ASSEMBLY BILL NO. 471–COMMITTEE ON JUDICIARY

(ON BEHALF OF THE OFFICE OF THE GOVERNOR)

MARCH 27, 2017

Referred to Committee on Judiciary

SUMMARY—Creates the Nevada Office of Cyber Defense Coordination. (BDR 43-917)

FISCAL NOTE: Effect on Local Government: No.
Effect on the State: Executive Budget.

~

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

AN ACT relating to cybersecurity; creating the Nevada Office of Cyber Defense Coordination within the Department of Public Safety; providing for the powers and duties of the Office; requiring the Nevada Commission on Homeland Security to consider a certain report of the Office when performing certain duties; providing for the confidentiality of certain information regarding cybersecurity; requiring certain state agencies to comply with the provisions of certain regulations adopted by the Office; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

This bill creates the Nevada Office of Cyber Defense Coordination within the Department of Public Safety, to be headed by an Administrator, who is appointed by the Director of the Department and is ex officio a nonvoting member of the Nevada Commission on Homeland Security. Under **section 10** of this bill, the Office must: (1) periodically review the information systems of state agencies; (2) identify risks to the security of those systems; and (3) develop strategies, standards and guidelines for preparing for and mitigating risks to, and otherwise protecting, the security of those systems. The Office must also: (1) coordinate performance audits and assessments of state agencies; and (2) coordinate statewide programs for awareness and training regarding risks to the security of information systems of state agencies.

Under **section 11** of this bill, the Office must establish partnerships with local governments, agencies of the Federal Government, the Nevada System of Higher Education and private entities that have expertise in cybersecurity or information

systems, must consult with the Division of Emergency Management of the Department of Public Safety and the Division of Enterprise Information Technology Services of the Department of Administration regarding strategies to prepare for and mitigate risks to, and otherwise protect, the security of information systems and must coordinate with the Investigation Division of the Department of Public Safety regarding gathering intelligence on and initiating investigations of cyber threats and incidents.

Section 12 of this bill requires the Office to establish policies and procedures for notifications to and by the Office of specific threats to information systems. **Section 12** also requires the Administrator of the Office to appoint a cybersecurity incident response team or teams and requires the Office to establish policies and procedures for the Administrator to convene such a team in the event of a specific threat to the security of an information system.

Section 13 of this bill 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. Under **section 22** of this bill, the first such plan must be prepared and made available not later than January 1, 2018, and under **section 13**, the plan must be updated every 5 years. Under **section 21** of this bill, the Nevada Commission on Homeland Security must consider the most recent plan when performing certain duties.

Section 14 of this bill requires the Office to prepare an annual report on the activities of the Office.

Section 15 of this bill provides that certain information of any state agency, including the Office, 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 only under certain circumstances.

Section 16 of this bill authorizes the Office to adopt any regulations necessary to carry out the provisions of this bill.

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

Section 1. Chapter 480 of NRS is hereby amended by adding thereto the provisions set forth as sections 2 to 16, inclusive, of this act.

Sec. 2. ***The Legislature hereby finds and declares that:***

1. The protection and security of information systems, and the coordination of efforts to promote the protection and security of information systems, are essential to protecting the health, safety and welfare of the people of this State.

2. The continued development of technologies relating to information systems and the expanding and diverse applications of those technologies pose significant implications for the functioning of any infrastructure in this State that is critical to the health, safety and welfare of the people of this State, particularly in the areas of transportation, health care, energy, education, law enforcement and commercial enterprises.

3. Information systems and the application of information systems relating to the operation of State Government and local governments make up a statewide cyberinfrastructure that is integral to the delivery of essential services to the people of this State and the essential functions of government that ensure the protection of the health, safety and welfare of the people of this State.

4. Protecting and securing the statewide cyberinfrastructure requires the identification of the areas in which information systems may be vulnerable to attack, unauthorized use or misuse or other dangerous, harmful or destructive acts.

5. Protecting and securing the statewide cyberinfrastructure requires an ability to identify and eliminate threats to information systems in both the public and private sectors.

6. Protecting and securing the statewide cyberinfrastructure requires a strategic statewide plan for responding to incidents in which information systems are compromised, breached or damaged, including, without limitation, actions taken to:

(a) Minimize the harmful impacts of such incidents on the health, safety and welfare of the people of this State;

(b) Minimize the disruptive effects of such incidents on the delivery of essential services to the people of this State and on the essential functions of government that ensure the protection of the health, safety and welfare of the people of this State; and

(c) Ensure the uninterrupted and continuous delivery of essential services to the people of this State and the uninterrupted and continuous operations of the essential functions of government that ensure the protection of the health, safety and welfare of the people of this State.

