

Steve Sisolak
Governor



Nevada Department of
Public Safety
DEDICATION PRIDE SERVICE

George Togliatti
Director

Sheri Brueggemann
Deputy Director

Office of Cyber Defense Coordination

Shaun Rahmeyer
Administrator

555 Wright Way

Carson City, Nevada 89711

Telephone (775)684-4616 / Fax (775) 684-4809

NOTICE OF INTENT TO ACT UPON A REGULATION

Notice of Hearing for the adoption of Regulations of the
Nevada Department of Public Safety, Office of Cyber Defense Coordination
as proposed in LCB File No. R088-19

The purpose of this hearing is to receive comments from all interested parties regarding the adoption of Regulations pertaining to Chapter 480 of the Nevada Administrative Code, pursuant to Nevada Revised Statute NRS 480.935 requiring each city and county of this State to adopt a Cybersecurity Incident Response Plan.

Name of Organization: Nevada Department of Public Safety
Office of Cyber Defense Coordination

Date & Time of Hearing: Tuesday, October 27, 2020 @ 8:00 a.m.

Pursuant to Governor's Emergency Directive 006, there will be no physical location for this meeting. The meeting may be viewed live over Zoom.

Via Videoconference at Zoom: <https://zoom.us/meeting/99330947272>

Meeting ID: 993 3094 7272

AGENDA

Note: Witnesses wishing to have their complete testimony/handouts included in the permanent record of this meeting should provide a written or electronic copy to the Committee administrative support staff. Minutes of the meeting are produced in a summary format and are not verbatim.

Items may be taken out of the order presented on the agenda at the discretion of the agency. Items may be combined for consideration at the discretion of the agency. Items may be pulled or removed from the agenda at any time.

1. Call to order and welcome
2. Public Comment – *Administrator may limit public comments to 2 minutes per speaker, but may not restrict comments based upon viewpoint. No action may be taken upon a matter raised under the public comment period, unless the matter itself has been specifically included on this Agenda as an action item.*
3. Presentation and Discussion of Proposed Regulation **relating to cybersecurity; outlining 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.**
4. Review of written comments.
5. Closing Public Comment - *Administrator may limit public comments to 2 minutes per speaker, but may not restrict comments based upon viewpoint. No action may be taken upon a matter raised under the public comment period, unless the matter itself has been specifically included on this Agenda as an action item.*
6. Adjournment

NOTICE & EXPLANATION

The purpose of this hearing is to receive comments from all interested persons regarding the adoption of a Regulation that pertains to Chapter 480 of the Nevada Administrative Code.

The following information is provided pursuant to the requirements of NRS 233B.0603:

1. **Statement of the need for and purpose of the proposed regulation:** In accordance with recently established provisions outlined in Senate Bill 69, the Department of Public Safety Office of Cyber Defense Coordination “*shall, by regulation, prescribe the contents of a cybersecurity incident response plan, without limitation, a plan:*”
 - *To prepare for a cybersecurity threat*
 - *To detect and analyze a cybersecurity threat*
 - *To contain, eradicate and recover from a cybersecurity threat*
 - *For post-incident activity that includes a discussion regarding lessons learned and any analytics associated with the cybersecurity incident.”*
2. **Description of the proposed regulation:** Proposed regulation *relating to cybersecurity; outlining 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.*

- 3. *Estimated Economic Impact:*** Throughout the legislative process of the 80th Nevada Legislative Session, in which Senate Bill 69 was enacted, no persons or organizations identified or relayed any comments or information indicating any economic impact related to the establishment of incident response plans.

Adverse Impacts: None.

Beneficial Impacts: A robust and mature cybersecurity incident response plan has a direct, measurable, and positive impact to any organization – with subsequent impact to an organization’s effect to the community and economy. A strong cybersecurity incident response plan can be the immediate difference between an organization’s – whether government or private sector – ability to effectively respond to a cyberattack and return to normal business operations, or not. In Nevada, political subdivisions play a significant role in the local and statewide economy. Their ability to conduct business affects critical aspects of the economy, including but not limited to, delivery of essential services (police, fire, and ambulance), social services, regulation, tax collection, permitting, and many other components of day-to-day commerce.

Immediate Impacts: Political subdivisions will increase their ability to proactively plan, prevent, and respond to cybersecurity threats.

Long-Term Impacts: Safer and more resilient communities.

- 4. *Estimated Cost of Enforcement:*** None.
- 5. *Overlap or duplication of regulations:*** None.
- 6. *Requirement pursuant to Federal Law:*** None.
- 7. *New fee or increases an existing fee:*** None.

Persons wishing to comment upon the proposed action of the Nevada Department of Public Safety, Office of Cyber Defense Coordination may appear at the scheduled public hearing or may address their comments, data, views, or arguments, in written form, to the Nevada Department of Public Safety, Office of Cyber Defense Coordination, 727 Fairview Drive, Suite F, Carson City, Nevada 89701. If no person who are directly affected by the proposed action appears to request time to make an oral presentation, the Nevada Department of Public Safety, Office of Cyber Defense Coordination may proceed immediately to act upon any written submissions.

A copy of this notice and the regulation to be adopted will be on file at the State Library, 100 Stewart Street, Carson City, Nevada, for inspection by members of the public during business hours. Additional copies of the notice and the regulation to be adopted will be available at Nevada Department of Public Safety, Office of Cyber Defense Coordination and in all counties in which an office of the agency is not maintained, at the main public library, for inspection and copying by members of the public during business hours. This notice and the text of the proposed regulation are also available in the State of Nevada Register of Administrative Regulations, which is prepared and published monthly by the Legislative Counsel Bureau pursuant to NRS 233B.0653, and on the Internet at <http://www.leg.state.nv.us>.

Copies of this notice and the proposed regulation will also be mailed to members of the public upon request. A reasonable fee may be charged for copies if it is deemed necessary. Upon adoption of any regulation, the agency, if requested to do so by an interested person, either before adoption or within 30 days thereafter, will issue a concise statement of the principal reasons for and against its adoption and incorporate therein its reason for overruling the consideration urged against its adoption.

This Notice of Intent to Act Upon a Regulation, together with the Agenda have been posted at the following locations:

Legislative Counsel Bureau, 555 E. Washington Avenue, Las Vegas, NV
Legislative Counsel Bureau, 401 S. Carson Street, Carson Street, Carson City, NV
NV Dept of Public Safety, 555 Wright Way, Carson City, NV
NV Dept of Business & Industry, 1830 College Parkway, Suite 100, Carson City, NV
NV Dept of Business & Industry, 3300 W Sahara Ave, Suite 425, Las Vegas, NV
Nevada County Public Libraries

Posted to the following websites:

Nevada Public Notice Website: www.notice.nv.gov

Nevada Legislative Counsel Bureau Website: www.leg.state.nv.us/App/Notice/A/

**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.*