APPENDIX 16

(SOUTH CAROLINA CYBER CONSEQUENCE MANAGEMENT PLAN)

TO THE SOUTH CAROLINA EMERGENCY OPERATIONS PLAN

I. INTRODUCTION

A. As required by state and federal law, South Carolina's policy is to be prepared for any emergency or disaster, including cyber incidents. A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems, which can lead to long-term unforeseen, cascading, and far-reaching consequences.

B. South Carolina State Regulations 58-1 and 58-101 require contingency plans and implementing procedures for major hazards, such as cyber incidents, coordinated by the State with counties that have a potential of being impacted.

II. PURPOSE

A. Provide a defined process for a coordinated and efficient response to the physical effects of a significant cyber incident within the State of South Carolina.

B. Define the roles and responsibilities for State Emergency Response Team (SERT) personnel to save lives and minimize physical damage to property and infrastructure (separate of computer or cyber-specific resources).

III. SCOPE

A. This plan is limited to the State of South Carolina's consequence management response to and recovery from the physical effects of a significant cyber incident. This includes cyber incidents occurring outside of the state but impacting critical systems and supply chains in South Carolina.

B. This plan is not designed to direct, nor does it specifically address the State's technical response to any specific public or private sector computer network to assist in the mitigation or recovery of any business enterprise or industrial control system. That response is led by the South Carolina Critical Infrastructure Cybersecurity (SC CIC) program and guided by the SC CIC Operational Plan.

C. Any cyber incident impacting private or public networks within South Carolina may be considered a criminal act. Criminal acts and resulting criminal investigative actions, to include the investigation, attribution, and apprehension of suspected threat actors, fall under the purview of the South Carolina Law Enforcement Division (SLED) or other federal law enforcement entities and are not addressed within the scope of this plan.

IV. FACTS AND ASSUMPTIONS

A. Facts

1. A significant cyber incident can occur at any time and with little or no warning. It may involve single or multiple governmental jurisdictions and geographic areas.

2. A significant cyber incident will require a coordinated consequence management effort from all levels of government, volunteer organizations, and private sector partners. No single private sector entity or local, tribal, state, or federal government agency possesses the authority or expertise to act unilaterally.

3. Recognizing that significant cyber incidents are a threat to the electronic infrastructure that supports the social, health, safety, and economic well-being of the citizens of South Carolina, Governor McMaster issued Executive Order 2017-08, establishing the South Carolina Critical Infrastructure Cybersecurity Executive Oversight Group.

B. Assumptions

1. Significant cyber incidents may disrupt, degrade, destroy information, or deny the use of critical assets (e.g., electric power and water industrial controls and telecommunication networks). Consequences associated with these events could overwhelm both public and private sector resources.

2. Reliable and secure alternate communication systems will be required to enable a coordinated multi-agency response in the event that current communication systems are inoperable.

3. The impact to lifeline sectors could significantly impede response and recovery efforts.

V. SITUATION

A. According to the National Cyber Incident Response Plan, the frequency of cyber incidents is increasing. The most significant cyber incidents have the capability to result in demonstrable harm and require deliberate planning, coordination, and exercises to respond effectively.

B. Based on current reporting, various nation-state adversaries and non-state actors (cyber criminals, terrorist groups, insider threats, and/or hackers) have demonstrated the intent and capability to gain unauthorized access, exploit, and/or attack both public and private sector computer networks.

C. Cyber insurance can offset costs from some of the most common cyber risks, such as data breaches and ransomware. However, private insurers have been taking steps to limit their potential losses so that costs to repair or replace damaged infrastructure systems may not be covered.

D. Significant cyber incidents initiate cascading effects that could affect each phase of emergency management and include interdependencies between lifeline sectors.

E. Interconnected computer networks regulate the flow of electrical power, natural gas, fuel, water, solid waste, financial services, medical care, public safety, telecommunications, and transportation systems. The consequences of a significant cyber incident could cause significant disruption to lifeline sector services as well as economic losses for South Carolina.

F. Coordination and communication between government agencies and private sector owner/operators will be critical to an effective response and recovery effort.