7. Protecting and securing the statewide cyberinfrastructure depends on collaboration and cooperation, including the sharing of information and analysis regarding cybersecurity threats, among local, state and federal agencies and across a broad spectrum of the public and private sectors.

8. Institutions of higher education play a critical role in protecting and securing statewide cyberinfrastructure by developing programs that support a skilled workforce, promote innovation and contribute to a more secure statewide cyberinfrastructure.

9. It is therefore in the public interest that the Legislature enact provisions to enable the State to prepare for and mitigate risks to, and otherwise protect, information systems and statewide cyberinfrastructure.

Sec. 3. ***As used in sections 2 to 16, inclusive, of this act, unless the context otherwise requires, the words and terms defined***

in sections 4 to 8, inclusive, of this act have the meanings ascribed to them in those sections.

Sec. 4. *"Administrator" means the Administrator of the Office of Cyber Defense Coordination appointed pursuant to section 9 of this act.*

Sec. 5. *"Information system" means any computer equipment, computer software, procedures or technology used to communicate, collect, process, distribute or store information.*

Sec. 6. *"Office" means the Nevada Office of Cyber Defense Coordination of the Department of Public Safety.*

Sec. 7. *"Security of an information system" includes, without limitation, the security of:*

1. The physical infrastructure of an information system; and

2. Information, including, without limitation, personal information, that is stored on, transmitted to, from or through, or generated by an information system.

Sec. 8. *"State agency" means every public agency, bureau, board, commission, department or division of the Executive Branch of State Government.*

Sec. 9. *The Nevada Office of Cyber Defense Coordination is hereby created and is composed of:*

1. The Administrator of the Office, who is appointed by the Director; and

2. Within the limits of legislative appropriations, a number of employees which the Director determines to be sufficient to carry out the duties of the Office.

Sec. 10. *1. The Office shall:*

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

(b) Identify risks to the security of information systems that are operated or maintained by state agencies.

(c) Develop and update, as necessary, strategies, standards and guidelines 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. ***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 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. 12. ***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 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.

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.

Sec. 13. *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.*

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 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 5 years.

Sec. 14. *1. 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 sections 2 to 16, inclusive, of this act and performing such duties and exercising such powers as are conferred upon it pursuant to sections 2 to 16, inclusive, of this act and any other specific statute;

(b) A 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 section 12 of this act, 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. The report required pursuant to subsection 1 must be submitted not later than January 1 of each year to the Governor, to the Information Technology Advisory Board created by NRS 242.122 and to the Director of Legislative Counsel Bureau.

Sec. 15. ***Any record of a state agency, including the Office, 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 only to another state agency 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.***

Sec. 16. ***1. The Office may adopt any regulations necessary to carry out the provisions of sections 2 to 16, inclusive, of this act.***

2. Every state agency shall, to the extent practicable, comply with the provisions of any regulations adopted by the Office pursuant to sections 2 to 16, inclusive, of this act.

Sec. 17. NRS 480.130 is hereby amended to read as follows:

480.130 The Department consists of:

1. An Investigation Division;
2. A Nevada Highway Patrol Division;
3. A Division of Emergency Management;
4. A State Fire Marshal Division;
5. A Division of Parole and Probation;
6. A Capitol Police Division;
7. ***A Nevada Office of Cyber Defense Coordination;***
8. A Training Division; and

~~[8.]~~ ***9.*** A General Services Division.

Sec. 18. NRS 480.140 is hereby amended to read as follows:

480.140 The primary functions and responsibilities of the divisions of the Department are as follows:

1. The Investigation Division shall:

(a) Execute, administer and enforce the provisions of chapter 453 of NRS relating to controlled substances and chapter 454 of NRS relating to dangerous drugs;

(b) Assist the Secretary of State in carrying out an investigation pursuant to NRS 293.124; and

(c) Perform such duties and exercise such powers as may be conferred upon it pursuant to this chapter and any other specific statute.

2. The Nevada Highway Patrol Division shall, in conjunction with the Department of Motor Vehicles, execute, administer and enforce the provisions of chapters 484A to 484E, inclusive, of NRS and perform such duties and exercise such powers as may be conferred upon it pursuant to NRS 480.360 and any other specific statute.

3. The Division of Emergency Management shall execute, administer and enforce the provisions of chapters 414 and 414A of NRS and perform such duties and exercise such powers as may be conferred upon it pursuant to chapters 414 and 414A of NRS and any other specific statute.

4. The State Fire Marshal Division shall execute, administer and enforce the provisions of chapter 477 of NRS and perform such duties and exercise such powers as may be conferred upon it pursuant to chapter 477 of NRS and any other specific statute.

