Cyber Incident Reporting

A Unified Message for Reporting to North Carolina State Government

This message is intended to bring awareness to the requirement to report cyber incidents in compliance with N.C.G.S. 143B-1379.

State agency cooperation and training; liaisons; county and municipal government reporting

Cyber incidents continue to be an increasing concern for state, local, and academic institutions within North Carolina. Every year, there has been a noted increase of attacks in the form of ransomware, data exfiltration and extortion and others, which have devastating impact to our state's critical infrastructure. This trend is forecasted to continue and remain a pervasive occurrence in the upcoming years.

A method we can use to reduce the risk to our citizen-facing services and sensitive data is to report cyber incidents as they occur. In doing so, the state will be able to provide subject matter experts, resources, and assistance in various forms ranging from consultation and guidance, to deployment of the North Carolina Joint Cyber Security Task Force (CSTF) to assist as needed. Incidents should be reported even if your agency is not requesting assistance.

The CSTF is comprised of law enforcement, emergency management, National Guard Cyber, Local Government IT Strike Team, State IT/cyber specialists and federal agencies. This team will provide incident coordination, resource support, and technical assistance to reduce the impact to the affected organization, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting the affected organization, the various members of the CSTF work in tandem to leverage their collective response expertise, apply their knowledge of cyberthreats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice.

This fact sheet explains when, what, and how to report to state government in the event of a cyber incident.

When to Report to the State

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of critical infrastructure (i.e., first responder networks, water, energy, etc.) and information systems. Reporting should take place within 24 hours of confirmation.

Cyber incidents resulting in significant damage are of particular concern to the state. Pursuant to N.C.G.S. 143B-1379, all local government entities must report all cyber incidents that may:

- Result in a significant loss of data, system availability, or control of systems
- Have an impact on a large number of victims

- Indicate unauthorized access to, or malicious software present on, critical information technology systems
- Affect critical infrastructure or core government functions
- Impact national security, economic security, or public health and safety

Examples include malware, denial of service, ransomware or large-scale hardware (server) disruptions.

Note: Incident reporting by private sector organizations is not mandated; however, it is highly encouraged.

What to Report

A cyber incident may be reported at various stages, even when complete information might not be available. Helpful information could include:

- Who you are
- Who experienced the incident
- What sort of incident occurred
- How and when the incident was initially detected
- What response actions have already been taken
- Who has been notified

The Statewide Cybersecurity Incident Report form, available at https://it.nc.gov, is designed to collect all relevant information to assist with response.

How to Report Cyber Incidents to the State

The state has multiple means to report cyber incidents.

Reporting Points of Contact	
State Agencies	Local Governments, Academic Institutions, Private Sector
Contact the NCDIT Customer Support Center at 800-722-3946. Use the Statewide Cybersecurity Incident Report form at https://it.nc.gov/report. Contact the Enterprise Security and Risk Management Office at mailto:DITThreatManagement@nc.gov.	Report cybersecurity incidents to the North Carolina Joint Cyber Security Task Force by contacting the North Carolina Emergency Management 24-Hour Watch Center at NCEOC@ncdps.gov, or at 1-800-858-0368. For general inquiries or support, contact the North Carolina Joint Cyber Security Task Force at ncisaac@ncsbi.gov.

Regardless of which method is used, the data is consolidated, tracked, and acted on by the CSTF. The state entity (e.g., N.C. Department of Public Safety or N.C. Department of Information Technology) receiving the initial report, will ensure coordination with relevant CSTF members.

Please note, this reporting does not override any other mandated federal reporting requirements.

Types of State Incident Response

Upon receiving a report of a cyber incident, the state's CSTF will establish a scoping call with the impacted entity to address the following high-level activities:

- **Incident response.** This includes conducting forensics to identify root-cause, damage assessment and mitigation, and coordination with law enforcement activities as needed. Lastly, it includes information-sharing of indicators of compromise.

- **Recovery response.** This effort could include establishing best practice recovery methods, system hardening, restoration of services and infrastructure rebuild.

Mission-Critical Support

Providing for effective public safety and implementing adequate homeland security measures to protect all North Carolinians, whether physical or in cyberspace, should be our singular focus.

To be successful, it will take a whole of government and whole of community approach requiring partnership, coordination, and collaboration across public, private, non-profit, and non-governmental organizations. Your organization is a mission critical part of this approach as we strive to protect all North Carolinians.