CYBERSECURITY (NCESF-2)

2023

I. INTRODUCTION

A. PURPOSE

The purpose of this appendix is to establish a systematic approach for addressing a cybersecurity incident that affects or threatens to affect the citizens, economy, or government of North Carolina. The goal of this approach will be to reduce impacts, enact effective cyber response measures, and support a timely recovery of state and local government IT assets, IT capabilities and critical infrastructure.

B. SCOPE

This incident response plan is applicable to state and local government operated information technology and critical infrastructure partners. In many cases, coordination between the lines of efforts, i.e. state, local, federal and private sector infrastructure owners, will be critical to the identification, protection, detection, response and recovery from a cyber incident.

II. SITUATION AND ASSUMPTIONS

A. SITUATION

Cybersecurity is the state of being protected against the criminal or unauthorized use of electronic data, or the measure taken to achieve this. The unauthorized intrusion of network systems and manipulations of these systems to include disruptions of services and extrication of sensitive data are elements of a cybersecurity incident.

B. ASSUMPTIONS

1. Information systems in the private and public sector are routinely probed and attacked on a continuous basis by a variety of known and unknown actors.

2. The potential for a cybersecurity incident exists at any given time.

3. A cybersecurity incident can produce cascading impacts that adversely affect the delivery of essential goods and services, harm the state's economy, degrade public services, and have other adverse outcomes.

4. A cybersecurity incident could be a part of a complex attack involving physical attacks or other malicious activity.

5. Ongoing deployments of information technologies in essential business processes and critical infrastructure increases the potential impact of a future incident.

6. Impacted entities may not be required to report cybersecurity incidents to the Joint Cybersecurity Task Force (JCTF), may not report cybersecurity incidents in a timely manner, or may not know who to alert unless previously notified.

7. Initial state or local response may be focused on the physical and operational impact of a cybersecurity incident, while the actual cause and impacts of the incident may remain undetermined for a period of time.

8. Cybersecurity incidents may overwhelm local government, state government and private sector resources.

III. ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

A. LEAD STATE AGENCY

1. NC DEPARTMENT OF PUBLIC SAFETY (NCDPS)

NORTH CAROLINA EMERGENCY MANAGEMENT (NCEM)

a. Member of the Join Cybersecurity Task Force as outlined below.

b. Coordinate requests for resources from all state agencies.

c. Request federal assistance as required.

B. LEAD TECHNICAL AGENCIES

NC JOINT CYBERSECURITY TASK FORCE (JCTF)

The JCTF serves as the lead task force responsible for directing technical response and recovery to an identified cybersecurity incident. The JCTF is chaired by the State Homeland Security Advisor and operated by four lead technical agencies:

1. North Carolina Local Government Information Systems Association (NCLGISA) IT Strike Team Leaders and designated deputies.

2. North Carolina Emergency Management (NCEM), Homeland Security Section Cyber Unit Manager and recognized deputies.

3. North Carolina Department of Information Technology (NCDIT) Chief State Risk Officer/State Chief Information Security Officer and designated deputies.

4. North Carolina National Guard (NCNG) Cyber Security Response Force Chief Information Officer and designated deputies.

The JCTF is responsible for:

1. Providing subject matter expertise and supporting information to aid in the declaration of a state of emergency or actions requiring the activation of this plan.

2. Escalating and downgrading cybersecurity levels.

3. Gathering cyber threat intelligence related to incidents and sharing information and intelligence with relevant partners for an all-hazards approach.

4. Identifying cyber related critical infrastructure and key resources.

5. Coordinating with all state, local, private and federal technical partners from a threat response perspective.

6. Establishing coordination calls between state, local and/or private affected entities, and ensuring the following:

    a. Legal agreements, i.e. Memorandums of Agreement/ Understanding (MOA/U) and/or Non-Disclosure Agreements (NDAs) are in place.

    b. Affected entity has established procedures to address:
        - Onsite crisis coordination (needed when multiple vendors are in use).
        - Types of forensic support on contract or needed.
        - Coordination calls.
        - Mechanisms on how Indicators of Compromise (IoCs) will be shared, e.g. HSIN or public releasable anonymized.
        - The capturing of appropriate minutes of coordination meetings.