VI. CONCEPT OF OPERATIONS

A. Crisis Management vs. Consequence Management.

1. Response to a significant cyber incident includes two major primary functions: crisis management and consequence management, which may be carried out consecutively or concurrently.

2. Definitions:

a. Crisis Management – Crisis management refers to measures that identify, acquire, and employ resources to anticipate, prevent, and/or mitigate a threat, to include the forensic work to identify the adversary.

b. Consequence Management – Consequence management refers to the measures taken to manage the physical effects of the crisis. This may include evacuation of populations, restoration of essential services, and recovery from the crisis event.

3. Crisis Management

a. SLED, through the SC CIC taskforce, is the lead agency for crisis management response to a significant cyber incident.

b. Crisis management of a significant cyber incident may include coordinating support to an affected computer network(s).

c. Additional resources from the federal government and private sector may be called upon to assist the state in the crisis management response.

d. Officials coordinating crisis management actions are obliged to protect sensitive investigative and operational data to support attribution and the possible prosecution of the threat actors. However, they will provide incident situational awareness information and threat data to interagency partners, to include SC CIC and the State Emergency Operations Center (SEOC).

4. Consequence Management

a. South Carolina Emergency Management Division (SCEMD) is the lead agency for the consequence management response to a significant cyber incident.

b. The primary focus of consequence management response and recovery efforts as identified in this plan will be on reducing impacts to the state's lifeline sectors. Following guidance from the Federal Emergency Management Agency (FEMA), the lifeline sectors in South Carolina are identified as:

(1) Safety and Security

(2) Food, Hydration, Shelter

(3) Health and Medical

(4) Energy (Power & Fuel)

(5) Communications

(6) Transportation

(7) Hazardous Materials

(8) Water Systems

c. Consequence management activities begin as soon as possible and may continue well beyond the conclusion of crisis management.

d. These activities include but are not limited to:

(1) Protecting public health and safety.

(2) Restoring essential government services.

(3) Providing emergency relief to governments, businesses, and individuals affected by the consequences of the significant cyber incident.

B. SEOC Activation.

The SEOC will activate based on:

1. The level of requested support;

2. The need to gain situational awareness of the incident; and/or

3. Upon the direction of the Governor.

C. Direction and Control

1. The SEOC will serve as the State's central coordination point for consequence management response during a significant cyber incident.

2. Liaisons

a. SCEMD will dispatch liaison(s) to affected county Emergency Operations Centers (EOC) as required or as requested.

b. The SCEMD liaison will assist the county in providing consequence management information to the SEOC for situational awareness and in coordinating resource requests.

3. Based on the situation, and in conjunction with intergovernmental partners and the private sector, a Unified Coordination Group (UCG) may be implemented for consequence management of the incident.

4. Throughout the incident, state agencies will report and coordinate event-related information to the SEOC.

D. Public Information

1. The SLED Public Information Officer (PIO) will be the lead PIO for the overall response to the cyber event. As the incident transitions to consequence management, SCEMD will assume the lead.

2. ESF-15 (Public Information) will be the main point of contact for consequence management messaging and SEOC communications. ESF-15 will coordinate all potentially law enforcement sensitive PIO messages through the Governor's Office and the Joint Information Center (JIC) and/or lead state PIO. The public will be made aware of potential adverse effects and of actions recommended to safeguard lives and property.

3. Public information releases from state and local agencies will be coordinated with the JIC or designated lead state PIO prior to dissemination.