5. The Division of Parole and Probation shall execute, administer and enforce the provisions of chapters 176A and 213 of NRS relating to parole and probation and perform such duties and exercise such powers as may be conferred upon it pursuant to those chapters and any other specific statute.

6. The Capitol Police Division shall assist in the enforcement of subsection 1 of NRS 331.140.

7. ***The Nevada Office of Cyber Defense Coordination shall:***

(a) Serve as the strategic planning, facilitating and coordinating office for cybersecurity policy and planning in this State; and

(b) Execute, administer and enforce the provisions of sections 2 to 16, inclusive, of this act and perform such duties and exercise such powers as may be conferred upon it pursuant to sections 2 to 16, inclusive, of this act and any other specific statute.

8. The Training Division shall provide training to the employees of the Department.

~~[8.]~~ ***9.*** The General Services Division shall:

(a) Execute, administer and enforce the provisions of chapter 179A of NRS and perform such duties and exercise such powers as may be conferred upon it pursuant to chapter 179A of NRS and any other specific statute;

(b) Provide dispatch services for the Department and other agencies as determined by the Director;

(c) Maintain records of the Department as determined by the Director; and

(d) Provide support services to the Director, the divisions of the Department and the Nevada Criminal Justice Information System as may be imposed by the Director.

Sec. 19. 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, 41.071, 49.095, 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, 130.312, 130.712, 136.050, 159.044, 172.075, 172.245, 176.015, 176.0625, 176.09129, 176.156, 176A.630, 178.39801, 178.4715, 178.5691, 179.495, 179A.070, 179A.165, 179A.450, 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, 250.087, 250.130, 250.140, 250.150, 268.095, 268.490, 268.910, 271A.105, 281.195, 281A.350, 281A.440, 281A.550, 284.4068, 286.110, 287.0438, 289.025, 289.080, 289.387, 289.830, 293.5002, 293.503, 293.558, 293B.135, 293D.510, 331.110, 332.061, 332.351, 333.333, 333.335, 338.070, 338.1379, 338.16925, 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, 372A.080, 378.290, 378.300, 379.008, 385A.830, 385B.100, 387.626, 387.631, 388.1455, 388.259, 388.501, 388.503, 388.513, 388.750, 391.035, 392.029, 392.147, 392.264, 392.271, 392.850, 394.167, 394.1698, 394.447, 394.460, 394.465, 396.3295, 396.405, 396.525, 396.535, 398.403, 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, 432.205, 432B.175, 432B.280, 432B.290, 432B.407, 432B.430, 432B.560, 433.534, 433A.360, 439.840, 439B.420, 440.170, 441A.195, 441A.220, 441A.230, 442.330, 442.395, 445A.665, 445B.570, 449.209, 449.245, 449.720, 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, 481.063, 482.170, 482.5536, 483.340, 483.363, 483.575, 483.659, 483.800, 484E.070, 485.316, 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.745, 640C.760, 640D.190, 640E.340, 641.090, 641A.191, 641B.170, 641C.760, 642.524, 643.189, 644.446, 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, 673.430, 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, 692A.117, 692C.190, 692C.3536, 692C.3538, 692C.354, 692C.420, 693A.480, 693A.615, 696B.550, 703.196, 704B.320, 704B.325, 706.1725, 706A.230, 710.159, 711.600, ***and section 15 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. 20. NRS 239C.120 is hereby amended to read as follows:

239C.120 1. The Nevada Commission on Homeland Security is hereby created.

2. The Governor shall appoint to the Commission 16 voting members that the Governor determines to be appropriate and who serve at the Governor's pleasure, which must include at least:

(a) The sheriff of each county whose population is 100,000 or more.

(b) The chief of the county fire department in each county whose population is 100,000 or more.

(c) A member of the medical community in a county whose population is 700,000 or more.

(d) An employee of the largest incorporated city in each county whose population is 700,000 or more.

(e) A representative of the broadcaster community. As used in this paragraph, "broadcaster" has the meaning ascribed to it in NRS 432.310.

(f) A representative recommended by the Inter-Tribal Council of Nevada, Inc., or its successor organization, to represent tribal governments in Nevada.

3. The Governor shall appoint:

(a) An officer of the United States Department of Homeland Security whom the Department of Homeland Security has designated for this State;

(b) The agent in charge of the office of the Federal Bureau of Investigation in this State; ~~[and]~~

(c) The Chief of the Division ~~[.]~~ ***; and***

(d) The Administrator of the Nevada Office of Cyber Defense Coordination appointed pursuant to section 9 of this act,

➥ as nonvoting members of the Commission.