1. **NC LOCAL GOVERNMENT INFORMATION SYSTEMS ASSOCIATION (NCGLISA)**

   INFORMATION TECHNOLOGY (IT) STRIKE TEAM

   a. Serve as one of the lead technical agencies responsible for directing technical response and recovery to an identified cybersecurity incident.

   b. Provide mutual support to local government entities impacted by any incident that exhausts their resources and capabilities.

   c. Identify and provide local government cyber and law enforcement support to aid local and tribal government organizations affected by cyber incidents.

   d. Provide technical skills to support the identification, protection, detection, response and recovery actions for cyber incidents impacting local government systems or infrastructure.

   e. Maintain local government cyber situational awareness and conduct information sharing activities with state, local and federal partners.

   f. Provide law enforcement support to collaborate with federal and state resources and aid in information sharing and timely response for the preservation of cybercrime evidence.

2. **NC DEPARTMENT OF INFORMATION TECHNOLOGY (NCDIT)**

   ENTERPRISE SECURITY AND RISK MANAGEMENT OFFICE (ESRMO)

   a. Serve as one of the lead technical agencies responsible for directing technical response and recovery to an identified cybersecurity incident.

   b. Share responsibility for providing subject matter expertise and supporting information to aid the declaration of a state emergency or actions requiring the activation of this plan.

   c. Share responsibility for the escalation and downgrade of cyber severity levels.

d. Monitor the state networks through the state's Security Operations Center (SOC) for cybersecurity incidents or other conditions which could disrupt essential information technology services in the state.

e. Share cybersecurity incident response and recovery activities with the State Emergency Response Team (SERT), and other external partners for situational awareness on DIT incidents falling under this plan and make recommendations to the SERT on additional response and recovery actions, as appropriate.

f. Coordinate with all state, local, private and federal technical partners from a threat response perspective.

g. Provide incident response and recovery personnel and resources to affected state, local and private sector partners as appropriate and as available.

h. Establish and maintain a continuity of operations plan for reestablishing access to hosted services following a disaster.

i. Coordinate cyber training and education of state sectors.

j. Provide advisory services as it relates to the use of 3rd party incident response vendor support.

3. NC DEPARTMENT OF PUBLIC SAFETY (NCDPS)

NORTH CAROLINA EMERGENCY MANAGEMENT (NCEM)

a. Serve as one of the lead technical agencies responsible for directing technical response and recovery to an identified cybersecurity incident.
b. Serve as lead response agency responsible for coordinating SERT resources and administering the North Carolina Mutual Aid System.

c. Coordinate with Joint Cybersecurity Task Force to maintain situational awareness and address consequence management as it relates to cybersecurity incidents.

d. Operate, house, and staff the Joint Information System/Center for coordination of public messaging related to any incident (once activated).

e. Provide emergency contracting support for SERT agencies.

f. Serve as a communications link between local, state and federal government agencies for information exchange and resource requests for asset response.

g. Identify cyber related critical infrastructure and key resources.

4. NORTH CAROLINA NATIONAL GUARD (NCNG)

CYBERSECURITY RESPONSE FORCE

a. Serve as one of the lead technical agencies responsible for directing technical response and recovery to an identified cybersecurity incident.

b. Provide trained cybersecurity specialists to assist state agencies, local governments, and critical infrastructure partners in responding to ongoing cybersecurity incidents and restoration of services if available and appropriate.

c. Provide cyber subject matter experts and liaison officers to assist DIT, other state agencies, local governments, and other critical infrastructure partner agencies if available and appropriate.

d. Provide lead support and technical subject matter expertise for cyber incidents affecting private sector critical infrastructure if available and appropriate.

e. Provide incident response and recovery resources such as information assurance, applications, and network operations personnel, for affected state, local and private sector partners.

f. Collect, analyze, and share cyber threat and vulnerability information with appropriate agencies/entities on affected state, local, and private sector critical infrastructures.

g. Conduct state missions including cyber activities incident response, as directed by the Governor and as permitted by law.

