Senate Bill No. 69–Committee on Government Affairs

CHAPTER.....

AN ACT relating to public safety; designating the month of October of each year as "Cybersecurity Awareness Month"; revising requirements relating to emergency response plans for schools, cities, counties and resort hotels; clarifying the authority of the Governor to call members of the Nevada National Guard into state active duty upon a request for assistance from certain governmental entities that have experienced a significant cybersecurity incident; requiring each city or county to adopt and maintain a cybersecurity incident response plan; revising the duties of the Nevada Office of Cyber Defense Coordination of the Department of Public Safety; requiring the Office to submit a quarterly report to the Governor regarding cybersecurity; revising provisions relating to the disclosure of records by the Office; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Under existing law, various days, weeks and months of observance are recognized in this State. (NRS 236.018-236.073) **Section 1** of this bill designates the month of October of each year as "Cybersecurity Awareness Month" in this State and requires the Governor to issue annually a proclamation encouraging the observance of Cybersecurity Awareness Month.

Existing law requires certain persons or entities to develop an emergency response plan for a school, a city or county, a resort hotel and a utility. (NRS 239C.250, 239C.270, 388.243, 394.1685, 463.790) **Sections 3 and 8** of this bill standardize the requirements for emergency response plans for a city or county or resort hotel so that each such entity: (1) is required to annually review the plan and provide a copy of each updated plan to the Division of Emergency Management of the Department of Public Safety by a certain date; or (2) is authorized to submit a written certification in lieu of a revised plan if the plan has not changed. **Sections 4 and 5** of this bill similarly require the board of trustees of a school district, the governing body of a charter school or the development committee of a private school to annually review and update an emergency response plan for the applicable school or schools and submit the plan to the Division by a certain date.

Section 8 additionally requires an emergency response plan developed by a resort hotel to include the name and telephone number of the person responsible for ensuring that the resort hotel is in compliance with the requirements in existing law relating to emergency response plans. In addition, **section 8** requires the Nevada Gaming Control Board to provide a list of resort hotels to the Division upon request if the Board maintains such a list. **Section 7** of this bill requires the Chief of the Division to provide notice to certain public officers or bodies regarding whether a person or entity the officer or body oversees has complied with the requirement that the person or entity annually submit a revised plan or, if applicable, a written certification. **Section 7** also requires the Division to: (1) develop a written guide to assist a person or governmental entity that is required to file an emergency response

plan; and (2) provide the guide to certain persons or governmental entities that are required to file an emergency response plan.

Under existing law, the Governor is authorized to order the Nevada National Guard into active service of the State for invasions, disasters, riots and other substantial threats to life or property. (NRS 412.122) **Section 6** of this bill provides specific authority to the Governor to call members of the Nevada National Guard into such active service upon a request for assistance from a political subdivision or governmental utility that has experienced a significant cybersecurity incident.

The Nevada Office of Cyber Defense Coordination is created under existing law in the Department of Public Safety. (NRS 480.920) The Office is required to perform a variety of duties relating to the security of information systems of agencies of the Executive Branch of State Government and to prepare and maintain a statewide strategic plan regarding the security of information systems in Nevada. (NRS 480.924-480.930)

Section 9 of this bill requires each city or county to adopt and maintain a cybersecurity incident response plan and file the plan with the Office. **Section 9** requires each city or county to review this plan at least once each year and, on or before December 31 of each year, file with the Office: (1) any revised plan resulting from the review; or (2) a written certification that the most recent plan filed is the current plan for the city or county. **Section 9** also makes such plans confidential. **Section 2** of this bill makes a conforming change.

Section 11 of this bill requires the Office to: (1) develop procedures for risk-based assessments that identify vulnerabilities in the information systems that are operated or maintained by state agencies and any potential threats that may exploit such vulnerabilities; (2) based on the results of risk-based assessments, identify risks to the security of information systems that are operated or maintained by state agencies; and (3) develop best practices for preparing for and mitigating such risks.

Existing law requires the Office to establish partnerships with local governments, the Nevada System of Higher Education and private entities that have expertise in cyber security or information systems to encourage the development of strategies to protect the security of information systems. (NRS 480.926) **Section 11.5** of this bill expands this requirement to include all private entities, to the extent practicable.

Existing law requires the Administrator of the Office to appoint a cybersecurity incident response team or teams to assist in responding to a threat to the security of an information system. (NRS 480.928) **Section 11.7** of this bill provides that such a team may include an investigator employed by the Investigation Division of the Department of Public Safety.

