APPENDIX 16

(SOUTH CAROLINA CYBER INCIDENT CONSEQUENCE MANAGEMENT PLAN)

TO THE SOUTH CAROLINA EMERGENCY OPERATIONS PLAN

I. INTRODUCTION

A. General

1. The South Carolina Cyber Incident Consequence Management Plan provides a defined process for a coordinated and efficient response to the physical effects of a Significant Cyber Incident within the State of South Carolina.

2. The plan defines the roles and responsibilities for intergovernmental and State Emergency Response Team (SERT) personnel to save lives and minimize the physical damage to property and infrastructure separate of actual computer or cyber specific resources.

3. Critical Infrastructure/Key Resources (CI/KR) vary greatly depending upon the level of government and jurisdictional needs. For the purposes of this plan, the definition of Critical Infrastructure/Key Resources is limited to the CI/KR located within South Carolina as defined within the 16 sectors identified by the Department of Homeland Security (DHS) and any facilities located outside state borders that would impact security, economic security or public health and safety as identified by the South Carolina Law Enforcement Division (SLED) Homeland Security Office.

4. This plan assigns an ESF to each sector of critical infrastructure (CI) as defined by DHS (See Table 1). However, the primary focus of consequence management response and recovery efforts as identified in this plan will be on the life-line sectors of CI. These life-line sectors are identified as:

   a. Transportation – ESF 1

   b. Communications – ESF 2

   c. Water / Wastewater – ESF 3

   d. Public Health – ESF 8

   e. Energy – ESF 12

B. Cyber Preparedness vs. Cyber Security. Cyber preparedness differs from cyber security in planning and operational focus.

1. Cyber Preparedness focuses on preparing for, responding to, mitigating and recovering from the cascading effects that occur in the physical environment as a result of a Significant Cyber Incident.

2. Cyber Security focuses on Computer Network Defense (CND) and seeks to prevent the unauthorized access, damage to, or illicit use of the computer network including the mitigation of threats once discovered.

C. The National Cyber Incident Response Plan (NCIRP), following guidance from Presidential Policy Directive 41 (PPD-41), has identified and defined two levels of cyber incidents that could impact the United States:

1. Cyber Incident – *An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information system, or information resident thereon.*

2. Significant Cyber Incident – *A cyber incident that is (or a group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the united States or to the public confidence, civil liberties, or public health and safety of the American people.*

II. PURPOSE

A. Provide a framework that provides for the flexibility required to plan and coordinate the operational procedures South Carolina will use in-consequence management to the physical effects of a Significant Cyber Incident endangering public health and safety, quality of life, or prevents or inhibits the provision of essential governmental services.

B. Identify and define the roles and responsibilities of the State, and State and Federal agencies, in providing resources to assist county and local governments in responding to and recovering from the negative physical effects from a Significant Cyber Incident affecting people and infrastructure located within their jurisdictions.

C. Identify ESF/SERT actions and responsibilities specific to a Significant Cyber Incident that are in addition to the responsibilities already outlined in the South Carolina Emergency Operations Plan (SCEOP) and its Annexes.

D. Incorporate the coordination mechanisms and structures of appropriate state, county, municipal, and private-sector plans into the overall consequence management response.

E. Identify and provide a process to mobilize state resources and conduct activities to guide and support local emergency management efforts through preparedness, response, recovery, and mitigation planning for the physical effects of a Significant Cyber Incident.

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.

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.

C. This plan supports the South Carolina Emergency Operations Plan (SCEOP) as Appendix 16.

IV. ASSUMPTIONS

A. 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.

B. A Significant Cyber Incident that disrupts CI/KR may occur at any time and with little or no warning. It may involve single or multiple governmental jurisdictions and geographic areas.

C. 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.

D. Significant Cyber Incidents may disrupt, degrade, destroy information, or deny the use of CI/KR (e.g., electric power and water industrial controls and telecommunication networks). Consequences associated with these events could overwhelm both public and private sector resources.

E. The impact to life-line critical infrastructure (e.g., water/wastewater, energy, transportation, communications, and public health infrastructures) could significantly impede response and recovery efforts.

F. Private-sector owner/operators of CI/KR resources located within South Carolina are vulnerable to cyber threats.

V. SITUATION

A. DHS has identified cyber related threats as a "threat and hazard of significant concern" in over half of the 16 designated sectors of Critical Infrastructure (CI).

B. This plan (SC Cyber Incident Plan) outlines the state's consequence management response and recovery to the physical effects of a Significant Cyber Incident.

C. Based on current reporting, various nation-state adversaries and non-state actors have demonstrated the intent and capability to gain unauthorized access, exploit and/or attack both public and private sector computer networks.

D. First-order dependencies and interdependencies between CI/KR sectors create vulnerabilities that can cause cascading negative effects to the physical environment and the citizens of South Carolina.

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

F. Coordination and communication with CI/KR private sector owner/operators will be critical to an effective response and recovery effort.