C. SUPPORTING STATE AGENCIES

1. NC INFORMATION SHARING AND ANALYSIS CENTER (ISAAC) FUSION CENTER

a. Support of the lead in response to cyber incidents.

b. Gather and share information with local, state and federal law enforcement agencies. Collect and analyze law enforcement information following the incident's conclusion.

c. Provide cyber liaison capabilities between DIT, DPS, NCNG, NCLGISA Strike Team, Private Sector and other local government and federal partners.

d. Provide accurate and timely information and intelligence products and provide direct analytical support for investigations.

e. Provide investigative response and triage resources as well as support the post-incident criminal investigation and associated forensics.

f. Notify the NCCIC of cybersecurity incidents for situational awareness purposes and to provide context and to scope of the incident.

2. STATE BUREAU OF INVESTIGATION (SBI)

a. Support of the lead agency in response to cyber incidents.

b. Provide maintenance of law and order due to unrests created as a result of the cyber event.

c. Intelligence gathering and warning dissemination.

d. Direct criminal investigation of a cyber event or coordination with federal entities.

e. In coordination with NCEM provide support for cyber terrorist incident activities.

3. STATE HIGHWAY PATROL (SHP)

a. Support of the lead agency in response to cyber incidents.

b. Provide maintenance of law and order due to unrests created as a result of the cyber event.

D. SUPPORTING FEDERAL AGENCIES AND EXTERNAL ENTITIES

1. FEDERAL BUREAU OF INVESTIGATION (FBI)

a. Serve as members of the Joint Cybersecurity Task Force.

b. Provide support with threat intelligence, information sharing, and investigation support as requested and dictated by the cyber incident.

c. Provide technical support capabilities for incident response and investigations.

d. Leverage the National Cyber Investigative Joint Task Force to augment investigations.

e. Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.

2. DHS CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA)

a. Serve as members of the Joint Cybersecurity Task Force.

b. Provide 24x7 cyber situational awareness, incident response, and management center resources.

c. Share information among public and private sectors to provide a common operating picture of vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

d. Facilitate coordination regarding cybersecurity risks and incidents across the civilian communities, SLTT governments, and the private sector.

e. Provide federal asset response support to the private sector in the form of on-site technical assistance (if requested by the impacted entity).

f. Reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community.

g. Coordinate efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors.

h. Act as the primary platform to coordinate the federal government's asset response to cyber incidents.

i. Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

3. U.S. SECRET SERVICE (USSS)

a. Serve as members of the Joint Cybersecurity Task Force.

b. Provide support with threat intelligence, information sharing, and investigation support as requested and dictated by the cyber incident.

c. Provide technical support capabilities for incident response and investigations.

d. Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.

4. MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER (MS-ISAC)

a. Provide additional support for forensics, continuous monitoring, SME consulting and awareness materials.

b. Act as a focal point for critical information exchange and coordination between the SLTT community and the federal government.

5. NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE (NCIJTF)

a. Serve as the lead federal agency for threat response activities.

b. Reports cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the federal government.

IV. CONCEPT OF OPERATIONS

A. GENERAL

The normal operation and maintenance of statewide information technology infrastructure is shared between multiple state, local, and private sector agencies and the Department of Information Technology (DIT). Many agencies maintain their own systems using internal IT staff and resources. DIT operates and maintains enterprise services, data centers, and other functions used throughout state government. DIT also operates several of the primary internet gateways used by state agencies and provides perimeter monitoring of traffic into and out of many areas of the state's network. These entities, working collaboratively, will provide the technical expertise and resources required to respond to and recover from a cybersecurity incident. North Carolina Emergency Management will support the technical response and recovery effort through coordination of SERT resources, public messaging via the Joint Information System/Center, and requests for resources (as required).

