Deliverables

- Non-disclosure agreements prior to start of on-site assessments
- Statement of work signed prior to start of on-site assessments
- Periodic written and/or verbal status updates
- Assessment presentation
- Executive level report with summarized results
- Detailed technical report with specific findings and recommendations
- Detailed training curriculum and objectives

Outreach

- Monthly training focused on current security trends
- Quarterly table top exercises
- Expanding publically available information sharing capabilities and resources

Threat Environment

The frequency and severity of cyber threats are growing at an alarming rate.

The barrier to entry into cyberspace for cyber-crime, espionage, and attack is low, incentives high, and vulnerabilities abundant.

Vulnerabilities are often related to outdated software or misconfigured networks threaten vectors against the confidentiality, integrity, and availability of critical systems throughout the United States.

1636 Gold Star Drive,
Raleigh, NC 27607
Phone: 984-664-7687

North Carolina Assessment and Assistance Team (NCAAT)

North Carolina National Guard

Ready
Reliable
Responsive
Relevant
at Home and Abroad

Purpose

North Carolina National Guard performs an assessment to fulfill annual security assessment requirements as well as to identify potential security, configuration, or network design deficiencies which may adversely impact the confidentialy, availability, or integrigy of agency networks, devices, and services.

Since 2020, 65 Cyber Security Assessments have been conducted by the NCAAT

Operational Mission

The NCNG performs security assessments utilizing NIST standards in conjunction with DOD Security Technical Implementation Guidelines.

The Assessment team uses the following information collection techniques:

- Interviews conducted with agency personnel, Automated network discovery/ scanning tools.
- Open source (e.g. Internet) information gathering.
- Obtaining technical configuration information for a sample of key network infrastructure devices.
- Examination of network documentation.
- Inspection of network equipment including physical-layer connectivity.

Technical Areas Covered

- Policy, Governance, Environment (Framework)
- Security (IDS, IPS, Firewall)
- Network (Router, Switch)
- System (Linux, Windows, Storage)
- Wireless (On net/Off net)

For Cyber Incident Reporting Please Call:

Primary - 800.722.3946
it.nc.gov/resources/cybersecurity-risk-management/statewide-cybersecurity-incident-report-form
Alternate - NCEM 24-HR Operations Center
919.733.3300

EMAIL: ng.nc.ncarng.mbx.g6-ncat@mail.mil