NATIONWIDE

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

POSITION VACANCY ANNOUNCEMENT 22-048a

Open Date: 23 June 2022 Close Date: 22 July 2022

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

BRANCH OF SERVICE: AIR NATIONAL GUARD (ANG)

POSITION TITLE: IT SPECIALIST (NETWORK)

HIGHEST GRADE AUTH PER ANGI 36-101, AGR/MIL TECH GRADE COMPARABILITY TABLE: TSgt/E6

UNIT MANNING DOCUMENT-GUARD GRADE/ POSITION AVAILABLE: TSgt/E6

ORGANIZATION/LOCATION: 175th Communications Flight, 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 NATIONWIDE TO CURRENT MEMBERS OF THE MARYLAND AIR NATIONAL GUARD AND THOSE ELIGIBLE FOR MEMBERSHIP

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

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] 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] 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] 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] Collects, processes, preserves, analyzes, and presents computer-related artifacts in support of network vulnerability mitigation [DCWF Code – 211] 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] 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] 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] 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] 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] 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]. 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] Provides end users tiered-level customer support by coordinating software, hardware, and network configuration, troubleshooting, resolution, security, maintenance, and training. [DCWF Code – 411] 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. Performs other duties as assigned.

AFSC

AFSC: 1D7X1B 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) 21 APR 2022. **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. **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. **Training:** For award of the 1D731X, completion of the suffix-specific course is mandatory. **Experience:** The following experience is mandatory for award of the AFSC indicated: There are no specific upgrade requirements for the slick AFSC 1D7X1 not already defined in the training AFI. For award of the 1D751X, qualification in and possession of 1D731X and experience in suffix specific functions. For award of the 1D771X, qualification in and possession of 1D751X and experience in suffix specific functions. For award of the 1D791, qualification in and possession of 1D77XX and experience managing and directing cyber defense activities. 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: 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:

- For 1D7X1, a minimum of position requirements.
- For 1D7X1A, a minimum Information Assurance Technical Level II certification.
- For 1D7X1B, a minimum Information Assurance Technical Level II certification.
- For 1D7X1D, a minimum Information Assurance Management Level I certification.
- For 1D7X1E, a minimum Information Assurance Technical Level II certification.
- For 1D7X1K, a minimum of position requirements.
- For 1D7X1R, a minimum of position requirements.
- For 1D7X1Z, a minimum of position requirements.

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.

4. *Specialty Shredouts:

Suffix Portion of AFS to Which Related
A Network Operations
B Systems Operations
D Security Operations
E Client Systems Operations
K Knowledge Operations
R RF Operations
Z Software Development Operations

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 or be able to obtain SECRET clearance.

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 **(fourth page of this announcement).**
☐ Most Recent Air Force Fitness Management System (AFFMSII)
☐ Letters of Recommendation, Cover Letter, Resume and other attachments are permitted, but are not mandatory.
☐ All DD214s or NGB 22
☐ Completed Questionnaire **(below)**

For Positions Advertised to "Current On-Board AGR Applicants Only":

☐ **Current On-Board AGR** member, you must submit Commander Memorandum of Authorization with your application**.**

Questionnaire:

Y / N

☐ ☐ Are you currently a Maryland Air National Guard Member? If not, What state?

☐ ☐ 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**):

Email: Phone:

FORDWARD APPLICATIONS AND ATTACHEMENTS VIA EMAIL TO: 175.WG.HRO.AGR.PROGRAM.Org@us.af.mil
SUBMIT ONE PDF DOCUMENT ENTITLED: 22-048a LAST NAME- IT SPECIALIST (NETWORK)

DUE TO COVID -19, WE WILL NO LONGER EXCEPT WALK INS. DROP OFF IS AVAILABLE TUESDAY- FRIDAY 0800 - 1600 AT THE FIFTH REGIMENT ARMORY MAILROOM LOCATED ON THE 1ST FLOOR. ALL APPLICATIONS MUST BE IN A SEALED EVELOPE LEGIBILITY HANDWRITTEN OR TYPED, WITH THE MEMBER NAME AND ANNOUNCEMENT NUMBER. NO EXCEPTIONS

IF MAILING, DO NOT STAPLE, OR DOUBLE SIDE PRINT DOCUMENTS.
MAIL APPLICATION AND ATTACHEMENTS TO:

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

Applications must be received in the HRO not later than close of business on the closing date!
Applications received after the closing date will not be considered.

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