Existing law requires the Office to prepare and make publicly available a statewide strategic plan that outlines policies, procedures, best practices and recommendations for preparing for and mitigating risks to, and otherwise protecting, the security of information systems in this State and for recovering from and responding to such threats. (NRS 480.930) **Section 12** of this bill provides that the statewide strategic plan must not identify or include information which allows for the identification of specific vulnerabilities in the information systems in this State. **Section 12** requires each agency of the State Government that has adopted a cybersecurity policy to: (1) test periodically the adherence of its employees to that policy; and (2) submit the results of the testing to the Office for consideration in the update of the statewide strategic plan. Finally, in addition to the annual report that the Office is required to submit in existing law regarding its activities, **section 13** of this bill requires the Office to submit a quarterly report to the Governor assessing the preparedness of Nevada to counteract, prevent and respond to potential cybersecurity threats. (NRS 480.932)

Existing law provides that any record of a state agency, including the Office, or a local government which identifies the detection of, the investigation of or a response to a suspected or confirmed threat to or attack on the security of an information system is not a public record and may be disclosed by the Administrator only to certain entities and only to protect the security of information systems or as a part of a criminal investigation. (NRS 480.940) **Section 13.5** of this bill clarifies that a record obtained from a private entity may only be disclosed in these circumstances.

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

THE PEOPLE OF THE STATE OF NEVADA, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. Chapter 236 of NRS is hereby amended by adding thereto a new section to read as follows:

1. The month of October of each year is designated as "Cybersecurity Awareness Month" in this State.

2. The Governor shall issue annually a proclamation encouraging the observance of Cybersecurity Awareness Month. The proclamation may, without limitation:

(a) Call upon state and local governmental agencies, private nonprofit groups and foundations, schools, businesses and other public and private entities to work toward the goal of helping all Americans stay safer and more secure online;

(b) Recognize the danger that cybersecurity threats pose to the economy and public infrastructure of this State; and

(c) Recognize the importance of collaboration among the departments and agencies in this State, the federal government and the private sector to keep this State safe from cybersecurity threats and to protect the residents of this State in the digital domain.

Sec. 2. NRS 239.010 is hereby amended to read as follows:

239.010 1. Except as otherwise provided in this section and NRS 1.4683, 1.4687, 1A.110, 3.2203, 41.071, 49.095, 49.293, 62D.420, 62D.440, 62E.516, 62E.620, 62H.025, 62H.030, 62H.170, 62H.220, 62H.320, 75A.100, 75A.150, 76.160, 78.152, 80.113, 81.850, 82.183, 86.246, 86.54615, 87.515, 87.5413, 87A.200, 87A.580, 87A.640, 88.3355, 88.5927, 88.6067, 88A.345, 88A.7345, 89.045, 89.251, 90.730, 91.160, 116.757, 116A.270, 116B.880, 118B.026, 119.260, 119.265, 119.267, 119.280, 119A.280, 119A.653, 119B.370, 119B.382, 120A.690, 125.130, 125B.140, 126.141, 126.161, 126.163, 126.730, 127.007, 127.057, 127.130, 127.140, 127.2817, 128.090, 130.312, 130.712, 136.050, 159.044, 159A.044, 172.075, 172.245, 176.01249, 176.015, 176.0625,

176.09129, 176.156, 176A.630, 178.39801, 178.4715, 178.5691, 179.495, 179A.070, 179A.165, 179D.160, 200.3771, 200.3772, 200.5095, 200.604, 202.3662, 205.4651, 209.392, 209.3925, 209.419, 209.521, 211A.140, 213.010, 213.040, 213.095, 213.131, 217.105, 217.110, 217.464, 217.475, 218A.350, 218E.625, 218F.150, 218G.130, 218G.240, 218G.350, 228.270, 228.450, 228.495, 228.570, 231.069, 231.1473, 233.190, 237.300, 239.0105, 239.0113, 239B.030, 239B.040, 239B.050, 239C.140, 239C.210, 239C.230, 239C.250, 239C.270, 240.007, 241.020, 241.030, 241.039, 242.105, 244.264, 244.335, 247.540, 247.550, 247.560, 250.087, 250.130, 250.140, 250.150, 268.095, 268.490, 268.910, 271A.105, 281.195, 281.805, 281A.350, 281A.680, 281A.685, 281A.750, 281A.755, 281A.780, 284.4068, 286.110, 287.0438, 289.025, 289.080, 289.387, 289.830, 293.4855, 293.5002, 293.503, 293.504, 293.558, 293.906, 293.908, 293.910, 293B.135, 293D.510, 331.110, 332.061, 332.351, 333.333, 333.335, 338.070, 338.1379, 338.1593, 338.1725, 338.1727, 348.420, 349.597, 349.775, 353.205, 353A.049, 353A.085, 353A.100, 353C.240, 360.240, 360.247, 360.255, 360.755, 361.044, 361.610, 365.138, 366.160, 368A.180, 370.257, 370.327, 372A.080, 378.290, 378.300, 379.008, 379.1495, 385A.830, 385B.100, 387.626, 387.631, 388.1455, 388.259, 388.501, 388.503, 388.513, 388.750, 388A.247, 388A.249, 391.035, 391.120, 391.925, 392.029, 392.147, 392.264, 392.271, 392.315, 392.317, 392.325, 392.327, 392.335, 392.850, 394.167, 394.1698, 394.447, 394.460, 394.465, 396.3295, 396.405, 396.525, 396.535, 396.9685, 398A.115, 408.3885, 408.3886, 408.3888, 408.5484, 412.153, 416.070, 422.2749, 422.305, 422A.342, 422A.350, 425.400, 427A.1236, 427A.872, 432.028, 432.205, 432B.175, 432B.280, 432B.290, 432B.407, 432B.430, 432B.560, 432B.5902, 433.534, 433A.360, 437.145, 439.840, 439B.420, 440.170, 441A.195, 441A.220, 441A.230, 442.330, 442.395, 442.735, 445A.665, 445B.570, 449.209, 449.245, 449A.112, 450.140, 453.164, 453.720, 453A.610, 453A.700, 458.055, 458.280, 459.050, 459.3866, 459.555, 459.7056, 459.846, 463.120, 463.15993, 463.240, 463.3403, 463.3407, 463.790, 467.1005, 480.365, 480.940, 481.063, 481.091, 481.093, 482.170, 482.5536, 483.340, 483.363, 483.575, 483.659, 483.800, 484E.070, 485.316, 501.344, 503.452, 522.040, 534A.031, 561.285, 571.160, 584.655, 587.877, 598.0964, 598.098, 598A.110, 599B.090, 603.070, 603A.210, 604A.710, 612.265, 616B.012, 616B.015, 616B.315, 616B.350, 618.341, 618.425, 622.310, 623.131, 623A.137, 624.110, 624.265, 624.327, 625.425, 625A.185, 628.418, 628B.230, 628B.760, 629.047, 629.069, 630.133, 630.30665, 630.336, 630A.555, 631.368,

