North Carolina National Guard - Cyber Security Response Force Capabilities

The NCNG has a Dual Mission: Dedicated to delivering continuous cyber support to safeguard both State and National critical infrastructure, networks, and data against threats. Through collaboration with State, Local, Tribal, and Territorial organizations, we provide proactive and reactive assistance to protect the State's critical assets from malicious actors. Additionally, in our Federal Mission, the NCNG employs its expert team's agility and readiness to provide superior cyber defense and security capabilities, enhancing the cybersecurity posture of our Nation and supporting Federal agencies in detecting, preventing, and responding to cyber threats.

STATE & LOCAL MUNICIPALITY SUPPORT 2023

- **18** Incident Response Missions
- **64** Hygiene Assessments
- **13** Penetration Tests
- **3** Statewide Elections
- **24** Outreach Events
- **2500+** Credentials Found
- **5000+** Critical Vulnerabilities Discovered
- **225** Vulnerable Ports Identified
- **60+** Forensic Images Captured
- **$1.49M** in IIJA Grant funding awarded to local government entities based on Assessment Reports and Recommendations

Lines of Effort

- **Quick Reaction Support (Cyber QRF):** A team of trained incident responders who lead the incident response process from start to finish. The team can be on the ground in hours and will work to restore operations as quickly as possible.
- **Cyber Hygiene Assessment:** A comprehensive review of cyber hygiene to include networks, infrastructure, policies, and procedures and provides a prioritized list of remediation actions.
- **Penetration Testing:** Simulates tactics, techniques, and procedures used by malicious actors to attempt to compromise agency security. Provides a detailed report of vulnerabilities in the network, both internal and external to the agency.
- **Continuous Monitoring:** Provides monitoring services for more than 150 agencies, including state partners, county governments, and community colleges. The team provides continuous oversight and alerts agencies to potential changes in their security posture in real-time and dark web monitoring services.
- **Training and Outreach:** The Cyber Team conducts regular training and tabletop exercises with state partners across a variety of cybersecurity-related matters. The team has conducted outreach training and briefings on cyber security best practices and video conferences covering continuity of operations planning, incident response plan development, and vulnerability management.
- **Forensics Support:** Conducts threat hunting and forensic analysis in response to a cyber incident. The team looks to identify the attack vectors, root cause of the incident, and indicators of compromise to help prevent the attack from recurring.
- **Surge Capability Support:** The NCNG surge capability allows the NCNG to bring soldiers and airmen with specialized skill sets onto the team to meet whatever the mission requires. The surge capability allows the team to run simultaneous missions by adding forces to meet targeted requirements without reallocating the engaged forces.

Personnel

- **2** Federal Technicians (Division Chief and Deputy who provide oversight for the team)
- **2** AGR Warrant Officer Technical Advisors (cannot touch keyboard for state missions)
- **8** Full-Time State Employees
- **25** Full-Time Temp-State Employees
- **3** Logistical Support Personnel
- Ability to surge to **50+** depending on the mission (election support, multi-site IR, etc.)

CYBER EXERCISES

- **Cyber Shield 2023:** National Guard units and partners participated in Cyber Shield to develop, train, and exercise cyber elements, threat analysis teams, incident handlers, reporting mechanisms, and leaders. NCNG has 40 exercise participants, including the Deputy Officer-in-Charge, the Deputy Opposing Forces Lead, and the Blue Team Work Group Lead.
- **Operation Tobacco Road 2023:** NCNG hosted the first ever state tactical cyber exercise, which included 36 personnel from critical infrastructure partners, including Community Colleges, Universities, Local Government, and others operating as cyber network defenders utilizing USCYBERCOM's Persistent Cyber Training Environment to defend against the NCNG Penetration Testing Team operating as the exercise opposing forces.