PROPOSED REGULATION OF THE

NEVADA OFFICE OF CYBER DEFENSE COORDINATION OF THE DEPARTMENT OF PUBLIC SAFETY

LCB FILE NO. R088-19I

The following document is the initial draft regulation proposed

by the agency submitted on 10/15/2019

REQUIREMENTS FOR CYBERSECURITY INCIDENT RESPONSE PLANS

General Provisions

NAC XXX.010 Definitions (NRS XXX.XXX) As used in this chapter, unless the context otherwise requires, the words and terms defined in NAC XXX.020 to XXX.XXX, inclusive, have the meanings ascribed to them in those sections.

NAC XXX.000 "Cyber Incident Response Plan" defined. "Cyber Incident Response Plan" means a set of predetermined and documented procedures to plan to, identify, contain, eradicate, recover, and derive and document lessons learned to/from a cybersecurity-related incident.

NAC XXX.000 "Certify" defined. "Certify" means to attest authoritatively in a written statement.

NAC XXX.000 "Confidential Data" defined. "Confidential Data" means to attest authoritatively in a written statement.

NAC XXX.000 "Data Breach" defined. "Data Breach" means an incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

NAC XXX.000 "Detect" defined. "Detect" means to discover or identify the presence or existence of a cyber-threat.

NAC XXX.000 "Distributed Denial of Service" defined. "Distributed Denial of Service" means a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.

NAC XXX.000 "Incident" defined. "Incident" means an occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences. Extended Definition: An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

NAC XXX.000 "Incident Response" defined. "Incident Response" means the activities that address a crisis or urgent situation within the pertinent domain, to mitigate immediate and potential threats.

NAC XXX.000 "Information Technology" defined. "Information Technology" means any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

NAC XXX.000 "Political Subdivision" defined. "Political Subdivision" means a city or county of this state.

NAC XXX.000 "Protected Data" defined. "Protected Data" means information about individuals, businesses, or any other information that is protected by law or regulation

NAC XXX.000 "Ransomeware" defined. "Ransomware" means a type of malware that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.

NAC XXX.000 "Sensitive Data" defined. "Sensitive Data" means

NAC XXX.000 "Threat" defined. "Threat" means a circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

NAC XXX.110 Cybersecurity incident response plan creation and maintenance. (NRS XXX.XXX**)**

1. Each political subdivision shall develop and maintain a documented cybersecurity incident response plan.

2. Each political subdivision shall review its cybersecurity incident response plan at least once per year, and as soon as practicable after the review is completed but not later than December 31st of each year, file with the Nevada Department of Public Safety – Office of Cyber Defense Coordination.

    (a) Non-substantive administrative plan adjustments to not require resubmission, as long as the annual filing with OCDC has been satisfied.

NAC XXX.120 Cybersecurity incident response plan elements. (NRS XXX.XXX**)**

1. Cybersecurity incident response plans must include the following:
    (a) Activities that preemptively build, reinforce, and/or improve readiness capabilities to prevent, protect against, detect, respond to, and recover from an incident(s).
        1. Purpose and objectives statement, summarizing the scope of the incident response plan and associated policies and procedures.
        2. Organizational cybersecurity lexicon or definition list of common cybersecurity terms.
        3. Written metrics for measuring cybersecurity incident organizational impact and the response capability and effectiveness of the organization.
        4. Define management and leadership personnel who will support the incident handling process through decision-making.
        5. Internal and external contact information to support incident response requirements.

6. Written plan for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the information security team.
7. Written plan for all personnel who will be involved in the incident response process outlining their roles, responsibilities, job titles and contact information.
8. Information sharing procedures, both internal and external, to ensure appropriate communication, and minimizing of information disclosure to unauthorized parties.
9. In additional to information technology, security, and management, organizations should consider incorporating the following internal groups into the cybersecurity incident response plan, as applicable:
    i. Legal
    ii. Public Affairs
    iii. Human Resources
    iv. Physical Security / Facilities Management

(b) Procedures to contact law enforcement or a regulatory body in a manner consistent with the requirements of law.

(c) Any actions taken to mitigate and recover from cyber incidents should be documented. This may include but not limited to location of backups, locations of network diagrams, current basslines of systems/network, etc.

1. Documented methodology, procedures, and tools to detect, identify, classify, and communicate current or potential cyber threats to organizational information technology systems.
    (a) Policy that define phases of incident handling.
    (b) Written method of documenting the attack vector used in incident.
    (c) A written method of documenting the indicators of that triggered the incident.
    (d) Procedures for analyzing and documenting the scope and impact of an incident.
    (e) Procedures to prioritize and handle concurrent incidents in one or multiple physical locations.
    (f) Procedures of incident notification process outlining who will be contacted and at what thresholds.
2. Procedures to prevent the spreading of and damage to information technology systems from a threat.
    (a) Written organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the information that should be included in the incident notification.
    (b) Procedures for isolating systems and gathering and storing evidence.
3. Processes and procedures for eradicating the threat from a compromised information technology system.

4. Restoration priority and processes and procedures to bring information technology systems impacted by a cyber incident back into a production state, including verification of data and system integrity.
5. Procedures to document cybersecurity incident lessons learned; including, areas of incident response success and failures, and recommendations on how to prevent future incidents. Significant cybersecurity incident lessons learned must be shared with city manager or county council within 90 days of an incident. Lessons learned will be used to update policies, procedures, guidelines and incident response plans.

NAC XXX.130 Cybersecurity incident response plan approval. (NRS XXX.XXX**)**

1. Incident response plans must include a statement of management commitment to incident response.
2. A city manager or county manager, whichever is applicable, must certify cyber incident response plans.

NAC XXX.140 Reporting cyber incidents. (NRS XXX.XXX**)**

1. Political subdivisions must report, within two business days, the following types of known or suspected cybersecurity incidents to the Nevada Department of Public Safety – Office of Cyber Defense Coordination.
    (a) Data Breach
    (b) Denial of Service Attack
    (c) Ransomware
    (d) Any other cybersecurity-related incident that disrupts the delivery of essential services for more than two business days, or directly affects life or property.