632.121, 632.125, 632.405, 633.283, 633.301, 633.524, 634.055, 634.214, 634A.185, 635.158, 636.107, 637.085, 637B.288, 638.087, 638.089, 639.2485, 639.570, 640.075, 640A.220, 640B.730, 640C.400, 640C.600, 640C.620, 640C.745, 640C.760, 640D.190, 640E.340, 641.090, 641.325, 641A.191, 641A.289, 641B.170, 641B.460, 641C.760, 641C.800, 642.524, 643.189, 644A.870, 645.180, 645.625, 645A.050, 645A.082, 645B.060, 645B.092, 645C.220, 645C.225, 645D.130, 645D.135, 645E.300, 645E.375, 645G.510, 645H.320, 645H.330, 647.0945, 647.0947, 648.033, 648.197, 649.065, 649.067, 652.228, 654.110, 656.105, 661.115, 665.130, 665.133, 669.275, 669.285, 669A.310, 671.170, 673.450, 673.480, 675.380, 676A.340, 676A.370, 677.243, 679B.122, 679B.152, 679B.159, 679B.190, 679B.285, 679B.690, 680A.270, 681A.440, 681B.260, 681B.410, 681B.540, 683A.0873, 685A.077, 686A.289, 686B.170, 686C.306, 687A.110, 687A.115, 687C.010, 688C.230, 688C.480, 688C.490, 689A.696, 692A.117, 692C.190, 692C.3507, 692C.3536, 692C.3538, 692C.354, 692C.420, 693A.480, 693A.615, 696B.550, 696C.120, 703.196, 704B.320, 704B.325, 706.1725, 706A.230, 710.159, 711.600, ***and section 9 of this act,*** sections 35, 38 and 41 of chapter 478, Statutes of Nevada 2011 and section 2 of chapter 391, Statutes of Nevada 2013 and unless otherwise declared by law to be confidential, all public books and public records of a governmental entity must be open at all times during office hours to inspection by any person, and may be fully copied or an abstract or memorandum may be prepared from those public books and public records. Any such copies, abstracts or memoranda may be used to supply the general public with copies, abstracts or memoranda of the records or may be used in any other way to the advantage of the governmental entity or of the general public. This section does not supersede or in any manner affect the federal laws governing copyrights or enlarge, diminish or affect in any other manner the rights of a person in any written book or record which is copyrighted pursuant to federal law.

2. A governmental entity may not reject a book or record which is copyrighted solely because it is copyrighted.

3. A governmental entity that has legal custody or control of a public book or record shall not deny a request made pursuant to subsection 1 to inspect or copy or receive a copy of a public book or record on the basis that the requested public book or record contains information that is confidential if the governmental entity can redact, delete, conceal or separate the confidential information from the information included in the public book or record that is not otherwise confidential.

4. A person may request a copy of a public record in any medium in which the public record is readily available. An officer, employee or agent of a governmental entity who has legal custody or control of a public record:

(a) Shall not refuse to provide a copy of that public record in a readily available medium because the officer, employee or agent has already prepared or would prefer to provide the copy in a different medium.

(b) Except as otherwise provided in NRS 239.030, shall, upon request, prepare the copy of the public record and shall not require the person who has requested the copy to prepare the copy himself or herself.

Sec. 3. NRS 239C.250 is hereby amended to read as follows:

239C.250 1. Each political subdivision shall adopt and maintain a response plan. Each new or revised plan must be filed within 10 days after adoption or revision with:

(a) The Division; and

(b) Each response agency that provides services to the political subdivision.

