DEPARTMENT OF THE AIR FORCE
MASSACHUSETTS NATIONAL GUARD

Human Resources Office
2 Randolph Road
Hanscom AFB, Massachusetts 01731-3001

ACTIVE GUARD RESERVE (AGR) – MILITARY VACANCY ANNOUNCEMENT #104-23-031

OPEN DATE: 27 JAN 2023 **EXPIRATION DATE: UNTIL FILLED**

Open To: All members eligible to enlist in Mass ANG, any AFSC.

Number of Positions:	**1**
Position Title:	**CYBER DEFENSE OPERATIONS**
Unit/Duty Location:	**104th Fighter Wing, Westfield, Massachusetts 01085**
Minimum/Maximum Grade Authorized:	**SrA/E3 – MSgt/E7**
Duty AFSC:	**1D7X1**
Required ASVAB:	**E: 60**
Security Clearance:	**T5**
PULHES:	**G, 3, 3, 3, 2, 3, 2**
Position POC:	**CMSgt Jeffrey Samuelson, 413-568-9151 ext. 698-2744** jeffrey.samuelson@us.af.mil
Technician Advertisement Refer to:	**N/A**

Application Email: 104fss.agrjobapps.org@us.af.mil
HRO Remote: 413-568-9151 ext. 698-1290 / 698-2509

POSITION IS CONTINGENT UPON THE AVAILABILITY OF FUNDS AND RESOURCES

Specialty Summary. Manages and performs Defensive Cyber Operations (DCO) and cyber functions (DoDIN operations) in garrison and in deployed environments. Surveys, secures, protects, defends, preserves, designs, builds, operates, and extends data, networks, net-centric capabilities, and other designated systems. This Air Force Specialty Code description incorporates the use of DoD Cyber Workforce Framework (DCWF) Codes to tie this specialty description to the framework. The DCWF was developed by the National Institute of Standards and Technology (NIST) and the DoD to establish a common lexicon and model for all cyber work. The DCWF will universalize training and education between academia, industry, and military. It will also enable talent management by ensuring the right Airmen, for the right assignment, at the right time.

Duties and Responsibilities:

1. Responds to disruptions within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, along with 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]

2. 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]

3. 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]

4. 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]

5. Collects, processes, preserves, analyzes, and presents computer-related artifacts in support of network vulnerability mitigation [DCWF Code – 211]

6. 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]

7. 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]

8. 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]

9. 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]

10. 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]

11. 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]

12. 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 AFECD, 31 Oct 22 58
understanding and expertise to make data driven business decisions that increase effectiveness or efficiency of operational forces. [DCWF Code – 421/422]

13. Provides end users tiered-level customer support by coordinating software, hardware, and network configuration, troubleshooting, resolution, security, maintenance, and training. [DCWF Code – 411]

14. Test, implements, deploys, maintains, sustains, troubleshoots, repairs, and administers standard and filed expedient radio frequency wireless, line-of-sight, beyond line-of-sight, wideband, and ground-based satellite and encryption transmission devices (infrastructure and hardware). Includes multiple waveform systems, establishes and maintains circuits, configures and manages system and network connectivity. [DCWF Code -521]

LENGTH OF TOUR

Initial AGR tour orders are probationary. The probationary period will be a minimum of three years and a maximum of six years. Follow-on tour will not exceed six years and will not be extended beyond an enlisted Airman's Expiration Term of Service (ETS) or an Officer's Mandatory Separation date (MSD).

SPECIAL REQUIREMENTS

See attachment 4 of AFECD for additional entry requirements.

MINIMUM QUALIFICATION REQUIREMENTS

1. Air National Guard, Air Force Reserve or the United States Air Force members who have not achieved a passing Fitness Assessment score are ineligible for entry into the AGR program.

2. Air National Guard members must meet the physical qualifications outlined in AFI 48-123 prior to entry on AGR duty.

3. An applicant on a medical profile may apply for AGR tours as long as meet the aforementioned requirement and subsequently are medically cleared off any DLC/medical profile prior to starting a new AGR tour.

4. Applicants who do not hold the duty AFSC for the advertised position must meet minimum ASVAB requirements.

5. Must meet any Special Requirements as specified in the Position Description.

6. Failure to obtain and maintain a SECRET or TOP SECRET (if applicable) security clearance will result in removal from the AGR program.

7. Selected individual must extend/re-enlist for a period equal to or greater than initial tour end date.

8. IAW ANGI 36-101, paragraph 5.3., to accept an AGR position, an applicant's military grade cannot exceed the maximum military authorized grade for the AGR position. Overgrade enlisted applicant must indicate, in writing, the willingness to be administratively reduced in grade when assigned to the position. Officers may not enter into the AGR program in an overgrade status.

9. IAW ANGI 36-101, paragraph 5.7, an individual must not have been previously separated for cause from active duty or previous Reserve Component AGR tour.

10. IAW ANGI 36-101, paragraph 5.10, applicants should be able to complete 20 years of active federal service prior to Mandatory Separation Date (MSD). Individuals selected for AGR tours that cannot attain 20 years of active federal service prior to reaching mandatory separation must complete a Statement of Understanding contained in Attachment 3 of ANGI 36-101.

11. IAW ANGI 36-101, paragraph 6.6.1., members should remain in the position to which initially assigned for a minimum of 24 months. TAG may waive this requirement when in the best interest of the unit, State, or Air National Guard.

12. Additional entry/retention requirements for AFSCs are outlined in the AFECD/AFOCD.

APPLICATION REQUIREMENTS

1. **NGB Form 34-1, signed (https://www.massnationalguard.org/index.php/careers/available-positions.html)**

2. **Current Report of Individual Personnel (RIP): Obtain from Virtual Military Personnel Flight (vMPF; https://w45.afpc.randolph.af.mil/AFPCSecureNet40/CheckPortal.aspx)**

3. **AF Form 422: Must be obtained and verified within 6 months from your Medical Group**

4. **myFitness Individual Tracker Report: Current & passing w/ 12 months https://myfss.us.af.mil/USAFCommunity/s/login/?ec=302&startURL=%2FUSAFCommunity%2Fs%2F)**

5. **SF 181, Ethnicity and Race Identification (https://www.massnationalguard.org/index.php/careers/available positions.html)**

6. **Pre-Employment Reference Check Form (https://www.massnationalguard.org/index/php/careers/available.positions.html; not required for 104th permanent on-board AGRs)**

7. **Last 3 EPRs (AFPC Secure, PRDA; https://w45.afpc.randolph.af.mil/AFPCSecureNet40/CheckPortal.aspx)**

☐ **Applications must be submitted by email NLT 2359 on the advertisement expiration date**

☐ **If submitting application by email, all required documents must be submitted as one .pdf file (no adobe portfolios please) to** 104fss.agrjobapps.org@us.af.mil

SUBJECT LINE OF EMAIL SUBMISSION MUST CONTAIN FULL BULLETIN NUMBER

NOTE: To combine files in one PDF, you must print any secure and/or digitally signed documents to "Microsoft PDF." Once printed, you can combine the newly printed PDF files with all other application documents.

MCPN: 0108815134
R: 294