G. Significant cyber incidents initiate cascading effects that could affect each phase of emergency management including preparedness, response, recovery and mitigation.

H. 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 of CI/KR operations and economic losses for South Carolina.

I. 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.

VI. ORGANIZATION & ASSIGNMENT OF RESPONSIBILITIES

A. Organization

1. County: The counties will respond to the physical effects of a Significant Cyber Incident based upon their established All-Hazards plans and organizations.

2. State: Due to the unique threat posed by a Significant Cyber Incident, management of the event would require the establishment of a state level Unified Coordination Group (UCG).

a. The UCG will be comprised of senior leaders representing State and Federal interests, and in certain circumstances tribal governments,

local jurisdictions, the private sector, and/or non-governmental organizations (NGO).

b. Individuals assigned to the UCG will vary depending upon the nature and scope of the Significant Cyber Incident.

c. Assignment to the UCG will require individuals from the public and private sector with the appropriate authorities to inform and provide recommendations to state executive leadership.

d. The South Carolina Intelligence and Information Center (SCIIC) will serve as the state's information sharing hub during the response to and recovery from a Significant Cyber Incident.

e. The Joint Disaster Intelligence Analysis Cell will serve as the interface to the SCIIC at the SEOC.

3. Private-Sector

a. CI/KR owner/operators are 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.

B. Responsibilities

1. County: Counties are responsible for providing capability to support operations in response to the physical effects of a Significant Cyber Incident.

2. State

a. General Responsibilities

(1) Responsible for the State's cyber preparedness, response, recovery planning and operations.

(2) The identification of key individuals and organizations within South Carolina that will act as liaisons to county, federal, and private sector partners.

(3) Provide coordination with and support to Federal departments and agencies on response activities related to state, county, local, and tribal priorities and systems.

(4) When necessary, coordinate with other states and territories regarding Significant Cyber Incident response and recovery operations.

(5) Maintain situational awareness regarding current cyber threats and disseminate date to intergovernmental and interagency partners.

b. South Carolina Emergency Management Division

(1) Lead agency for the State's consequence management efforts in response to and recovery from the physical effects of a Significant Cyber Incident.

(2) Through the Joint Disaster Intelligence and Analysis Cell (JDIAC), coordinate with SLED and the SCIIC on any possible follow-on actions a cyber adversary could take that could cause additional impacts to CI within South Carolina.

(3) Coordinate with federal partners (FEMA) regarding consequence management response to and recovery from a Significant Cyber Incident.

c. South Carolina Law Enforcement Division

(1) Lead agency for the criminal investigation of a Significant Cyber Incident.

(2) Functions as the State's hub for Indications & Warning (I&W), Information Sharing, Non-Technical Threat Data, and Notification of Significant Cyber Incident information through the South Carolina Intelligence & Information Center (SCIIC).

(3) Lead state coordinating agency with federal partners in threat response, asset (network) response, intelligence and information sharing of a Significant Cyber Incident.

3. Federal

a. The national roles and responsibilities in response to a Significant Cyber Incident were established and outlined within the National Cyber Incident Response Plan (NCIRP).

b. The NCIRP implements presidential guidance from PPD-41 and is broken down into three broad roles and responsibilities:

(1) Threat Response

(a) Threat response activities are defined as "investigative, forensic, analytical, and mitigation activities, interdiction of a threat actor and providing attribution that may lead to information sharing and operational synchronization with asset response activities".

(b) The Federal Bureau of Investigation (FBI) is the lead federal department/agency responsible for Threat Response.

(2) Asset Response

(a) Asset response activities are defined as "furnishing technical assistance to affected entities, mitigating vulnerabilities, identifying additional at-risk entities and assessing their risk to the same or similar vulnerabilities."

(b) The Department of Homeland Security (DHS) is the lead federal department/agency responsible for Asset Response.

(3) Intelligence Support

(a) Intelligence support during response to a Significant Cyber Incident is defined as "activities […] to build situational threat awareness; and share of related threat indicators; analysis of threats; identify and acknowledge gaps; and ultimately create a comprehensive picture of the incident."

(b) The Office of the Director of National Intelligence is the lead federal department/agency responsible for intelligence support.

4. Private-Sector: Private Sector owner/operators of CI/KR assets assist State and County agencies and departments regarding preparedness, response, and recovery activities.

VII. CONCEPT OF OPERATIONS

A. General

1. Crisis Management vs. Consequence Management.

a. The response to a Significant Cyber Incident includes two major primary functions, Crisis Management and Consequence Management, which may be carried out consecutively or concurrently.

b. Definitions:

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

(2) Consequence Management – Consequence management refers to the measures taken to manage the physical effects of the crisis. This may include evacuation of populations, loss of utility and/or essential services, and recovery from the crisis event.

c. Crisis Management

(1) SLED is the lead agency for Crisis Management response to a Significant Cyber Incident.