4. The Senate Majority Leader shall appoint one member of the Senate as a nonvoting member of the Commission.

5. The Speaker of the Assembly shall appoint one member of the Assembly as a nonvoting member of the Commission.

6. The term of office of each member of the Commission who is a Legislator is 2 years.

7. The Governor or his or her designee shall:

(a) Serve as Chair of the Commission; and

(b) Appoint a member of the Commission to serve as Vice Chair of the Commission.

Sec. 21. NRS 239C.160 is hereby amended to read as follows:

239C.160 The Commission shall, within the limits of available money:

1. Make recommendations to the Governor, the Legislature, agencies of this State, political subdivisions, tribal governments, businesses located within this State and private persons who reside in this State with respect to actions and measures that may be taken to protect residents of this State and visitors to this State from potential acts of terrorism and related emergencies.

2. ~~[Make]~~ ***Upon consideration of the most recent statewide strategic plan prepared by the Nevada Office of Cyber Defense Coordination pursuant to section 13 of this act, make*** recommendations to the Governor, through the Division, on the use of money received by the State from any homeland security grant or related program, including, without limitation, the State Homeland Security Grant Program and Urban Area Security Initiative, in accordance with the following:

(a) The Division shall provide the Commission with program guidance and briefings;

(b) The Commission must be provided briefings on existing and proposed projects, and shall consider statewide readiness capabilities and priorities for the use of money, administered by the Division, from any homeland security grant or related program;

(c) The Commission shall serve as the public body which reviews and makes recommendations for the State's applications to the Federal Government for homeland security grants or related programs, as administered by the Division; and

(d) The Commission shall serve as the public body which recommends, subject to approval by the Governor, the distribution

of money from any homeland security grant or related program for use by state, local and tribal government agencies and private sector organizations.

3. Propose goals and programs that may be set and carried out, respectively, to counteract or prevent potential acts of terrorism and related emergencies before such acts of terrorism and related emergencies can harm or otherwise threaten residents of this State and visitors to this State.

4. With respect to buildings, facilities, geographic features and infrastructure that must be protected from acts of terrorism and related emergencies to ensure the safety of the residents of this State and visitors to this State, including, without limitation, airports other than international airports, the Capitol Complex, dams, gaming establishments, governmental buildings, highways, hotels, information technology infrastructure, lakes, places of worship, power lines, public buildings, public utilities, reservoirs, rivers and their tributaries, and water facilities:

(a) Identify and categorize such buildings, facilities, geographic features and infrastructure according to their susceptibility to and need for protection from acts of terrorism and related emergencies; and

(b) Study and assess the security of such buildings, facilities, geographic features and infrastructure from acts of terrorism and related emergencies.

5. Examine the use, deployment and coordination of response agencies within this State to ensure that those agencies are adequately prepared to protect residents of this State and visitors to this State from acts of terrorism and related emergencies.

6. Assess, examine and review the use of information systems and systems of communication used by response agencies within this State to determine the degree to which such systems are compatible and interoperable. After conducting the assessment, examination and review, the Commission shall:

(a) Establish a state plan setting forth criteria and standards for the compatibility and interoperability of those systems when used by response agencies within this State; and

(b) Advise and make recommendations to the Governor relative to the compatibility and interoperability of those systems when used by response agencies within this State, with particular emphasis upon the compatibility and interoperability of public safety radio systems.

7. Assess, examine and review the operation and efficacy of telephone systems and related systems used to provide emergency 911 service.

8. To the extent practicable, cooperate and coordinate with the Division to avoid duplication of effort in developing policies and programs for preventing and responding to acts of terrorism and related emergencies.

9. Submit an annual briefing to the Governor assessing the preparedness of the State to counteract, prevent and respond to potential acts of terrorism and related emergencies, including, but not limited to, an assessment of response plans and vulnerability assessments of utilities, public entities and private business in this State. The briefing must be based on information and documents reasonably available to the Commission and must be compiled with the advice of the Division after all utilities, public entities and private businesses assessed have a reasonable opportunity to review and comment on the Commission's findings.

10. Perform any other acts related to their duties set forth in subsections 1 to 9, inclusive, that the Commission determines are necessary to protect or enhance:

(a) The safety and security of the State of Nevada;

(b) The safety of residents of the State of Nevada; and

(c) The safety of visitors to the State of Nevada.

Sec. 22. The Nevada Office of Cyber Defense Coordination shall prepare and make available to the public the statewide strategic plan required pursuant to section 13 of this act not later than January 1, 2018.

Sec. 23. The provisions of subsection 1 of NRS 218D.380 do not apply to any provision of this act which adds or revises a requirement to submit a report to the Legislature.

Sec. 24. This act becomes effective on July 1, 2017.

㉚