HUMAN RESOURCES OFFICE
MARYLAND NATIONAL GUARD
219 WEST HOFFMAN STREET
BALTIMORE, MARYLAND 21201-2288
TELEPHONE: (667) 296-3498

POSITION VACANCY ANNOUNCEMENT 25-038a

Open Date: 19 February 2025 **Close Date: 20 March 2025**

FULL TIME MILITARY / ACTIVE GUARD RESERVE (AGR) POSITION VACANCY

BRANCH OF SERVICE: AIR NATIONAL GUARD (ANG)

POSITION TITLE: CYBER WARFARE OPERATION/ CYBER INTELLIGENCE (1B4X1) (1N4X1A)

HIGHEST GRADE AUTH PER ANGI 36-101, AGR/MIL TECH GRADE COMPARABILITY TABLE: MSgt/E7

UNIT MANNING DOCUMENT-GUARD GRADE/ POSITION AVAILABLE: MSgt/E7

ORGANIZATION/LOCATION: 276th Cyberspace Operations Squadron, MDANG, 2701 Eastern Boulevard, Middle River, Maryland 21220-2801

SALARY: Full Military Pay and Allowances, depending on rank and longevity of selectee

WHO MAY APPLY: OPEN TO CURRENT MEMBERS OF THE MARYLAND AIR NATIONAL GUARD AND THOSE ELIGIBLE TO BECOME MEMBERS.

QUALIFICATION/ELIGIBILITY REQUIREMENTS

1. Refer to ANGI 36-101, The Active Guard/Reserve Program, for general eligibility requirements for initial entry into the AGR Program and specific guidelines for utilization, and assignment of currently on-board AGR members.
2. Applicants must meet the physical qualifications outlined in AFI 48-123, Medical Examination and Standards.
3. Applicant must meet weight requirements at the time of entry into the AGR Program. Any member on the ANG Fitness Improvement Program is ineligible for entry into AGR status.
4. Applicant should be able to complete 20 years of active duty service prior to mandatory separation.
5. Category 1 AGR resources (recruiters, security forces, range, air defense, civil support) are fenced and are not able to move AGR asset.
6. Highly desired that member have completed the appropriate level of PME corresponding to their grade/rank.

BRIEF OF DUTIES AND RESPONSIBILITIES

Performs duties to develop, sustain, and enhance cyberspace capabilities to defend national interests from attack and to create effects in cyberspace to achieve national objectives. Plans and conducts Defensive Cyberspace Operations (DCO) using established tactics, techniques, and procedures to achieve Service, CCMD, Cyber Mission Force (CMF) and national objectives. Executes command and control (C2) synchronization of assigned cyberspace forces and de-conflicts cyberspace operations across the kinetic and non-kinetic spectrum. Supports cyberspace capability development, testing, and implementation. Partners with Joint, Interagency, Intergovernmental, and Multinational forces to detect, deny, degrade, disrupt, destroy, manipulate, and mitigate adversarial access to sovereign national or partner cyberspace systems. Develops and executes tactics, techniques, and procedures (TTPs) for defensive cyberspace operations. Analyzes national defense guidance and strategic objectives to create operational policies and plans. Implements policies through the development of TTPs in support of assigned cyber capability execution. Applies forensic, malware analysis, and reverse engineering TTPs to determine the extent of the battle damage sustained during cyberspace attacks. Performs research and development in support of information warfare. This may include developmental testing and evaluation or operational testing and evaluation to support new capability development or to support modifications of existing capabilities. Establishes performance standards, trains, and conducts evaluations to ensure personnel are proficient, qualified, and certified. Plans, conducts, and evaluates exercises to enhance operational readiness and ensure adherence to operational procedures. Duties and responsibilities of a 1B4X1 do not include contract management, oversight and/or Contractor Officer Representative (COR) responsibilities. Prepares oral and written communications using principles, practices, techniques and analytical methods and interpersonal relations practices. Performs other duties as assigned.

