Framework, DISA STIGs).
4. Experience with encryption technologies, secure communications, and cryptographic equipment management (e.g., COMSEC).
5. Certified Information Systems Security Professional (CISSP) or CompTIA Cybersecurity Analyst (CySA+) (recommended).
6. CompTIA Network+ or Cisco Certified Network Associate (CCNA) (recommended).
7. Master's degree in Information Technology, Computer Science, Cybersecurity or related field (recommended).

SPECIAL INSTRUCTIONS:

1.Must not be under current suspension of favorable personnel actions, or have reason to be under current suspension of favorable personnel actions.
2. Current T32 or T10 AGR Soldiers must separate from their current orders and start an Initial Tour with the DCARNG T32 AGR program if selected.
3. All applicants subject to review of Retention Control Points considering their total Active Federal Service years.
4. This announcement is for a One-Time Occasional Tour (OTOT) not-to-exceed 3 years.

EQUAL EMPLOYMENT OPPORTUNITY: All applicants will receive consideration without regard to age, race, color, national origin, creed, religion, politics, marital status, membership/non-membership in an employee organization, or other non-merit reasons not interfering with membership in the Army National Guard or performance of required duties.

POSITIONS OF SIGNIFICANT TRUST (POST): In accordance with DA EXORD 193-14 & NGB SMOM 15-017, all Soldiers hired into sensitive duty positions are required to have favorable POSTscreening. Soldiers not meeting this requirement will not be hired into AGR status.

PAY AND ALLOWANCES/MAJOR BENEFITS: AGR personnel receive base pay, subsistence (BAS), quarter's allowance (BAH), Variable Housing Allowance (VHA), applicable uniform allowances, full medical care in military facilities, and partial medical care and TRICARE benefits for dependents.

ADDITIONAL INFORMATION: Restoration rights for federal employees accepting AGR tours will be in accordance with applicable federal personnel regulations. Personnel in a bonus program should refer to applicable FY SRIP to determine if continuation in SRIP/ SLRP is permitted prior to entry on AGR status. AGR personnel are subject the Uniform Code of Military Justice.

How to Apply

The forms and documents listed on the application checklist must be submitted as **ONE** .pdf file (**do not** submit as PDF Portfolio) through email. Applications and Checklist must be received in the AGR Office no later than 1630 hours (Eastern) on the closing date of the announcement.

1. Email AGR Applications To: ngdcAGRbranch@army.mil

2. The AGR Management team will provide notification that your application has been received.

Applicant's rank/name:
Applicant's Email:

Applicant Status: □ T32 □ T10 □ AGR □ ADOS □ M-Day

AGR APPLICATION CHECKLIST

_____**1.NGB Form 34-1 AGR Application**, can be found under Career Resources at https://www.ngbpmc.ng.mil/Forms/NGB-Forms/ (Include e-mail address at the top 1st page of NGB Form 34-1 and signature on pg 3)

_____**2.Certified Board Selection ERB/ORB.** Within 30 days - must include applicable MOS or AOC and ASVAB Scores.

_____**3.Individual Medical Readiness Record.** Must include current Periodic Health Assessment date and PULHES**.** PHA must be current within 12 months.

_____**4. DA Form 3349 Physical Profile (If Applicable)**. No temporary profiles are accepted except pertaining to pregnancy.

_____**5. DA 5500/ DA 5501 (If Applicable)**

_____**6. Last ACFT for record within the past 6 months.** Either DA 705 with digital signatures or ITR (Individual Training Record) report out of DTMS (Digital Training Management System) *PPOM 22-23 requires passing ACFT within 6 months as of 1 April 2023.

_____**7.DA Form 2166-8 NCOER / DA Form 67-8/9 OERs – last 5 copies.** SPC/E4 or a newly promoted SGT or 1LT (Doesn't have 3 NCOERs/ OERs), will need a letter of recommendation from Unit Commander or BN AO within 6 months of closing of announcement.

_____**8. All DD Form 214's and DD Form 215's** (must have items 23-30 included)

_____**9. NGB Form 23/23b** (Current National Guard Soldier) Retirements Points History Statement (RPAM) (Must be pulled in last 30 days from closing of announcement.)

_____**10. Security Clearance Memo**. Must have a final Security Clearance Verification. Memo from a Security Clearance Manager must be dated within 90 days from date of announcement. NO JPAS printouts.

_____**11. OPAT Scorecard (DA Form 7888)** (Applicable if current PMOS is in a lower physical category than advertised MOS)

_____**12. DA Form 4836/ Oath of Extension of Enlistment or Reenlistment (Required for Enlisted)** (*Applicants must have a minimum of three years on their current contract before HRO will cut AGR/OTOT orders*).

NOTE: PLACE THE JOB ANNOUNCEMENT AS PAGE 1 - ensure that all required documents (As Applicable) on the checklist are in included with your application in the listed order above. Applications that have been returned for correction will need to resubmit complete packets with the corrected documents before job announcement closes in order for their packet to be considered. **It is mandatory that all SMs have a minimum of three years on their current ETS (or required time to cover a OTOT) in order for HRO to produce AGR orders and to complete an AGR Initial Tour.**

Evaluation Process: Applicants will be evaluated solely on the 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 POCs 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.