2. The response plan required by subsection 1 ***and any revised response plan pursuant to subsection 3*** must include:

(a) A drawing or map of the layout and boundaries of the political subdivision;

(b) A drawing or description of the streets and highways within, and leading into and out of, the political subdivision, including any approved routes for evacuation;

(c) The location and inventory of emergency response equipment and resources within the political subdivision;

(d) The location of any unusually hazardous substances within the political subdivision;

(e) A telephone number that may be used by residents of the political subdivision to receive information and to make reports with respect to an act of terrorism or related emergency;

(f) The location of one or more emergency response command posts that are located within the political subdivision;

(g) A depiction of the location of each police station, sheriff's office and fire station that is located within the political subdivision;

(h) Plans for the continuity of the operations and services of the political subdivision, which plans must be consistent with the provisions of NRS 239C.260; and

(i) Any other information that the Commission may determine to be relevant.

3. ***Each political subdivision shall review its response plan at least once each year and, as soon as practicable after the review is completed but not later than December 31 of each year, file with the Division and each response agency that provides services to the political subdivision:***

(a) Any revised response plan resulting from the review; or

(b) A written certification that the most recent response plan filed pursuant to subsection 1 is the current response plan for the political subdivision.

4. Except as otherwise provided in NRS 239.0115, a plan filed pursuant to the requirements of this section, including any revisions adopted thereto, is confidential and must be securely maintained by the entities with whom it is filed pursuant to subsection 1 ~~[.]~~ ***or 3.*** An officer, employee or other person to whom the plan is entrusted by the entity with whom it is filed shall not disclose the contents of such a plan except:

(a) Upon the lawful order of a court of competent jurisdiction;

(b) As is reasonably necessary in the case of an act of terrorism or related emergency; or

(c) Pursuant to the provisions of NRS 239.0115.

Sec. 4. NRS 388.245 is hereby amended to read as follows:

388.245 1. Each development committee shall, at least once each year, review and update as appropriate the plan that it developed pursuant to NRS 388.243. In reviewing and updating the plan, the development committee shall consult with the director of the local organization for emergency management or, if there is no local organization for emergency management, with the Chief of the Division of Emergency Management of the Department of Public Safety or his or her designee.

2. Each development committee shall provide an updated copy of the plan to the board of trustees of the school district that established the committee or the governing body of the charter school that established the committee.

3. ***On or before July 1 of each year, the board of trustees of the school district that established the committee or the governing body of the charter school that established the committee shall submit for approval to the Division of Emergency Management of the Department of Public Safety the plan updated pursuant to subsection 1.***

4. The board of trustees of each school district and the governing body of each charter school shall:

(a) Post a notice of the completion of each review and update that its development committee performs pursuant to subsection 1 at each school in its school district or at its charter school;

(b) File with the Department a copy of the notice provided pursuant to paragraph (a);

(c) Post a copy of NRS 388.229 to 388.266, inclusive, at each school in its school district or at its charter school;

(d) Retain a copy of each plan developed pursuant to NRS 388.243, each plan updated pursuant to subsection 1 and each deviation approved pursuant to NRS 388.251;

(e) Provide a copy of each plan developed pursuant to NRS 388.243 and each plan updated pursuant to subsection 1 to:

(1) Each local public safety agency in the county in which the school district or charter school is located; ***and***

(2) ~~[The Division of Emergency Management of the Department of Public Safety; and~~

~~(3)]~~ The local organization for emergency management, if any;

(f) Upon request, provide a copy of each plan developed pursuant to NRS 388.243 and each plan updated pursuant to subsection 1 to a local agency that is included in the plan and to an employee of a school who is included in the plan;

(g) Provide a copy of each deviation approved pursuant to NRS 388.251 as soon as practicable to:

(1) The Department;

(2) A local public safety agency in the county in which the school district or charter school is located;

(3) The Division of Emergency Management of the Department of Public Safety;

(4) The local organization for emergency management, if any;

(5) A local agency that is included in the plan; and

(6) An employee of a school who is included in the plan; and

(h) At least once each year, provide training in responding to a crisis and training in responding to an emergency to each employee of the school district or of the charter school, including, without limitation, training concerning drills for evacuating and securing schools.

~~[4.]~~ ***5.*** The board of trustees of each school district and the governing body of each charter school may apply for and accept gifts, grants and contributions from any public or private source to carry out the provisions of NRS 388.229 to 388.266, inclusive.

Sec. 5. NRS 394.1688 is hereby amended to read as follows:

394.1688 1. Each development committee shall, at least once each year, review and update as appropriate the plan that it developed pursuant to NRS 394.1687. In reviewing and updating the plan, the development committee shall consult with the director of the local organization for emergency management or, if there is no local organization for emergency management, with the Chief of the Division of Emergency Management of the Department of Public Safety or his or her designee.

2. ~~[Each]~~ ***On or before July 1 of each year, each*** development committee shall provide an updated copy of the plan to the governing body of the school.