4. See Annex 15 (Public Information) to the South Carolina Emergency Operations Plan (SCEOP) for additional information.

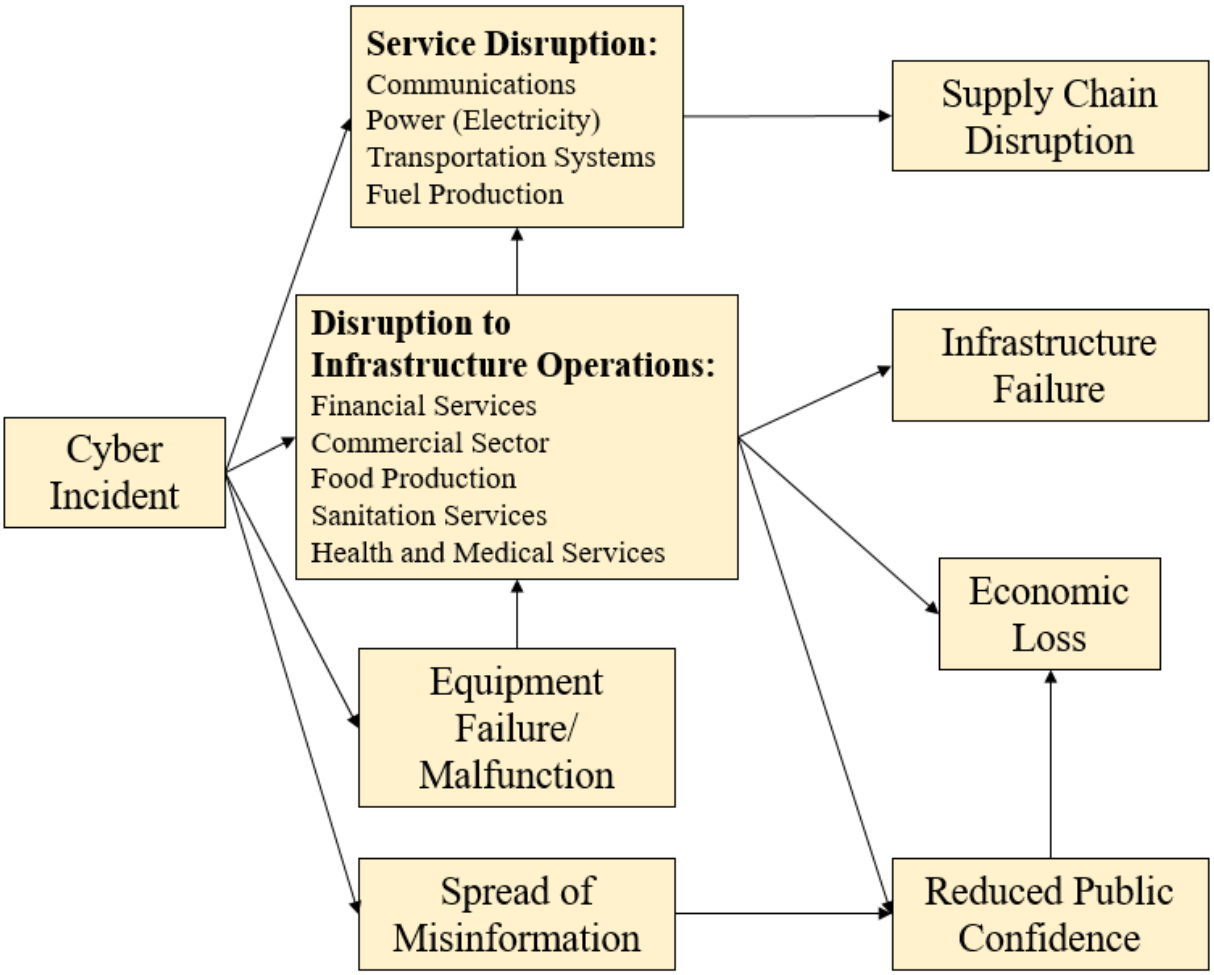
VII. DISASTER INTELLIGENCE AND COMMUNICATIONS

A. See Section VIII (Disaster Intelligence and Communications) of the SCEOP.

B. Lifeline Sector Analysis

1. All lifeline sectors can be disrupted by a significant cyber incident, with the impacts varying widely based on the specific cyber incident.

2. The flowchart below gives a basic analysis of potential cascading impacts following a cyber incident. Additional impacts by lifeline sector are listed within the annexes to this plan.



VIII. ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

A. See Section IX (Organization and Assignment of Responsibilities) of the SCEOP for the general roles and responsibilities of county, state, and federal agencies in preparation, response, and recovery from a disaster impacting the State.

B. Organization

1. The Executive Group, consisting of state agency directors/representatives and key advisors as needed, will advise and assist the Governor in executive-level decision making.