AFSC

AFSC: 1B471 Applicants must meet the basic eligibility requirements specified in ANGI 36-101, The Active Guard/Reserve Program and the Air Force Enlisted Classification Directory (AFECD) 30 APR 2024. **Knowledge:** Knowledge is mandatory of: computer operating systems, software applications, database concepts, common programming languages, hardware components, networking fundamentals (such as network protocols, network addressing, and network infrastructure), telecommunications theory, and data communications. Airmen in this specialty must be proficient on wireless technologies and understand cryptography, to include utilization and exploitation techniques. Airmen must also have an understanding of

applicable laws governing cyber operations. **Education:** For entry into this specialty, prior coursework in Science, Technology, Engineering, and Mathematics (STEM) is desirable. An Associate's degree or higher in related STEM fields and/or an Information Technology (IT) certification are also desirable. **Training:** For award of AFSC 1B431, completion of the Cyber Warfare Operations initial skills course is mandatory unless specifically waived by the 1B Career Field Manager. **Experience:** The following experience is mandatory for award of the AFSC indicated: 3.4.1. 1B451. Qualification in and possession of AFSC 1B431 and experience performing functions such as offensive and defensive cyber operations. **1B471:** Qualification in and possession of AFSC 1B451. Also, experience performing and supervising functions such as offensive and defensive cyber operations. **Other:** The following are mandatory as indicated for entry into this specialty: A minimum score of 70 on the Air Force Electronic Data Processing Test (EDPT). Armed Services Vocational Aptitude Battery (ASVAB) must have been taken within 2 years from date retraining application is submitted. See attachment 4 for additional entry requirements. For award and retention of these AFSCs: 3.5.2.1. Must attain and maintain foundational work-role qualification IAW DoDM 8140.01AA, *Cyberspace Workforce Qualification and Management Program*. Currently, the Air Force mandates cybersecurity workforce position qualification by requiring cyber workforce personnel to maintain a minimum Information Assurance Technical Level II certification in accordance with AFMAN 17- 1303, *Information Assurance Workforce Improvement Program*. Certification will continue to be required until DoDM 8140.01AA publication AND upon modification of Air Force certification requirement via AFMAN 17-1303 modification, supersession, or rescission, if determined applicable. In this context, the term cybersecurity workforce is inclusive of 1B work-roles IAW AFMAN 17- 1303. Specialty requires routine access to Tier 5 (T5) information, systems, or similar classified environments. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management*, and AFMAN 17-1301, *Computer Security (COMPUSEC)*. Completion of a current T5 Investigation IAW DoDM 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program Management*. Award of the entry level without a completed T5 Investigation is authorized provided an interim Top Secret security clearance has been granted according to DoDM 5200.02, AFMAN 16-1405.