3. The governing body of each private school shall:

(a) Post a notice of the completion of each review and update that its development committee performs pursuant to subsection 1 at the school;

(b) File with the Department a copy of the notice provided pursuant to paragraph (a);

(c) Post a copy of NRS 388.253 and 394.168 to 394.1699, inclusive, at the school;

(d) Retain a copy of each plan developed pursuant to NRS 394.1687, each plan updated pursuant to subsection 1 and each deviation approved pursuant to NRS 394.1692;

(e) ~~[Provide]~~ ***On or before July 1 of each year, provide*** a copy of each plan developed pursuant to NRS 394.1687 and each plan updated pursuant to subsection 1 to:

(1) Each local public safety agency in the county in which the school is located;

(2) The Division of Emergency Management of the Department of Public Safety; and

(3) The local organization for emergency management, if any;

(f) Upon request, provide a copy of each plan developed pursuant to NRS 394.1687 and each plan updated pursuant to subsection 1 to a local agency that is included in the plan and to an employee of the school who is included in the plan;

(g) Upon request, provide a copy of each deviation approved pursuant to NRS 394.1692 to:

(1) The Department;

(2) A local public safety agency in the county in which the school is located;

(3) The Division of Emergency Management of the Department of Public Safety;

(4) The local organization for emergency management, if any;

(5) A local agency that is included in the plan; and

(6) An employee of the school who is included in the plan; and

(h) At least once each year, provide training in responding to a crisis and training in responding to an emergency to each employee of the school, including, without limitation, training concerning drills for evacuating and securing the school.

4. As used in this section, "public safety agency" has the meaning ascribed to it in NRS 388.2345.

Sec. 6. NRS 412.122 is hereby amended to read as follows:

412.122 1. The Governor may in case of invasion, disaster, insurrection, riot, breach of the peace, or imminent danger thereof, or other substantial threat to life or property, ***or upon a request for assistance from a political subdivision or governmental utility, as defined in NRS 239C.050, that has experienced a significant cybersecurity incident,*** order into active service of the State for such a period, to such an extent and in such a manner as he or she deems necessary all or any part of the Nevada National Guard. The authority of the Governor includes the power to order the Nevada National Guard or any part thereof to function under the operational control of the United States Army, Navy or Air Force commander in charge of the defense of any area within the State which is invaded or attacked or is or may be threatened with invasion or attack.

2. In case of the absence of the Governor from the State, or if it is impossible to communicate immediately with the Governor, the civil officer making a requisition for troops may, if the civil officer deems the necessity imminent and not admitting of delay, serve a copy of the requisition, together with a statement of the Governor's absence or the impossibility of immediately communicating with the Governor, upon the following officers in this order:

(a) Lieutenant Governor;

(b) Adjutant General; and

(c) Other officers designated in a chain of command prescribed by Office regulations.

➥ If the call is afterward disapproved by the Governor, the troops called into service must be disbanded immediately.

3. The Governor may order into active service of the State for such a period, to such an extent and in such a manner as the Governor deems necessary units or individual members of the Nevada National Guard when in his or her judgment the services of the units or members are required for:

(a) The furtherance of the organization, maintenance, discipline or training of the Nevada National Guard;

(b) The welfare of the public; or

(c) Ceremonial functions of the State Government.

4. Whenever any portion of the Nevada National Guard is employed pursuant to subsection 1, the Governor, if in his or her judgment the maintenance of law and order will thereby be promoted, may by proclamation declare the county or city in which the troops are serving, or any specified portion thereof, to be under martial law.

Sec. 7. NRS 414.040 is hereby amended to read as follows:

414.040 1. A Division of Emergency Management is hereby created within the Department of Public Safety. The Chief of the Division is appointed by and holds office at the pleasure of the Director of the Department of Public Safety. The Division is the State Agency for Emergency Management and the State Agency for Civil Defense for the purposes of the Compact ratified by the Legislature pursuant to NRS 415.010. The Chief is the State's Director of Emergency Management and the State's Director of Civil Defense for the purposes of that Compact.

2. The Chief may employ technical, clerical, stenographic and other personnel as may be required, and may make such expenditures therefor and for other expenses of his or her office within the appropriation therefor, or from other money made available to him or her for purposes of emergency management, as may be necessary to carry out the purposes of this chapter.

3. The Chief, subject to the direction and control of the Director, shall carry out the program for emergency management in this state. The Chief shall coordinate the activities of all organizations for emergency management within the State, maintain liaison with and cooperate with agencies and organizations of other states and of the Federal Government for emergency management and carry out such additional duties as may be prescribed by the Director.