State agencies are responsible for creating and maintaining cyber incident response and business continuity plans that describe how the agency will respond to and recover from cybersecurity incidents. These plans define specific roles, responsibilities, and procedures for agency personnel. The plans are maintained by each agency's Chief Information Security Officer or designee, as well as by the DIT Enterprise Security and Risk Management Office (ESRMO).

Cybersecurity incidents affecting local government critical infrastructure systems will be supported by the Joint Cybersecurity Task Force. Localities can request JCTF assistance through established emergency management processes. Cybersecurity incidents affecting privately owned critical infrastructure should be managed by the infrastructure owner/operator. If additional resources are needed, private owners/operators should exhaust all existing support channels before requesting assistance from the state.

B. NOTIFICATION

1. STATE NOTIFICATION

In accordance with N.C.G.S. § 143B-1379 state agencies that experience an information security incident will notify the DIT Enterprise Security and Risk Management Office (ESRMO) within 24 hours of confirmation.

Notification can occur through the following mechanisms:

Online: https://it.nc.gov/cybersecurity-situation-report

Telephone: 1-800-722-3946.

Local government and private partners may report confirmed and suspected incidents affecting their operations to the NCEM 24-Hour Operations Center for situational awareness and information sharing purposes at 919-733-3300. The ESRMO will make appropriate notifications to lead and supporting agencies as described in this annex and any other external entities as required. Based on the severity of the situation, the SERT Leader may request supporting agencies to participate in coordination conference calls or report to the State Emergency Operations Center (EOC). Note: If the incident is reported to DHS or FBI, the Secretary of Public Safety/Homeland Security Advisor will be notified to ensure coordinated messaging.

2. FEDERAL NOTIFICATION

The National Cyber Incident Response Plan outlines the activities and focus of the supporting federal agencies. Upon receiving a report of a cyber incident, the federal government will promptly focus its efforts on two activities: threat response and asset response.

- Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter malicious cyber activity.

- Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community and mitigating potential privacy risks to affected entity. The state will leverage the below reporting chain for efficiency and standardization of processes.

DIT will ensure that all federal threat and asset response supporting agencies are notified appropriately (see contact details in Table 1).

Threat Response
Federal Bureau of Investigation (FBI): FBI Field Office Cyber Task Forces: http://www.fbi.gov/contactus/field Internet Crime Complaint Center (IC3): https://www.ic3.gov
National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center: cywatch@fbi.gov or (855) 292-3937
United States Secret Service (USSS) Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices
United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI) HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or www.ice.gov/webform/hsi-tip-form HSI Field Offices: https://www.ice.gov/contact/hsi HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes
Asset response
National Cybersecurity and Communications Integration Center (NCCIC) (888) 282-0870 or NCCIC@hq.dhs.gov United States Computer Emergency Readiness Team: http://www.us-cert.gov

Table 1 Key Federal Threat and Asset Response Supporting Agencies

3. PUBLIC NOTIFICATION

DIT and NCEM will coordinate through the JIS to provide public information for any incident affecting state entities or critical infrastructure. The impacted entity shall provide a representative to the JIS to ensure consistency and coordination.

C. RESPONSE AND RECOVERY ACTIONS

The state will leverage the NCCIC Cyber Incident Scoring System (NCISS) in order to assess the impact and severity of a cyber incident. The various levels outlined in Table 2 will only be determined after an impact assessment has been conducted and will factor the likelihood of the threat materializing. North Carolina defines “significant cyber incident” as any incident with the classification level of High, Severe, or Emergency. For incidents impacting

state resources, appropriate members of the JCTF will determine the extent of a response.

The JCTF will be responsible for classifying the cyber disruption level. An upgrade may occur if there is substantial intelligence received to indicate a need or if a cyber incident has increased in its overall impact to the affected areas. Increasing the response action and stages is accomplished as an effort to prevent the incident from spreading. Increasing the cyber level should be managed gradually and an assessment conducted regularly throughout the process.
In order to downgrade the level, careful assessment must be conducted. A downgrade will only occur once there is confirmation that the indicators leading to the declaration have been neutralized. Similar to upgrade procedures, downgrading will occur incrementally.

