Nevada Division of Emergency Management Cybersecurity Consequence Management

The primary focus of consequence management response and recovery efforts as identified in this plan will be on the lifeline sectors of critical infrastructure (CI). Following guidance from the Federal Emergency Management Agency (FEMA), the lifeline sectors in Nevada are identified as:

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

A. 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.

B. 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.

DEM's consequence management preparedness, response to, and recovery from the physical effects of a significant cyber incident. Cyber incidents occurring outside of the state but impacting critical systems and supply chains in Nevada are also a concern.

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.

II. Crisis Management vs. Consequence Management

A. 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 that 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. The Nevada Cyber Security Task Force (CSTF) and the Office of Cyber Defense Coordination (OCDC) are the lead groups for crisis management response to a significant cyber incident.

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

D. Consequence Management

1. DEM is the lead agency for the consequence management response to a significant cyber incident.

2. Consequence management in Nevada 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.

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.

III. NVOC Activation

A. The NVOC will activate based on:

1. The level of requested support from Cyber Security experts;

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

3. Upon the direction of the Governor.

B. Public Information

1. The OCDC Public Information Officer (PIO) will be the lead PIO for the overall response to the cyber event.

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

3. The DEM PIO will coordinate with the OCDC PIO and relevant PIOs on the release of information pertaining to the crisis management of the event.

IV. Organization

A. Due to the unique threat posed by a significant cyber incident, management of the event would require the establishment of a Unified Coordination Group (UCG) or a Policy Group (PG).

1. The UCG would 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).

2. The PG for the state would be members of the Nevada CSTF and the affected agency, jurisdiction, or sector.

3. The NVOC, in coordination with OCDC, will serve as the state's information sharing hub during the response to and recovery from a significant cyber incident.

4. Private Sector: CI/KR owner/operators are organized around multiple business model constructs based on their individual risk management criteria. 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 will vary based upon the mission area currently being addressed.

1. PSTF - OCDC General Responsibilities

A. Responsible for the State's cyber mitigation, preparedness, response, and recovery planning and response to cyber events.

B. Identify key individuals and organizations within Nevada that will act as liaisons to county, federal, and private sector partners.

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

D. Coordinate with other states and territories regarding significant cyber incident response and recovery operations.

E. Maintain situational awareness regarding current cyber threats and disseminate data to intergovernmental and interagency partners.

2. DEM Responsibilities

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 OCDC, coordinate with NVOC on any possible follow-on actions a cyber-adversary could take that could cause additional impacts to CI within Nevada.

C. Coordinate with federal partners (e.g. FEMA) regarding consequence management response to and recovery from a significant cyber incident.

3. Emergency Support Function Actions Responsivities

A. ESF-1 (Transportation) Maintain situational awareness on the cyber threat to transportation assets in Nevada. Ensure possible physical consequences resulting from cyber threats to critical transportation infrastructure are reported to the NVOC.

B. ESF-2 (Communications) Maintain situational awareness on the cyber threat to communications assets in Nevada. Ensure any possible identified physical effects resulting from cyber threats to critical communications infrastructure are reported to the NVOC.

C. ESF-3 (Public Works and Engineering) Maintain situational awareness on the cyber threat to water/ wastewater assets in Nevada. Ensure any possible identified physical effects resulting from cyber threats to water/wastewater networks are reported to the NVOC.

D. ESF-4 (Firefighting) Maintain situational awareness on the cyber threat to firefighting assets in Nevada. Ensure any possible identified physical effects resulting from cyber threats to critical firefighting infrastructure are reported to the NVOC.

E. ESF-6 (Mass Care) Maintain situational awareness on the cyber threat to mass care assets in Nevada. Ensure any possible identified physical effects resulting from cyber threats to critical mass care infrastructure are reported to the NVOC.

F. ESF-8 (Health and Medical Services) Maintain situational awareness on the cyber threat to health and medical assets in Nevada. Ensure any possible identified physical effects resulting from cyber threats to critical health and medical infrastructure are reported to the NVOC.

G. ESF-9 (Search and Rescue) Maintain situational awareness on the cyber threat to search and rescue assets in Nevada. Ensure any possible identified physical effects resulting from cyber threats to critical search and rescue infrastructure are reported to the NVOC.

H. ESF-10 (Environmental and Hazardous Materials Operations) Maintain situational awareness of the cyber threat to critical regulated facilities in Nevada. Report to the NVOC any identified physical effects resulting from the cyber threat to critical regulated facilities and associated infrastructure.

L. ESF-11 (Agriculture) Maintain situational awareness on the cyber threat to agribusiness and critical supply chains impacting Nevada. Maintain communications between supporting agencies, industry stakeholders, and federal partners including the national Food and Agriculture Sector leadership. Identify and coordinate resources as needed to support response efforts, mitigation, and recovery of impacted agribusiness, critical supply chains, systems, or economy.

I. ESF-12 (Energy) Maintain situational awareness on the cyber threat to energy infrastructure in Nevada. Ensure any possible identified physical effects resulting from cyber threats to critical energy infrastructure are reported to the NVOC and Energy Sector. Coordinate with Energy Sector to determine response and recovery needs.

J. ESF-13 (Public Safety - Law Enforcement) Maintain situational awareness on the cyber threat to law enforcement infrastructure in Nevada. Ensure any possible identified physical effects resulting from cyber threats to critical law enforcement infrastructure are reported to the NVOC. Coordinate law enforcement requests with local officials to include safeguarding of affected critical facilities.

K. ESF-14 (Cross Sector Business and Infrastructure) Maintain situational awareness on the cyber threat to critical infrastructure in Nevada. Ensure any possible identified physical effects resulting from cyber threats to critical infrastructure are reported to the NVOC and appropriate sector. Coordinate with private sector and DHS CISA - Cyber to determine response and recovery needs.

L. ESF-15 (Public Information and Warning) Maintain situational awareness of the cyber threat to any facilities in Nevada. Coordinate messaging with OCDC for a unified message in support of the sector, jurisdiction, or agency that is impacted.

M. ESF-16 (National Guard) Maintain situational awareness of the cyber threat to any facilities in Nevada. Coordinate available resources to support the sector, jurisdiction, or agency that is impacted. Coordinate DOD information through appropriate channels and the NVOC.

N. ESF-17 (Cybersecurity)