4. The Chief shall assist in the development of comprehensive, coordinated plans for emergency management by adopting an integrated process, using the partnership of governmental entities, business and industry, volunteer organizations and other interested persons, for the mitigation of, preparation for, response to and recovery from emergencies or disasters. In adopting this process, the Chief shall conduct activities designed to:

(a) Eliminate or reduce the probability that an emergency will occur or to reduce the effects of unavoidable disasters;

(b) Prepare state and local governmental agencies, private organizations and other persons to be capable of responding appropriately if an emergency or disaster occurs by fostering the adoption of plans for emergency operations, conducting exercises to test those plans, training necessary personnel and acquiring necessary resources;

(c) Test periodically plans for emergency operations to ensure that the activities of state and local governmental agencies, private organizations and other persons are coordinated;

(d) Provide assistance to victims, prevent further injury or damage to persons or property and increase the effectiveness of recovery operations; and

(e) Restore the operation of vital community life-support systems and return persons and property affected by an emergency or disaster to a condition that is comparable to or better than what existed before the emergency or disaster occurred.

5. In addition to any other requirement concerning the program of emergency management in this State, the Chief shall:

(a) Maintain an inventory of any state or local services, equipment, supplies, personnel and other resources related to participation in the Nevada Intrastate Mutual Aid System established pursuant to NRS 414A.100;

(b) Coordinate the provision of resources and equipment within this State in response to requests for mutual aid pursuant to NRS 414.075 or chapter 414A of NRS; ~~[and]~~

(c) Coordinate with state agencies, local governments, Indian tribes or nations and special districts to use the personnel and equipment of those state agencies, local governments, Indian tribes or nations and special districts as agents of the State during a response to a request for mutual aid pursuant to NRS 414.075 or 414A.130 ~~[.]~~ ***; and***

(d) Provide notice:

(1) On or before February 15 of each year to the governing body of each political subdivision of whether the political subdivision has complied with the requirements of NRS 239C.250;

(2) On or before February 15 of each year to the Chair of the Public Utilities Commission of Nevada of whether each utility that is not a governmental utility has complied with the requirements of NRS 239C.270;

(3) On or before February 15 of each year to the Governor of whether each governmental utility described in subsection 1 of NRS 239C.050 has complied with the requirements of NRS 239C.270;

(4) On or before February 15 of each year to the governing body of each governmental utility described in subsection 2 of NRS 239C.050 of whether each such governmental utility has complied with the requirements of NRS 239C.270;

(5) On or before August 15 of each year to the Superintendent of Public Instruction of whether each board of trustees of a school district, governing body of a charter school or governing body of a private school has complied with the requirements of NRS 388.243 or 394.1687, as applicable; and

(6) On or before November 15 of each year to the Chair of the Nevada Gaming Control Board of whether each resort hotel has complied with the requirements of NRS 463.790.

6. The Division shall perform the duties required pursuant to chapter 415A of NRS.

7. The Division shall perform the duties required pursuant to NRS 353.2753 at the request of a state agency or local government.

8. The Division shall develop a written guide for the preparation and maintenance of an emergency response plan to assist a person or governmental entity that is required to file a plan pursuant to NRS 239C.250, 239C.270, 388.243, 394.1687 or 463.790. The Division shall review the guide on an annual basis and revise the guide if necessary. On or before January 15 of each year, the Division shall provide the guide to:

(a) Each political subdivision required to adopt a response plan pursuant to NRS 239C.250;

(b) Each utility required to prepare and maintain an emergency response plan pursuant to NRS 239C.270;

(c) Each development committee required to develop a plan to be used in responding to a crisis, emergency or suicide by:

(1) A public school or charter school pursuant to NRS 388.243; or

(2) A private school pursuant to NRS 394.1687; and

(d) Each resort hotel required to adopt an emergency response plan pursuant to NRS 463.790.

Sec. 8. NRS 463.790 is hereby amended to read as follows:

463.790 1. Each resort hotel shall adopt and maintain an emergency response plan. Each new or revised plan must be filed within 3 days after adoption or revision with each local fire department and local law enforcement agency whose jurisdiction includes the area in which the resort hotel is located and with the Division of Emergency Management of the Department of Public Safety.

2. The emergency response plan required by subsection 1 must include:

(a) A drawing or map of the layout of all areas within the building or buildings and grounds that constitute a part of the resort hotel and its support systems and a brief description of the purpose or use for each area;

(b) A drawing or description of the internal and external access routes;

(c) The location and inventory of emergency response equipment and resources;

(d) The location of any unusually hazardous substances;

(e) The name and telephone number of ~~[the]~~ ***:***

(1) The emergency response coordinator for the resort hotel; ***and***

(2) The person responsible for ensuring that the resort hotel is in compliance with this section;

(f) The location of one or more site emergency response command posts;

(g) A description of any special equipment needed to respond to an emergency at the resort hotel;

(h) An evacuation plan;

(i) A description of any public health or safety hazards present on the site; and

(j) Any other information requested by a local fire department or local law enforcement agency whose jurisdiction includes the area in which the resort hotel is located or by the Division of Emergency Management.

3. ***Each resort hotel shall review its emergency response plan at least once each year and, as soon as practicable after the review is completed but not later than November 1 of each year, file with each local fire department and local law enforcement agency whose jurisdiction includes the area in which the resort hotel is located and with the Division of Emergency Management:***

(a) Any revised emergency response plan resulting from the review; or

(b) A written certification that the most recent emergency response plan filed pursuant to this subsection or subsection 1 is the current emergency response plan for the resort hotel.

