

**Traditional (DSG)  
Cyberspace Warfare Operator**

<b>MARYLAND AIR NATIONAL GUARD 175<sup>th</sup> Wing</b> 2701 Eastern Blvd Middle River, MD 21220	<b>ANNOUNCEMENT #:</b> FY24 COS-01
	<b>DATE:</b> 23 Jan 2023
	<b>CLOSING DATE: OPEN UNTIL FILLED</b>
<b>UNIT: 275<sup>th</sup> Cyberspace Operations Sq.</b>	<b>AFSC:</b> 1B471
<b>MIN GRADE:</b> E-4/SrA <b>MAX GRADE:</b> E-6 TSgt	<b>AREA OF CONSIDERATION:</b> Current members of the Maryland Air National Guard or members eligible to become members of the MDANG in the grade of E-4 – E-6 in AFSC 1B471.
<b>POSITION TITLE:</b> Cyberspace Warfare Operator	

**SPECIALTY SUMMARY**

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.

**QUALIFICATIONS AND SELECTION FACTORS:**

- This is a DSG position. Selection for this position does not constitute accession into a permanent AGR program. Tour may be extended pending resource availability with NGB, and TAG approval, by exception.
- Applicants must currently be a E-4 – E-6 and hold the 1B4X1 AFSC to apply.
- The selectee must possess excellent interpersonal skills, and organizational skills.

**DUTIES AND RESPONSIBILITIES:**

Conducts Defensive Cyber Operations (DCO). Plans and/or conducts DCO actions to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Cyber warfare operators conduct both DCO-Internal Defense Measures (DCO-IDM). DCO-IDM duties performed by cyber warfare operators do not include passive defense measures intended to maintain and operate the DODIN such as configuration control, patching, or firewall operations. Cyber warfare operator missions conducted as part of DCO-IDM should utilize the workforce's highly specialized skills such as pro-active and aggressive internal threat hunting for advanced and/or persistent threats, reverse engineering, and malware analysis. Integrates DCO actions into Combatant Command, warfighting, or service boards, bureaus, cells, centers, and working groups as required for inclusion into operational and strategic planning efforts.

1B4X1 Cyber Mission Force DCO work roles include but not limited to: Cyber Operations Planner, Host Systems Analyst, Network Systems Analyst, Network Systems Technician, Data Engineer, Data Analytics Support, and Malware Analyst.

## **Specialty Qualifications:**

**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:

- 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:
  - o A minimum score of 70 on the Air Force Electronic Data Processing Test (EDPT).
  - o Armed Services Vocational Aptitude Battery (ASVAB) must have been taken within 2 years from date retraining application is submitted.

## **APPLICATION PROCEDURES:**

PT History Report, Records Review RIP and last 3 performance evaluations (EPRs) if available and Commanders Concurrence Letter. Questions may be directed to TSgt Justin Rogers 410-918-6685 or send an e-mail to: [justin.rogers.19@us.af.mil](mailto:justin.rogers.19@us.af.mil)

**EMAIL APPLICATION TO: [justin.rogers.19@us.af.mil](mailto:justin.rogers.19@us.af.mil)**