Cyber Readiness

Responding at Network Speed

The Issue

National Guard cyber Soldiers and Airmen operating in state **Title 32** face barriers to participating in federal cyber missions requiring federal **Title 10 authorities.** These limitations prevent the Guard from accessing critical equipment, attending valuable training, and contributing to national cyber operations at the speed and scale required.

Understanding the Threat

Everything depends on digital systems: banking, emergency response, power grids, traffic control, and communications.

When systems are hacked or disrupted, the consequences can include stolen money, identity theft, shut-down services, damaged infrastructure, and **risks to public safety.**

Understanding the Guard's Role

As part of protecting the homeland, the Guard supports both state and federal cyber response and helps protect networks, assess threats, and reduce risk.

Guard cyber teams respond to real-world incidents at home, including ransomware and attacks affecting schools, local governments, and other public systems.

What the Guard Offers:

Deep cyber expertise
Civilian cutting-edge skills
Strong demand
Embedded in our communities

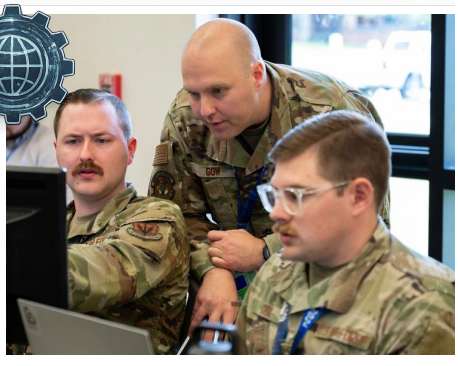
What the Guard Needs:

Predictable pathway from T32 to T10
Timely access to federal missions
Consistent training opportunities
Ability to quickly respond

The Solution

Support a streamlined, structured transition process that:

- Enables rapid activation for federal cyber missions
- Preserves governor authority and state control
- Supports continuous JQR qualification and readiness
- Enhances integration with active-duty cyber forces
- Provides flexible support to national cyber operations



ASK: Introduce the "National Guard Cyber Integration and Readiness Act" to streamline the transition from Title 32 to Title 10.

NGAUS POC: Julian Plamann, Julian.Plamann@ngaus.org
Deputy Director, Government Affairs, Joint & Personnel Programs

Protecting Our Network and Nation

Minnesota (July 2025): Minnesota National Guard responded to a major cyberattack after the city of St. Paul's response capacity was exceeded. Guard cyber personnel embedded with city staff, strengthened endpoint security, and supported recovery for 17 days.

Maryland (Fall 2025): Maryland Air National Guard cyber Airmen responded to a cyberattack that temporarily affected parts of the state government network. The response took a "whole of government approach" and included cyber threat hunters, attack analysts, cybersecurity engineers, and penetration testers.

North Carolina (May 2020): North Carolina National Guard deployed its Cyber Security Response Force to help Person County and the City of Roxboro recover from a cyberattack that disrupted phones, email, and internet services – showing how Guard cyber teams can help local governments restore essential operations after an attack.

Current Capabilities

Army National Guard

Cyber Protection Teams
Defend the DODIN, protect priority missions, prepare forces for combat

Defensive Cyber Ops Elements
Defensive internal measures to secure National Guard portion of the DODIN & respond to state cyber emergenicies as directed by Governor or Adjutant General

Cyber Warfare Companies
Full spectrum cyber operations support, OPFOR support to exercises, & pen-testing

Cyber Security Companies
Vulnerability assessments, forensics analysis, Industrial Control Systems expertise, USCYBERCOM Readiness Inspections,

Air National Guard

Cyber Protection Teams
Defend the DODIN, protect priority missions, prepare force for combat

Mission Defense Teams
Defensive cyber operations on specific weapons platform/system

National Mission Teams
Intelligence-driven cyber operations against nation state actors in defense of the nation

Red Team
Vulnerability assessments of friendly networks in support of Combatant Command & Service requirements

ASK: Introduce the "National Guard Cyber Integration and Readiness Act" to streamline the transition from Title 32 to Title 10.

NGAUS POC: Julian Plamann, Julian.Plamann@ngaus.org
Deputy Director, Government Affairs, Joint & Personnel Programs