4. A plan filed pursuant to the requirements of this section, including any revisions adopted thereto, is confidential and must be securely maintained by the department, agency and Division with whom it is filed. An officer, employee or other person to whom the

plan is entrusted by the department, agency or Division shall not disclose the contents of such a plan except:

(a) Upon the lawful order of a court of competent jurisdiction; or

(b) As is reasonably necessary in the case of an emergency involving public health or safety.

5. If the Board maintains a list of resort hotels, the Board shall provide a copy of the list to the Division of Emergency Management, upon request, for purposes of this section.

~~[4.]~~ ***6.*** As used in this section, the term "local law enforcement agency" means:

(a) The sheriff's office of a county;

(b) A metropolitan police department; or

(c) A police department of an incorporated city.

Sec. 9. Chapter 480 of NRS is hereby amended by adding thereto a new section to read as follows:

1. Each political subdivision shall adopt and maintain a cybersecurity incident response plan. Each new or revised plan must be filed within 10 days after adoption or revision with the Office.

2. The Office shall, by regulation, prescribe the contents of a cybersecurity incident response plan, which must include, without limitation, a plan:

(a) To prepare for a cybersecurity threat;

(b) To detect and analyze a cybersecurity threat;

(c) To contain, eradicate and recover from a cybersecurity incident; and

(d) For postincident activity that includes a discussion regarding lessons learned and any analytics associated with the cybersecurity incident.

3. Each political subdivision shall review its cybersecurity incident response plan at least once each year and, as soon as practicable after the review is completed but not later than December 31 of each year, file with the Office:

(a) Any revised cybersecurity incident response plan resulting from the review; or

(b) A written certification that the most recent cybersecurity incident response plan filed pursuant to this subsection or subsection 1 is the current cybersecurity incident response plan for the political subdivision.

4. Except as otherwise provided in NRS 239.0115, a cybersecurity incident response plan filed pursuant to the requirements of this section, including any revisions adopted

thereto, is confidential and must be securely maintained by the Office. An officer, employee or other person to whom the plan is entrusted by the Office shall not disclose the contents of such a plan except:

(a) Upon the lawful order of a court of competent jurisdiction;

(b) As is reasonably necessary in the case of an act of terrorism or related emergency; or

(c) Pursuant to the provisions of NRS 239.0115.

5. As used in this section, "political subdivision" means a city or county of this State.

Sec. 10. NRS 480.902 is hereby amended to read as follows:

480.902 As used in NRS 480.900 to 480.950, inclusive, ***and section 9 of this act,*** unless the context otherwise requires, the words and terms defined in NRS 480.904 to 480.912, inclusive, have the meanings ascribed to them in those sections.

Sec. 11. NRS 480.924 is hereby amended to read as follows:

480.924 ~~[1.]~~ The Office shall:

~~[(a) Periodically review the information systems that are operated or maintained by state agencies.~~

~~(b) Identify]~~

1. Develop procedures for risk-based assessments that identify vulnerabilities in the information systems that are operated or maintained by state agencies and any potential threats that may exploit such vulnerabilities.

2. Based on the results of risk-based assessments, identify risks to the security of information systems that are operated or maintained by state agencies.

~~[(c)]~~ ***3.*** Develop ~~[and update, as necessary, strategies, standards and guidelines]~~ ***best practices*** for preparing for and mitigating risks to, and otherwise protecting, the security of information systems that are operated or maintained by state agencies.

~~[(d) Coordinate performance audits and assessments of the information systems of state agencies to determine, without limitation, adherence to the regulations, standards, practices, policies and conventions of the Division of Enterprise Information Technology Services of the Department of Administration that are identified by the Division as security related.~~

~~(e) Coordinate statewide programs for awareness and training regarding risks to the security of information systems that are operated or maintained by state agencies.~~

~~2. Upon review of an information system that is operated or maintained by a state agency, the Office may make~~

~~recommendations to the state agency and the Division of Enterprise Information Technology Services regarding the security of the information system.]~~

Sec. 11.5. NRS 480.926 is hereby amended to read as follows:

480.926 The Office shall:

1. Establish partnerships with:

(a) Local governments;

(b) The Nevada System of Higher Education; and

(c) Private entities ~~[that have expertise in cyber security or information systems,]~~ ***, to the extent practicable,***

➥ to encourage the development of strategies to prepare for and mitigate risks to, and otherwise protect, the security of information systems that are operated or maintained by a public or private entity in this State.

2. Establish partnerships to assist and receive assistance from local governments and appropriate agencies of the Federal Government regarding the development of strategies to prepare for and mitigate risks to, and otherwise protect, the security of information systems.

3. Consult with the Division of Emergency Management of the Department and the Division of Enterprise Information Technology Services of the Department of Administration regarding the development of strategies to prepare for and mitigate risks to, and otherwise protect, the security of information systems.

