REVISED PROPOSED REGULATION OF THE

NEVADA OFFICE OF CYBER DEFENSE COORDINATION

OF THE DEPARTMENT OF PUBLIC SAFETY

LCB File No. R088-19

February 5, 2020

EXPLANATION – Matter in ***italics*** is new; matter in brackets [~~omitted material~~] is material to be omitted.

AUTHORITY: §§1-23, NRS 480.935 and 480.950.

A REGULATION relating to cybersecurity; providing certain requirements for cybersecurity incident response plans; requiring a political subdivision to document or report certain information relating to a cybersecurity incident; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law authorizes the Nevada Office of Cyber Defense Coordination of the Department of Public Safety to adopt regulations regarding the security of information systems. (NRS 480.950) Existing law requires each city and county of this State to adopt a cybersecurity incident response plan. Existing law requires the Office to prescribe the contents of such a plan by regulation. (NRS 480.935) **Section 17** of this regulation outlines the required contents of a cybersecurity incident response plan. **Section 18** of this regulation authorizes a political subdivision to incorporate certain internal groups into the cybersecurity incident response plan. **Section 19** of this regulation provides that a cybersecurity incident response plan becomes effective when certified by a city manager or county manager, as applicable. **Section 20** of this regulation requires a political subdivision to document actions taken to mitigate or recover from an incident. **Section 21** of this regulation requires a political subdivision to report significant information learned from an incident to a city or county manager, as applicable, within 90 days after an incident. **Section 22** of this regulation requires a political subdivision to report to the Office certain types of cybersecurity incidents within 1 business day after a known or suspected incident and include certain information in such report. **Section 23** of this regulation provides that a purely administrative or non-substantive change to a cybersecurity incident response plan is not considered a revision for the purposes of the filing requirement of NRS 480.935.

Section 1. Chapter 480 of NAC is hereby amended by adding thereto the provisions set forth as sections 2 to 23, inclusive, of this regulation.

Sec. 2. ***As used in this chapter, unless the context otherwise requires, the words and terms defined in sections 3 to 16, inclusive, of this regulation have the meanings ascribed to them in those sections.***

Sec. 3. ***"Certification" means to attest authoritatively in a written statement.***

Sec. 4. ***"Cybersecurity incident response plan" means a cybersecurity incident response plan that satisfies the requirements of section 17 of this regulation.***

Sec. 5. ***"Data breach" means an incident where protected or sensitive information is, without limitation, copied, transmitted, viewed, stolen or used by a person not authorized to do so.***

Sec. 6. ***"Detect" means to discover or identify the presence or existence of a cybersecurity threat.***

Sec. 7. ***"Distributed denial of service" means a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or the surrounding infrastructure of the target with a flood of Internet traffic.***

Sec. 8. ***"Incident" means an occurrence that:***

1. Actually or potentially results in adverse consequences to an information system or the information such a system processes, stores or transmits and may require an incident response to mitigate the actual or potential adverse consequences.

2. Is a violation or imminent threat of violation of a security policy or procedure or acceptable use policy of a political subdivision.

Sec. 9. ***"Incident response" means the activities that address an incident within the pertinent domain to mitigate immediate and potential adverse consequences or threats.***

Sec. 10. *"Information system" means any equipment or interconnected system or subsystem of equipment that processes, transmits, receives or interchanges data or information.*

Sec. 11. *"Office" means the Nevada Office of Cyber Defense Coordination of the Department of Public Safety.*

Sec. 12. *"Political subdivision" means a city or county of this State.*

Sec. 13. *"Protected information" means information about any person protected by law or regulation.*

Sec. 14. *"Ransomware" means a type of malware that attempts to deny or denies access to the data of a user of an information system until a ransom is paid.*

Sec. 15. *"Sensitive information" means any information the loss, misuse, modification or unauthorized access of which could adversely affect the public, the privacy of persons as provided by law or regulation or the interests of this State.*

Sec. 16. *"Threat" and "cybersecurity threat" mean a circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact the operations or assets, including, without limitation, information and information systems, of a political subdivision, person, other governmental entity or the public.*

Sec. 17. *A cybersecurity incident response plan must include:*

1. Measures that preemptively build, reinforce and improve the capability to prevent, protect against, detect, respond to and recover from an incident, including, without limitation:

(a) A statement of purpose and a statement of objectives that summarizes the scope of the cybersecurity incident response plan and associated policies and procedures;

(b) A list of common cybersecurity terms and associated definitions;

(c) Written metrics for measuring:

(1) The impacts of an incident on the political subdivision; and

(2) The capability and effectiveness of the political subdivision to engage in an incident response;

(d) A list of management and leadership personnel who will support an incident response;

(e) A list of internal and external contacts and associated contact information to support an incident response;

(f) A written plan for all personnel, including, without limitation, employees and contractors, regarding reporting computer anomalies and incidents to the proper personnel;

(g) A written plan for all personnel who will be involved in an incident response, including, without limitation, employees and contractors, that outlines the roles, responsibilities, job titles and contact information of such personnel;

(h) Procedures for sharing information, both internally and externally, to ensure appropriate communication and minimize information disclosure to unauthorized parties;

(i) Procedures to contact law enforcement or a regulatory body, as applicable, in a manner consistent with legal requirements; and

(j) Procedures to contact and inform any external entity that may be impacted by an incident due to a networked connection between the political subdivision and the entity affected by such an incident.

2. Documented methodology, procedures and tools to detect, identify, classify and communicate current or potential cybersecurity threats to information systems, including, without limitation:

(a) Defined phases of handling an incident;

(b) A written method of documenting the attack vector used in an incident;

(c) A written method of documenting the indicators that triggered an incident or incident report;

(d) Procedures for analyzing and documenting the scope and impact of an incident;

(e) Procedures to prioritize and handle concurrent incidents in one or more physical locations; and

(f) Procedures outlining which persons will be notified of an incident and the phase during the handling of an incident that such persons will be notified.

3. Procedures to prevent the damage to and spread of damage to information systems from a threat, including, without limitation:

(a) Recurring cybersecurity training programs for all personnel, including, without limitation, employees and contractors, who use the information systems of a political subdivision;

(b) Written standards for the time required for administrators of information systems and other personnel to report anomalous events to the proper personnel, the mechanisms for such reporting and the information that should be included in such a report; and

(c) Procedures for isolating information systems and gathering and storing evidence.

4. Processes and procedures to eradicate the threat from a compromised information system.

5. Processes and procedures to restore information systems impacted by an incident back to a state of production, including, without limitation, verification of data and the integrity of information systems.

6. Procedures to document information learned from an incident, including, without limitation, procedures to document:

(a) Areas of incident response successes and failures; and

(b) Recommendations on the prevention of future incidents.

7. A statement of commitment by management to an incident response.

Sec. 18. *In addition to information technology, cybersecurity and management groups, a political subdivision may consider incorporating legal, public affairs, human resources, physical security and facilities management groups of the political subdivision into the cybersecurity incident response plan.*

Sec. 19. *A cybersecurity incident response plan becomes effective upon certification by a city manager or county manager, as applicable.*

Sec. 20. *A political subdivision shall document any actions taken to mitigate or recover from an incident, including, without limitation, documenting current baselines of information systems and the location of backups and network diagrams.*

Sec. 21. *A political subdivision shall report any significant information learned from an incident to a city manager or county manager, as applicable, within 90 days after an incident. Such information may be used to update policies, procedures, guidelines and cybersecurity incident response plans.*

Sec. 22. *1. A political subdivision shall report to the Office within 1 business day after a known or suspected incident that is:*

(a) A data breach;

(b) A distributed denial of service incident;

(c) A ransomware incident; or

(d) Any other incident that disrupts the delivery of essential services for more than 1 business day or directly affects life or property.

2. The report submitted pursuant to subsection 1 must contain information on:

(a) The date and time of the incident;

(b) The type of incident;

(c) The type of information system or data affected by the incident;

(d) The known and projected impact of the incident to the political subdivision;

(e) Whether law enforcement, a regulatory body or external entity that could be affected by an incident have been notified of the incident, if applicable; and

(f) Any additional resources that are needed by the political subdivision to respond to the incident, if applicable.

Sec. 23. ***A purely administrative or non-substantive change to a cybersecurity incident response plan shall not be deemed a revision for the purpose of any requirement to file a revised plan pursuant to NRS 480.935.***