AFSC: 1N4X1A General duties: Provides cyber intelligence planning and operations support to cyberspace and computer network operations. Supports analytical aspects of various Air Force and Joint intelligence, surveillance, and reconnaissance operations by collating, analyzing, evaluating, and disseminating cyber intelligence information. Produces cyber technical products to include target assessments, adversary studies of the cyberspace operational environment, situation reports, and other intelligence products as required. Utilizes all- source intelligence information to produce and present topical high-interest technical and operational intelligence briefings to all levels of command. Creates and maintains technical and operational databases using diverse computer hardware and software applications. Computer Network Operations: Conducts global collection, exploitation, and signals analysis critical to cryptologic and cyber operations missions. Counters emerging target technologies and gains new access to adversary communications. Exploits and maintains access to worldwide networks. Delivers information in compliance with legal, policy, formatting, and timeliness requirements. Utilizes digital network analysis to conduct computer network exploitation operations on foreign targets that directly enable computer network defense of critical US systems and infrastructure. Provides projection of power capabilities to commanders across US major commands. Cyberspace Operations: Provides key intelligence enabling offensive and defensive cyberspace operations for US Cyber Command. Conducts analysis of metadata, target analysis, and target research. Identifies target communications within global networks and conducts target technology trends research. Performs global network analysis and mapping, to include technology, activities, and communications, in order to determine target traffic behavior patterns. Analyzes exploitation opportunities for information systems and infrastructure. Utilizes methods and applications of tools used for exploitation and analysis of computer systems and network vulnerabilities. Provides intelligence planning and operations support for target delivery, development, and reporting for cyberspace operations. Intelligence Training Supporting Cyber Operations: Instructs military personnel on cyber intelligence collection, analysis, and reporting requirements and procedures. Collates intelligence and operations materials to impart proper tradecraft supporting air, space, and cyberspace signals intelligence analysis. Drives development of discovery and tradecraft to broadly enable cryptologic, DoD, and Air Force missions. Integrates information assurance, cyber, cryptologic authorities, and data to evolve development of tradecraft and generate measurable mission outcomes. Processes, exploits, and disseminates intelligence products and conducts analysis concerning threat countries or targets of interest via written and/or verbal means. These products provide specificity and knowledge to commanders and national leaders to impact tactical through strategic level decision making processes. Cyber Network Defense and Malware Analysis: Utilizes various analytical tools and techniques to identify and track potential cyber threats, malware, and malicious cyber actors. Collaborates with intelligence analysts, network defenders, and information technology professionals to ensure timely and accurate discovery and reporting of cyber threats to Department of Defense and Intelligence Community stakeholders **Knowledge.** Must gain and maintain knowledge of global communications procedures; analytical techniques; organization of the national intelligence structure; intelligence organizations and systems; Information Operations; organization of designated military forces; geography; collection and reporting, systems, principles, methods, and procedures; effective writing principles; oral and written intelligence information presentation; and directives for handling, disseminating, and safeguarding classified information. **Education**. For entry into this specialty, completion of high school with courses in composition, speech, English, geography, world history, statistics, algebra, geometry, and computer applications is desirable. 3.3. **Training.** The following training is mandatory for award of the AFSC indicated: 1N431A. Completion of the Digital Network Analysis Fundamentals course and Joint Cyber Analysis course. For U.S. Space Force, completion of the Digital Network Analysis Fundamentals course, Joint Cyber Analysis course and Space Warfighter Intelligence Formal Training Unit is mandatory until replaced by new courses as determined by US Space Force. **Other**. The following are mandatory as indicated: For entry into this specialty: No speech disorders or noticeable communications deficiencies as defined by AFI 48-123, Medical Examinations and Standards. Must obtain a minimum score of 46 required on the Tailored Adaptive Personality Assessment System (TAPAS)/ Armed Services Vocational Aptitude Battery (ASVAB) selection model. See attachment 4 for additional entry requirements. 3.5.2. For award and retention of AFSC 1N4X1X, the following are mandatory: When required for a current or pending assignment, must successfully complete and pass a Counterintelligence (CI) polygraph test and meet all customer access eligibility requirements. Airmen unable to access mission, systems and/or facilities after 12 months of investigation/security screening will be considered for retraining or separation. Maintain local network access IAW AFI 17-130, Cybersecurity Program Management and AFMAN 17-1301, Computer Security. 1N451A and 1N471A. Completion of the Joint Cyber Analysis course for RegAF (effective 1 Aug 2019 for Air Force Reserve component) airmen is mandatory for those in grades TSgt (E-6) and below with less than 15 years of time in service. Specialty requires routine access

to Tier 5 (T5) information, systems, or similar classified environment. Completion and favorable adjudication of a current T5 Investigation IAW DoDM 5200.02, AFMAN 16-1405, Air Force Personnel Security Program, is mandatory. **NOTE**: Initial attendance in 1N4X1A AFSC awarding course without a completed T5 clearance is authorized provided an interim T5 clearance eligibility has been granted IAW Intelligence Community Directive (ICD) 704. Airmen who cannot obtain at least an Interim T5 clearance for programmed class-start are not eligible for entry into the AFSC.