It is important to note that a cyber disruption level may be declared prior to an actual cyber incident occurring and without any attributed impact. This declaration could be made as a result of actionable and targeted intelligence received. The severity levels, description and baseline cyber support responses are captured in table 2:

CYBER DISRUPTION ESCALATION PROTOCOL			
LEVEL	**COLOR**	**DESCRIPTION / IMPACT**	**BASELINE CYBER SUPPORT**
Emergency	**Black**	Poses an imminent threat to the provision of wide-scale critical infrastructure services, state government stability, or the lives of North Carolina residents.	State of Emergency is declared. Full Cyber package which may contain National Guard, Private Sector, State and Federal Cyber resources. EMAC support may be requested. Incident reporting by affected party is mandatory.
Severe	**Red**	Likely to result in a significant impact to public health or safety, economic security, foreign relations, or civil liberties. Involvement of any actual, suspected, or potential breach of bulk Restricted or Confidential Data.	State of Emergency is declared. Full Cyber package which may contain National Guard Defensive Cyber Operations, Private Sector and State Cyber resources. Incident reporting by affected party is mandatory.

CYBER DISRUPTION ESCALATION PROTOCOL			
LEVEL	**COLOR**	**DESCRIPTION / IMPACT**	**BASELINE CYBER SUPPORT**
		Immediate attention required including the engagement of Data Owners and performing short-term containment including taking down potentially compromised systems and applications. Multiple systems likely to be exploited with high criticality to business functionality.	
High	**Orange**	Likely to result in a demonstrable impact to public health or safety, economic security, foreign relations, civil liberties, public confidence or state/agency reputation. Serious attempt or actual interruption in availability, or negative impact to confidentiality or integrity or Data Breach. Repeated or persistent Medium Incident. May include systems with low to moderate criticalities which are affected by vulnerabilities likely to be exploited.	The state will activate MOU with National Guard Defensive Cyber Operations Team and provide onsite cyber recovery and remediation support. Incident reporting by affected party is mandatory.
Medium	**Yellow**	May impact public health or safety, economic security, foreign relations, civil liberties, public confidence or state/agency reputation. One instance of a clear attempt to obtain unauthorized information or access; a repeated or persistent low incident. May also include the accidental internal exposure of employee records. May also include vulnerabilities with a rare rate of occurrence on	The state may provide remote cyber support and consultation services. Incident reporting is mandatory

CYBER DISRUPTION ESCALATION PROTOCOL			
LEVEL	**COLOR**	**DESCRIPTION / IMPACT**	**BASELINE CYBER SUPPORT**
		critical systems.	
Low	**Green**	Unlikely to result in a demonstrable impact to public health or safety, economic security, foreign relations, civil liberties, public confidence or state/agency reputation. One instance of potentially unfriendly activity (e.g., port scan, malware detections, unexpected performance peak, observation of potentially malicious user activity, theft of a device, etc.	State resources will not be deployed; however, incident reporting is required from the affected party. The state may provide recommendations as requested. Incident reporting by affected party is mandatory.

Table 2 Cyber Disruption Escalation Protocol and Levels

INCIDENT RESPONSE PROCESS

In the event that this plan is activated, the lead technical agency, supported by the JCTF will use the following process flow diagram throughout the cyber incident response (see Figure 1.)