(2) Crisis management of a Significant Cyber Incident may include coordinating support to an affected computer network(s).

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

(4) 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, the South Carolina Information and Intelligence Center (SCIIC), and the State Emergency Operations Center (SEOC).

d. Consequence Management

(1) Consequence Management in South Carolina is based on an All-Hazards approach designed to encompass all emergencies independent of their underlying cause. This approach would be enacted when a Significant Cyber Incident creates the possibility of cascading negative effects in the physical environment.

(2) SCEMD is the lead agency for the consequence management response to a Significant Cyber Incident.

(3) Consequence Management supports activities conducted by multiple agencies and is coordinated by emergency management.

(4) Consequence Management activities begin as soon as possible and may continue well beyond the conclusion of crisis management.

(5) These activities include but are not limited to:

(a) Protecting public health and safety

(b) Restoring essential government services

(c) Providing emergency relief to governments, businesses, and individuals affected by the consequences of the Significant Cyber Incident.

2. Due to the unique and dynamic nature of the cyber threat, a state-level coordinated effort to assist in the management of the consequences of a Significant Cyber Incident will typically be required.

3. Coordination among local, state, federal and the private sector is vital to establish and maintain situational awareness, identify any possible cascading effects, and to ensure appropriate response and recovery actions are taken.

4. The lead agencies for Crisis and Consequence Management should mutually determine when Crisis Management activities are complete.

5. This framework may be implemented with or without the activation of the SCEOP.

B. SEOC Activation. The SEOC will activate based on:

1. The level of requested support; or

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 the 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.

2. The SCEMD PIO is the lead PIO for the consequence management response to the cyber event.

3. The SCEMD PIO will coordinate with the SLED PIO and relevant PIOs on the release of information pertaining to the consequence management of the event.

E. Emergency Support Function Actions

1. General

a. The ESF actions listed within this section are specific tasks related to the consequence management of the physical effects a Significant Cyber Incident.

b. Each ESF identified represents their respective life-line sector of CI.

c. These cyber specific responsibilities fall within the consequence management response phase to a Significant Cyber Incident.

2. ESF 1 (Transportation)

a. In coordination with the JDIAC, maintain situational awareness on the cyber threat to transportation assets in South Carolina.

b. Ensure possible physical consequences resulting from cyber threats to critical Transportation infrastructure are reported to the SEOC.

c. Assist SEOC planners and analysts with the identification of Transportation sector interdependencies with other sectors of CI/KR.

3. ESF 2 (Communications)

a. In coordination with the JDIAC, maintain situational awareness on the cyber threat to communications assets in South Carolina.

b. Ensure any possible identified physical effects resulting from cyber threats to critical communications infrastructure are reported to the SEOC.

c. Assist SEOC planners and analysts with the identification of Communications sector interdependencies with other sectors of CI/KR.

4. ESF 3 (Public Works & Engineering)

a. Water/Wastewater

(1) In coordination with the JDIAC, maintain situational awareness on the cyber threat to water/wastewater assets in South Carolina.

(2) Ensure any possible identified physical effects resulting from cyber threats to critical dam and water/wastewater networks are reported to the SEOC.

(3) Assist SEOC planners and analysts with the identification of Water/Wastewater Sector interdependencies with other sectors of CI/KR.

5. ESF 8 (Health and Medical Services)

   a. In coordination with the JDIAC, maintain situational awareness on the cyber threat to Health/Public Health assets in South Carolina.

   b. Ensure any possible identified physical effects resulting from cyber threats to critical Health/Public Health infrastructure are reported to the SEOC.

   c. Assist SEOC planners and analysts with the identification of Health/Public Health sector interdependencies with other sectors of CI/KR.

6. ESF 12 (Energy)

   a. In coordination with the JDIAC, maintain situational awareness on the cyber threat to Energy infrastructure in South Carolina.

   b. Ensure any possible identified physical effects resulting from cyber threats to critical Energy infrastructure are reported to the SEOC.

   c. Assist SEOC planners and analysts with the identification of Energy sector interdependencies with other sectors of CI/KR.

7. ESF 14 (Recovery and Mitigation)

   a. Request a federal disaster declaration to seek assistance with mitigating degradation, disruption or destruction to infrastructure and infrastructure systems based on the scope and magnitude of the event.

   b. Coordinate the delivery of services as applicable under the Stafford Act and the Code of Federal Regulations.

   c. Coordinate joint damage assessments to determine the impact on housing, economic stability, infrastructure and other critical functional areas that deliver services to the citizens of the State.

   d. Request as required federal agency support as outlined in the National Disaster Recovery Framework to assist in assessments and delivery of agency specific assistance.

VIII. 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 an annual 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.

IX. AUTHORITIES & REFERENCES

A. Authorities

1. See Attachment C of the South Carolina Emergency Operations Plan, April 2018

B. References

1. Sector Risk Snapshots, DHS, May 2014

2. National Cyber Incident Response Plan (Draft), DHS, September 2016