4. Coordinate with the Investigation Division of the Department regarding gathering intelligence on and initiating investigations of cyber threats and incidents.

Sec. 11.7. NRS 480.928 is hereby amended to read as follows:

480.928 1. The Office shall establish policies and procedures for:

(a) A state agency to notify the Office of any specific threat to the security of an information system operated or maintained by the state agency;

(b) Any other public or private entity to voluntarily notify the Office of any specific threat to the security of an information system;

(c) The Office to notify state agencies, appropriate law enforcement and prosecuting authorities and any other appropriate public or private entity of any specific threat to the security of an information system of which the Office has been notified; and

(d) The Administrator to convene a cybersecurity incident response team appointed pursuant to subsection 2 upon notification

of the Office of a specific threat to the security of an information system.

2. In consultation with appropriate state agencies, local governments and agencies of the Federal Government, the Administrator shall appoint a cybersecurity incident response team or teams. ***Such a team may include, without limitation, an investigator employed by the Investigation Division of the Department.***

3. A cybersecurity incident response team appointed pursuant to subsection 2 shall convene at the call of the Administrator and, subject to the direction of the Administrator, shall assist the Office and any appropriate state agencies, local governments or agencies of the Federal Government in responding to the threat to the security of an information system.

4. A private entity may, in its discretion, use the services of a cybersecurity incident response team appointed pursuant to subsection 2.

Sec. 12. NRS 480.930 is hereby amended to read as follows:

480.930 1. The Office shall prepare and make publicly available a statewide strategic plan that outlines policies, procedures, best practices and recommendations for preparing for and mitigating risks to, and otherwise protecting, the security of information systems in this State and for recovering from and otherwise responding to threats to or attacks on the security of information systems in this State. ***The statewide strategic plan prepared and made available pursuant to this subsection must not identify or include information which allows for the identification of specific vulnerabilities in the information systems in this State.***

2. The statewide strategic plan must include, without limitation, policies, procedures, best practices and recommendations for:

(a) Identifying, preventing and responding to threats to and attacks on the security of information systems in this State;

(b) Ensuring the safety of, and the continued delivery of essential services to, the people of this State in the event of a threat to or attack on the security of an information system in this State;

(c) Protecting the confidentiality of personal information that is stored on, transmitted to, from or through, or generated by an information system in this State;

(d) Investing in technologies, infrastructure and personnel for protecting the security of information systems; and

(e) Enhancing the voluntary sharing of information and any other collaboration among state agencies, local governments,

agencies of the Federal Government and appropriate private entities regarding protecting the security of information systems.

3. The statewide strategic plan must be updated at least every 2 years.

4. A private entity may, in its discretion, make use of the information set forth in the statewide strategic plan.

5. Each agency of the State Government that has adopted a cybersecurity policy shall test the adherence of its employees to that policy on a periodic basis. Such an agency shall submit the results of the testing to the Office annually for consideration in the update of the statewide strategic plan.

Sec. 13. NRS 480.932 is hereby amended to read as follows:

480.932 1. ***The Office shall quarterly prepare and submit to the Governor a report assessing the preparedness of the State, as of the date of the report, to counteract, prevent and respond to potential cybersecurity threats. The report must be based on information and documents readily available to the Office.***

2. The Office shall annually prepare a report that includes, without limitation:

(a) A summary of the progress made by the Office during the previous year in executing, administering and enforcing the provisions of NRS 480.900 to 480.950, inclusive, ***and section 9 of this act*** and performing such duties and exercising such powers as are conferred upon it pursuant to NRS 480.900 to 480.950, inclusive, ***and section 9 of this act*** and any other specific statute;

(b) A general description of any threat during the previous year to the security of an information system that prompted the Administrator to convene a cybersecurity incident response team pursuant to NRS 480.928, and a summary of the response to the threat;

(c) A summary of the goals and objectives of the Office for the upcoming year;

(d) A summary of any issues presenting challenges to the Office; and

(e) Any other information that the Administrator determines is appropriate to include in the report.

~~[2.]~~ ***3.*** The report required pursuant to subsection ~~[1]~~ ***2*** must be submitted not later than July 1 of each year to the Governor and to the Nevada Commission on Homeland Security created by NRS 239C.120.

Sec. 13.5. NRS 480.940 is hereby amended to read as follows:

480.940 1. Any record of a state agency, including the Office, or a local government ***, including, without limitation, a***

record obtained from a private entity, which identifies the detection of, the investigation of or a response to a suspected or confirmed threat to or attack on the security of an information system is not a public record and may be disclosed by the Administrator only to another state agency or local government, a cybersecurity incident response team appointed pursuant to NRS 480.928 and appropriate law enforcement or prosecuting authorities and only for the purposes of preparing for and mitigating risks to, and otherwise protecting, the security of information systems or as part of a criminal investigation.

2. The Office shall not require any private entity to provide any information or data that, in the sole discretion of the private entity, would compromise any information system of the private entity if such information or data were made public.

Sec. 14. This act becomes effective upon passage and approval.