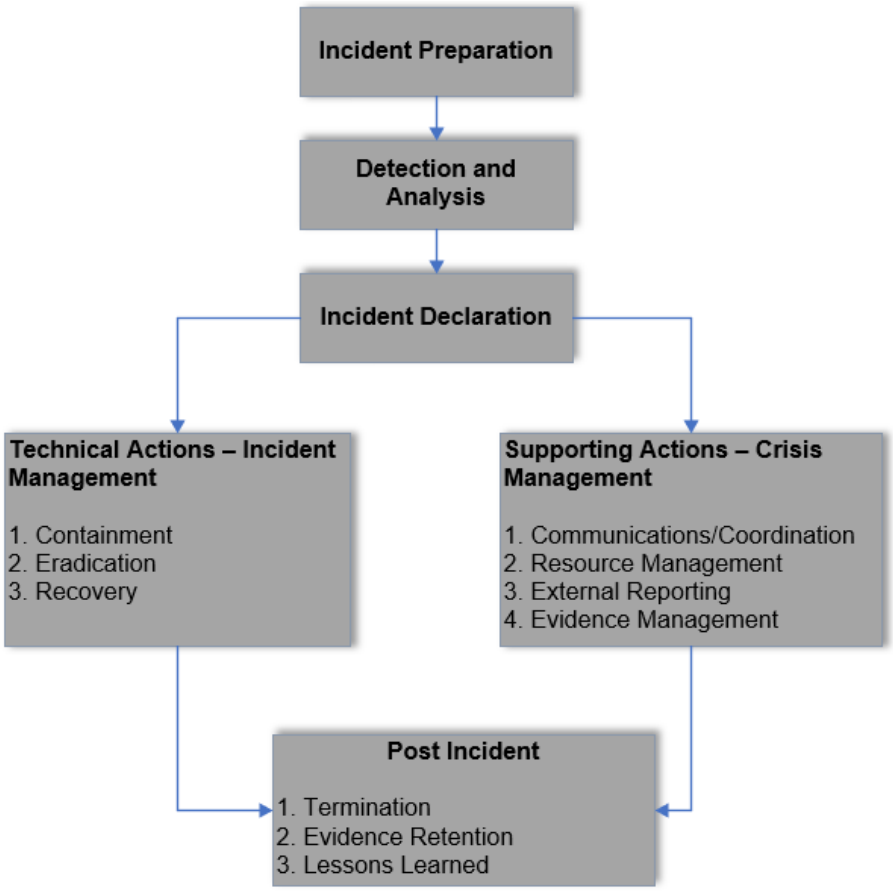


Figure 1 Incident Response Phases

1. PREPARATION

a. The JCTF will maintain situational awareness of cybersecurity threats through a variety of federal, state, and private sector information-sharing resources.

b. The State SOC is located in DIT and is managed 24 hours per day. The State SOC leads the coordination and response efforts in assessing and managing cyber incidents affecting the state government networks.

2. DETECTION AND ANALYSIS

a. The JCTF will assess the extent and severity of the cybersecurity incident through analysis of log files, audit trails, system contents, or other indicators of compromise. The JCTF determines the level of response required to respond to incidents and directs the utilization of agency resources to minimize incident exposure. Once the severity level has been identified, the JCTF will make the necessary coordination activities as needed.

b. If any data classified as restricted, highly restricted or other protected information is confirmed to be compromised the affected entity will immediately notify the JCTF as indicated in above notification procedures and any other authorities required by laws or appropriate regulations.

3. INCIDENT DECLARATION

a. The Joint Information System/Center (JIS/JIC) will be activated to coordinate public messaging and media requests. SERT partners may be asked to augment personnel to staff the Joint Information Center (as required).

b. The Joint Cybersecurity Mission Center (JCMC) located at the State EOC will be used as the primary location for coordination of all operational response activities and resource allocations. This coordination includes communicating significant cyber incident related situational awareness and activities to State EOC partners, the Governor's office, NCCIC, and the HSA to monitor and prepare for the possible onset of any further consequences.

4. CONTAINMENT

a. The JCTF will coordinate and/or provide technical support to the impacted entity to take appropriate measures to isolate, contain or mitigate further service disruptions related the cybersecurity incident.

    i. Law enforcement agencies may request that intrusions continue for a limited period of time in order to facilitate collection of evidence and techniques, tactics, and procedures (TTPs). These requests will be considered on a situationally dependent basis in coordination with JCTF and the affected entity.

b. Once the method of intrusion/compromise is known, the affected entity(s) will implement corrective actions to reduce the risk of further disruption. During this phase, it is important that all stakeholders maintain situational awareness. The JCTF will provide information technology support for collaboration tools and services as needed.

c. The JIS/JIC will publish regular press releases updating the public on response activities and respond to information requests, as appropriate.

