# MILITARY VACANCY ANNOUNCEMENT

## ANNOUNCEMENT NUMBER: K3 MVA 25-014

| | | | |
|---|---|---|---|
| **Open Date:** | 1-Apr-2025 | **Close Date:** | |
| **Unit:** | 116 ACS (Cyber Conversion) | | |
| **Position Title:** | Cyber Warfare Operations (Current/Qualified) | | |
| **AFSCs:** | 1B4 | | |
| **Grade:** | SSgt - TSgt | | |
| **Status:** | **Drill-Status Guardsman** | | |
| **Cross-Train:** | No | | |

### Who May Apply:

Current on-board members of the Oregon Air Natonal Guard

Members eligible to join the Oregon Air National Guard

### How to Apply:

Current 1B4, not a cross training opportunity. Application package will consist of a single PDF including a resume detailing your experience, military and civilian education, a record review RIP (from vMPF) w/in 60 days, and a copy of current Physical Fitness Assessment Report.

### Email Packages to:

142WG.Cyber@us.af.mil / Subject Line: K3 MVA 25-014 Application-Last, First Name

## DUTIES AND RESPONSIBILITIES

Conducts DCO. Plans and/or conducts DCO actions to defend the DoDIN and other friendly cyberspace. DCO includes threat-informed 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)and DCO-Response Actions (DCO-RA). 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 CCMD, warfighting and/or service boards, bureaus, cells, centers, and working groups as required for inclusion into operational and strategic planning efforts.

As a Cyberspace Warfare Operator, the applicant will maintain Combat Mission Ready status to perform the phases of a Cyberspace Protection Team or Cyber-to-Physical mission. Will perform individual memory process analysis using built-in tools and capabilities. Configuration and security of Unix/Linux services. Will perform tasks with file systems, permissions, and operation system configurations. Captures the memory of individual processes and analyzes it using built-in tools and capabilities. Provides analytic expertise in network traffic and understand network traffic signatures and discover anomalies through net flows and traffic analysis. Will identify, assess, and mitigate intrusions into networks that are vital to Department of Defense Information Network security and conduct packet capturing, traffic and analyzes full packet captures using Graphic User Interface or command-line based tools. Assists in developing network topology mapping, network-based signatures, advanced network detection rules and alerts, and highly tailored queries and dashboards in order gain a holistic view of the network. Implements directives from higher headquarters. Ensures necessary operations are conducted to provide command and control, secure and non-secure voice and data, and other battlespace effects.

Reset Form