2. Due to the unique threat posed by a significant cyber incident, management of the event may also require the establishment of a smaller Unified Coordination Group (UCG) in addition to the Executive Group.

   a. Individuals assigned to the UCG will vary depending upon the nature and scope of the significant cyber incident. At a minimum, SLED and SCEMD will be a part of the UCG.

   b. Senior leaders from additional state agencies, the federal government, local jurisdictions, the private sector, and/or non-governmental organizations could be added to the UCG as necessary based on the specific cyber incident.

3. SC CIC will serve as the state's information sharing hub during the response to and recovery from a significant cyber incident.

4. The Disaster Intelligence Group (DIG) will serve as the interface to SC CIC at the SEOC.

C. Responsibilities

1. South Carolina Emergency Management Division (SCEMD)

   a. Lead agency for coordinating the State's consequence management efforts in response to and recovery from the physical effects of a significant cyber incident.

   b. Through the DIG, coordinate with SLED and SC CIC to identify any possible follow-on actions a cyber adversary could take that could cause additional impacts to lifeline sectors within South Carolina.

   c. Coordinate with federal partners regarding consequence management response to and recovery from a significant cyber incident.

2. South Carolina Law Enforcement Division (SLED)

   a. Lead agency for the state's crisis management efforts in response to and recovery from the virtual effects of a significant cyber incident.

   b. Lead agency for the criminal investigation of a significant cyber incident.

   c. Through SC CIC, coordinate with state and federal partners in threat response, asset (network) response, intelligence, and information sharing of a significant cyber incident.

   d. Function as the state's hub for indications and warning, information sharing, non-technical threat data, and notification of significant cyber incident information through SC CIC.

   e. In accordance with the ESF-13 (Law Enforcement) Annex, provide a liaison from SC CIC to the SEOC to integrate with ESF-13 and provide situational awareness to the Executive Group.

3. Emergency Support Functions (ESFs)

   a. Upon notification of SEOC activation from a significant cyber incident, prepare personnel, equipment, and other resources to staff the SEOC and/or perform duties as listed in Section IX (Organization and Assignment of Responsibilities) of the SCEOP.

   b. Maintain situational awareness on the cyber threat to critical resources and assets in South Carolina.

   c. Ensure possible physical consequences resulting from cyber threats are reported to the SEOC.

   d. Coordinate with the SERT on the identification of lifeline sector interdependencies following a significant cyber incident.

4. Federal

   The national roles and responsibilities in response to a significant cyber incident are established and outlined within the National Cyber Incident Response Plan.

5. Private Sector

   a. The private sector is organized around multiple business model constructs based on their individual risk management criteria.

b. Many larger corporations have developed internal emergency operations and business continuity elements within their organizations to support cyber event response and recovery operations.

IX. ADMINISTRATION, LOGISTICS, AND FINANCE

A. Administration and Finance. See Annex 7 (Finance and Administration) to the SCEOP.

B. Logistics. See Attachment A (SC Logistics Plan) to the SCEOP.

X. CONTINUITY OF GOVERNMENT (COG)

See Section VII (Concept of Operations), Paragraph L (Continuity of Government) of the SCEOP.

XI. CONTINUITY OF OPERATIONS (COOP)

See Section VII (Concept of Operations), Paragraph M (Continuity of Operations) of the SCEOP.

XII. PLAN DEVELOPMENT & MAINTENANCE

A. SCEMD is the lead agency for the development, coordination, review, and updating of this plan.

B. As a minimum, SCEMD will review and update this appendix on a biennial basis. The review will include any updates to the National Response Framework (NRF), National Incident Management System (NIMS) and other relevant State and Federal guidance.

XIII. AUTHORITIES & REFERENCES

A. Authorities

1. See Attachment C of the SCEOP.

2. South Carolina Executive Order 2017-08 Establishing the South Carolina Critical Infrastructure Cybersecurity Executive Oversight Group

B. References

1. National Cyber Incident Response Plan, December 2016

2. South Carolina Critical Infrastructure Cybersecurity Operations Plan

XIV. ANNEXES

Annexes have been developed for responding to incidents associated with the following:

A. Water/Wastewater System

B. Electric Grid (published separately as the Long-Term Power Outage Plan, Appendix 15 to the SCEOP)

C. Refined Oil/Fuel (published separately as the Emergency Refuel Plan, Appendix 9 to the SCEOP)