Continued National Guard Integration in the Total Cyber Mission & Training

Fiscal Year 2024 Fact Sheet

NGAUS

Cyber-warfare specialists serving with the 175th Cyberspace Operations Group of the Maryland Air National Guard engage in weekend training at Warfield Air National Guard Base, Middle River, Md.

The Issue

The National Guard is and should continue to be a critical partner in developing, planning, and executing the Department of Defense strategy in the cyber domain.

Background

The evolving and persistent array of cyber-based threats to the United States requires continued action and coordination at all levels of government. As requirements in the cyber domain continue to develop, the National Guard supports state and federal authorities with 3,900 servicemembers in 59 cyber units across nearly 40 states.

In 2016, the National Cyber Incident Response Plan recognized that the National Guard is in a "unique position to assist in information sharing, situational awareness, secure communications and incident response." National Guard servicemembers easily leverage civilian cyber skill sets to contribute to the long-term cyber mission as an integral part of the Department of Defense's Cyber Mission Force (CMF).

The traditional part-time nature of the majority of the National Guard force also allows the Department of Defense to retain well-trained cyber warriors when they depart the Active Component after their service obligation is complete for other opportunities. The National Guard captures the experience of those servicemembers while allowing them to seek other career opportunities, which significantly reduces the military's challenge of training and retaining highly skilled warriors.

The National Guard also excels in providing cyber skills to the states under command of the Governors. Many states have advanced cyber constructs, plans, and policies that play a vital part in preventing, mitigating, and responding to cyber events outside federal domains.

Recommendation

- Ensure the National Guard is fully resourced to support all facets of cyber operations, including improving the current cyber training pipeline
- Allow the National Guard to serve as a conduit for cyber operations between federal, state, and local governments, as well as the private sector
- Establish in each state, territory, and District of Columbia National Guard Cyber Security Incident Response Teams to perform analysis, protection, and respond to emergencies
- Provide additional full-time staffing authorizations to build the Defensive Cyber Operations Element (DCOE) and robust full time support to conduct network defense

The cyber domain requires teamwork and partnerships across all government sectors and the private sector. Because of the unique authorities afforded to it by law, the National Guard continues to be an important bridge between federal and state operations contributing to training, coordination, response, mitigation, and recovery efforts. The National Guard is also a vital part of our nation's effort to effectively operate in and work with state, local, and private entities within the cyber domain.

Learn more at **ngaus.org**

NGAUS Contact **Julian Plamann**
LEGISLATIVE AFFAIRS MANAGER, JOINT PROGRAMS
julian.plamann@ngaus.org