5. ERADICATION

a. When the incident has been contained, the JCTF will coordinate and provide technical support to the affected entity to ensure that mandatory forensics is conducted on all impacted systems, networks, infrastructure to ensure against residual vulnerabilities.

b. Audit trails, log files, and other forensic information should be retained to the greatest extent that is reasonably feasible for the purposes of later analysis and investigation.

c. The JIS/JIC will continue to provide public messaging and information request support for the affected entity(s) and SERT partners.

6. RECOVERY

a. For affected agencies, the JCTF will assist in the restoration and recovery efforts to restore services and return state information technology infrastructure to normal operations. DIT will lead this effort when state agencies are affected. Restoration may include actions such as restore from “clean” backups or software installations, replacement of damaged/unrecoverable equipment, or rebuilding/restoration of systems.

b. All affected entities should validate configurations using approved configuration baselines, (e.g. Security and Technical Implementation Guides (STIGS)), CIS benchmarks and vulnerability testing to ensure systems are no longer susceptible to various methods of attack, prior to being placed into production.

c. NCEM will coordinate SERT activities in support of the recovery effort.

d. The JIS/JIC will publish regular press releases updating the public on recovery activities and respond to information requests until transitioning public messaging activities back to individual agencies.

7. LESSONS LEARNED

a. The JCTF will work with the affected entity to identify policy options or best practices that could prevent similar incidents in the future or improve the overall state's defense and response capabilities.

b. The JCTF may also recommend and/or coordinate implementation of such actions statewide, including with local government entities. The affected entity has the lead to collect documentation resulting from the incident for post incident analysis and TTP modifications.

V. DIRECTION CONTROL AND COORDINATION

A. LOCAL

The agency responsible for the operation and maintenance of local government information technology infrastructure varies between jurisdictions. All local government activities to respond and recover from cybersecurity incidents will be conducted in accordance with established local policies and plans. Local governments may be able to obtain required resources from neighboring jurisdictions through mutual aid agreements.

B. STATE

State assistance may be requested through emergency management channels if the incident exhausts local government resources. State response activities will be coordinated through the SERT. The SERT will have overall incident command for the response and recovery operation. The State Chief Information Officer or their designee will serve as the primary agency technical advisor to the SERT during the response and recovery phases of the incident. The SERT may request support from other states through the Emergency Management Assistance Compact (EMAC).

In the event of an exceptionally severe or widespread disruption the Governor or General Assembly may declare a state of emergency in accordance with the North Carolina Emergency Management Act and as described in the North Carolina Emergency Operations Plan.

C. FEDERAL

In the event an incident exceeds state capabilities or there is a need for federal resources, the state may request federal assistance through the US-CERT, MS-ISAC, DHS and/or NSA. Depending on the need, the National Cyber Incident Response Plan identifies when reporting to the federal government is appropriate. The following are listed as reportable cyber incidents:

- Result in a significant loss of data, system availability, or control of systems;
- Impact 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; or
- Impact national security, economic security, or public health and safety.