SPECIAL INFORMATION (IF APPLICABLE)

1. Appropriate military uniform will be worn during duty hours.
2. Existing MDANG promotion policies apply.
3. Initial tours may not exceed 3 years. Follow-on tour lengths may be from 1 to 6 years.
4. Official notification to applicants of selection or non-selection is by letter from the Human Resources Office (HRO).
5. May be authorized PCS IAW the JFTR.
6. Must currently have TS/SCI clearance with Counterintelligence Polygraph
7. Must hold 1B4X1 or 1N4X1A AFSC and hold at least the 3 skill level.
8. Cyber Mission Force (CMF) qualifications preferred.
9. Some travel for conferences, training and exercises.
10. May require mobilization for Cyber Mission Forces.

APPLICATION PROCEDURES / REQUIRED DOCUMENTS (IF APPLICABLE)

INCOMPLETE APPLICATIONS WILL NOT BE ACCEPTED
APPLICATIONS WILL NOT BE RETURNED!

SUBMIT APPLICATION IN ORDER LISTED BELOW

☐ NGB Form **34-1** ***Application for Active Guard Reserve (AGR) Position,*** **DATED 20131111**, Signed, dated and annotated with Vacancy Announcement Number.
☐ Military Personnel **Report of Individual Person (RIP) Attached, or Virtual MPF Inquiry Will Suffice**.
☐ AGR Profile Verification Statement **(third page of this announcement).**
☐ Most Recent Air Force Fitness Management System (AFFMSII)
☐ Letters of Recommendation, Resume and other cyber certificates are permitted
☐ All DD214s or NGB 22
☐ Completed Questionnaire **(below)**

Questionnaire:

Y/N
☐☐ Are you currently a Maryland Air National Guard Member? _____
☐☐ Are you currently AGR? If so, what State? _____
☐☐ Are you currently a Technician? If so, what State? _____
☐☐ Are you currently deployed? If so, what location? _____
☐☐ Are you currently on ADOS? If so, with who? & what is the ending date? _____
☐☐ Are you currently in a "fenced" position? _____

Please provide current telephone number and **Military Email** address **(**Selection and Non-selection Memos will be sent via **Encrypted Email**):_____, _____

FORDWARD APPLICATIONS AND ATTACHEMENTS VIA EMAIL TO: 175.WG.HRO.AGR.PROGRAM.Org@us.af.mil
SUBMIT ONE PDF DOCUMENT ENTITLED: 25-038a (LAST NAME) – CYBER WARFARE OPERATIONS

ALL APPLICATIONS MUST BE SUBMITTED ELECTRONICALLY! NO EXCEPTIONS.
Applications must be received in the HRO office, by 1700 on the closing date. Applications received after the closing date WILL NOT BE CONSIDERED.

Human Resources Office
ATTN: NGMD-HRO-AGR-AIR
Fifth Regiment Armory
29th Division Street
Baltimore, MD 21201-2288

AGR VACANCY APPLICATION
PROFILE VERIFICATION STATEMENT

NAME _____ ANNOUNCEMENT # _____

A. FITNESS PROGRAM TEST VERIFICATION

MEMBER MEETS STANDARDS IN ACCORDANCE WITH AFI 36-2905

YES NO

_____
*Signature/Rank/Title Verifying Official

*Current supervisor, commander, or designated WMP Monitor

B. APTITUDE SCORES

Mech: _____ Admin: _____ Gen: _____ Elect: _____

_____
**Signature/Rank/Title Verifying Official

**Current supervisor, commander, or Customer Service Representative

C. CURRENT AF Form 422, PHYSICAL PROFILE SERIAL REPORT

P:___ U:___ L:___ H:___ E:___ S:___ X Factor ___ Dated _____

MEMBER IS IS NOT QUALIFIED FOR WORLD WIDE SERVICE

_____
**Signature/Rank/Title Medical Certifier

ATTACH TO NGB FORM 34-1
APPLICATION FOR ACTIVE GUARD/RESERVE (AGR) POSITION