AIR NATIONAL GUARD
117TH AIR REFUELING WING (AMC)
SUMPTER SMITH JOINT NATIONAL GUARD BASE
BIRMINGHAM, ALABAMA 35217

ACTIVE GUARD RESERVE (AGR) – MILITARY VACANCY ANNOUNCEMENT # 23-062

OPEN DATE: 15 NOVEMBER 2023 **EXPIRATION DATE: 15 DECEMBER 2023**

Open To: NATIONWIDE

Number of Positions: 1
Position Title: CYBER DEFENSE OPERATOR
Position Number: 102829434
Minimum/Maximum Grade Authorized: A1C-SSGT
Duty AFSC: 1D7X1Q Eligible
Security Clearance: TS/ SCI REQ'D
Unit/Duty Location: 117th INTELLIGENCE SQUADRON

Selecting Official: Lt Col Matthew Burns
HRO Remote: MSgt Samantha Crotzer (205) 714-2686

If your current grade exceeds the maximum grade of this announcement, you must submit a written statement indicating willingness to accept an administrative reduction.

APPLICATION REQUIREMENTS

1. **Signed NGB Form 34-1, https://www.ngbpdc.ngb.army.mil/Portals/27/forms/ngb%20forms/ngb34-1.pdf?ver=2018-09-28-105133-833**
2. **Current Report of Individual Personnel (RIP): Obtain from Virtual Military Personnel Flight (vMPF)**
3. **AF Form 422: Must be signed and verified within 6 months from your Medical Group**
4. **Air Force Fitness Management System II (AFFMSII) Fitness Report: Must be Current and passing**
5. **All applications must be submitted with a completed AGR Eligibility Checklist, found in ANGI 36-101. Your unit's HRO Remote Designee or the appropriate FSS representative must complete this checklist.**

Note: (E8/E9/O4/O5/O6 Only) Promotion and hiring is contingent upon control grade availability

---

E-Mail completed application packages to:

JFHQ-AL MDM
ATTN: MSG JIMMY L. ACOFF
ng.al.alarng.list.j1-air-mdm@army.mil
P.O. Box 3711
Montgomery, AL 36109-0711

All emailed packages must be in a single PDF

CYBER DEFENSE OPERATIONS
(Changed 30 Apr 23)

1. ★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 incorporates the use of DoD Cyber Workforce Framework (DCWF) Codes to tie this specialty 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. Cyber, communications and Information Technology capabilities critically underpin all Air and Space Force core missions. The delivery of operationally focused governance and investment to drive sustainability and reliability for this domain is a warfighting necessity. This drives the Department of the Air Force (DAF) forward with real actions which enables modernizing and achieving the cyber posture required to meet pacing challenges. This fully mission capable model develops Airmen that can complement multiple work roles and build technical experts by using the advanced competency levels through the Occupational Competency Model referenced in the Career Field Educations Training Plan (CFETP) available on e-pubs.

2.1. The available duties and responsibilities can encompass:

2.2. ★Enterprise Operations delivers enduring cyber mission capabilities. Enterprise Operations includes all applicable statutes, but specifically the designing, building, provisioning, maintaining, and sustaining information systems, including warfighter communications, within the Department of the Air Force (DAF). The Department of Defense Information Network (DoDIN) operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DoD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DoDIN.

2.3. ★Mission Defense Activities conducts targeted defense of the DoDIN and other DoD systems to execute DAF operations. Operations focus on identifying, locating, and defeating specific threats that compromise the security of the communications, information, electromagnetic environment, or industrial systems through defensive and protective measures within a specified operational area. Operations in contested, degraded, and denied environments to include but not limited to DoD networks, airborne platforms, austere environments, AOC/JOCs (Air & Space Operations Center/Joint Operations Center), Weapons Systems, ICS (Industrial Control Systems) & SCADA (Supervisory Control and Data Acquisition) systems, and other interconnected devices that play a role in mission effectiveness.

2.4. ★Data Operations enables data driven decisions through delivering the employment of information operations and software development methodologies. Operations modernizes and enhances warfighter and weapon system/platform capabilities through the rapid design, development, testing, delivery, and integration of reliable, secure mission-enabling systems. Provides automated solutions for Commanders requiring real-time, data-driven decisions.

2.5. ★Expeditionary Communications delivers cyber capabilities in austere and mobile environments. Expeditionary Communications includes all applicable statutes, but specifically datalinks, the building, operating, maintaining, securing, and sustaining of tactical and communications networks when needed to support warfighter requirements, systems employed in austere, mobile, and/or expeditionary environments, to provide command and control in support of Air and Space Force missions.

3.1. ★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 include; national and international laws, policies, and ethics related to operational cybersecurity; operational risk management processes; and specific operational impacts of lapses in cybersecurity. Radio propagation factors along with understanding regulations governing use of the electromagnetic spectrum. The installation and maintenance management functions include; wire transmission principles; electrical and light wave communications; antenna fundamentals, and cable testing procedures.

3.2. 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.

3.3. Training. For award of the 1D731X, completion of the suffix-specific course is mandatory.

3.4. Experience. The following experience is mandatory for award of the AFSC indicated: 3.4.1. There are no specific upgrade requirements for the slick AFSC 1D7X1 not already defined in the training AFI.

3.4.2. For award of the 1D751X, qualification in and possession of 1D731X and experience in suffix specific functions.

3.4.3. For award of the 1D771X, qualification in and possession of 1D751X and experience in suffix specific functions.

3.4.4. For award of the 1D791, qualification in and possession of 1D77XX and experience managing and directing cyber defense activities.

3.5. Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty: 3.5.1.1.1. ★See attachment 4 for additional entry requirements.

3.5.1.1.2. ★Prior qualification of attaining and maintaining an Information Assurance Technical Level II or Information Assurance Manager Level I certification IAW DoD 8570.01-M, *Information Assurance Workforce Improvement Program* for retraining can waive minimum ASVAB requirements.

3.5.2. For award and retention of these AFSCs: 3.5.2.1 ★Must attain and maintain a minimum certification level based on position requirements IAW AFMAN 17-1303, *Cybersecurity Workforce Improvement Program* and DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, as specified by AFSC shred and/or work role SEI:

3.5.2.2 ★For 1D7X1X, a minimum certification level is based on position requirements, or a minimum of an Information Assurance Technical Level II certification or Information Assurance Manager Level I certification.

3.5.2.3 ★ Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security*.

3.5.3. ★Specialty requires routine access to classified information, systems, missions, and environments to include but not limited to Sensitive Compartmented Information Facilities (SCIF), Airborne platforms, Agile Combat Employment, Nuclear Command Control & Communications (NC3), and a multitude of emerging mission requirements in a highly contested domain IAW DoDM 5200.01-DAFMAN 16-1405. 3.5.3.1 ★ Must maintain & sustain highest security clearance level received up to Top Secret (Tier 5) or based on current position requirements.
3.5.3.2 ★ Completion of a background investigation according to DoDM 5200.01 - DAFMAN 16-1405, *Personnel Security Program Management*, is mandatory.

NOTE: Award of the 3-skill level without a completed investigation is authorized provided minimum of interim Tier 5 (Top-Secret) clearance has been granted according to DoDM 5200.01 - AFMAN 16-1405.