VI. REFERENCES

A. N.C.G.S. § 143B-1376. Statewide security standards

B. N.C.G.S. § 143B-1379. State agency cooperation; liaisons

C. N.C.G.S.§ 143B-1377. State CIO approval of security standards and risk assessments

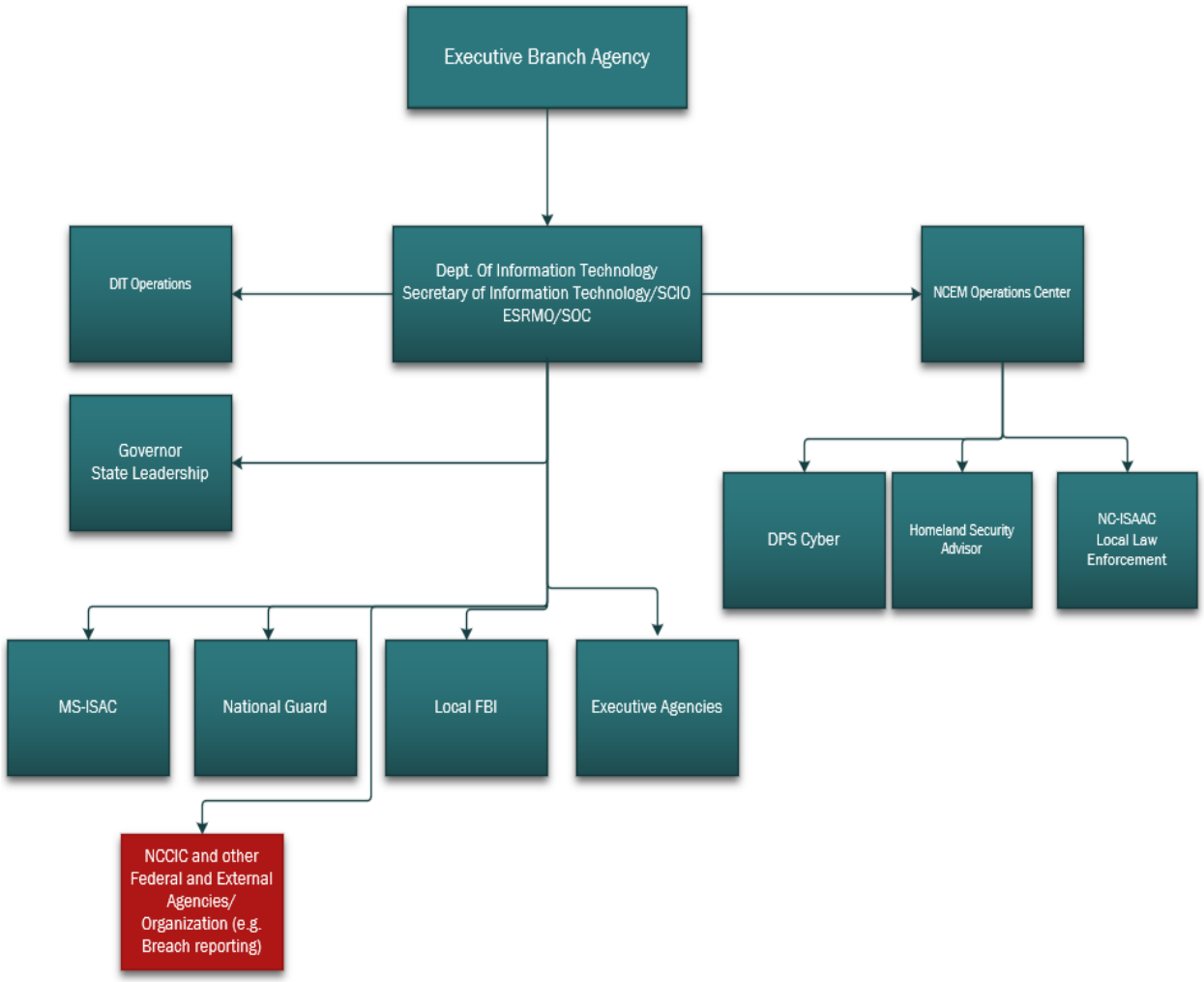
D. N.C.G.S. § 75-65. Protection from security breaches

E. N.C.G.S. § 75-60. Identity Theft Protection Act

F. N.C.G.S. §§166A North Carolina Emergency Management Act

G. National Cyber Incident Response Plan, 2016

ATTACHMENT A – SIGNIFICANT CYBER INCIDENTS AFFECTING STATE AGENCY(S) NOTIFICATION PROCESS



ATTACHMENT B – SIGNIFICANT CYBER INCIDENTS AFFECTING LOCAL GOVERNMENT OR OTHER NON-STATE ENTITY(S) NOTIFICATION PROCESS