**S.B. 395**

SENATE BILL NO. 395–SENATORS SPEARMAN, CANNIZZARO, DENIS, MANENDO, PARKS; CANCELA, FORD, RATTI, SEGERBLOM AND WOODHOUSE

MARCH 20, 2017

JOINT SPONSORS: ASSEMBLYMEN ARAUJO, FRIERSON AND THOMPSON

Referred to Committee on Government Affairs

SUMMARY—Makes various changes relating to the cybersecurity of critical infrastructure. (BDR 19-794)

FISCAL NOTE: Effect on Local Government: May have Fiscal Impact.
Effect on the State: Yes.

CONTAINS UNFUNDED MANDATE (§ 10)
(NOT REQUESTED BY AFFECTED LOCAL GOVERNMENT)

~

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

AN ACT relating to cybersecurity; requiring the Nevada Commission on Homeland Security to designate certain entities, assets or systems as critical infrastructure; requiring the owner or operator of critical infrastructure to develop and implement a cybersecurity plan; requiring an owner or operator of critical infrastructure to have such a cybersecurity plan evaluated by the Commission or an evaluator of cybersecurity; requiring the owner or operator of critical infrastructure immediately report a significant cybersecurity incident to the Commission; prohibiting, with limited exception, the Commission from disclosing proprietary information or specific information indicating a cybersecurity weakness; requiring evaluators of cybersecurity to be licensed; and providing other matters properly relating thereto.

**Legislative Counsel's Digest:**

Under existing law, the Nevada Commission on Homeland Security, with 16 voting members appointed by the Governor: (1) makes recommendations regarding

actions and measures that may be taken to protect people in this State from potential acts of terrorism and related emergencies; (2) makes recommendations and takes other actions regarding the application for and receipt and use of money from federal grant programs, and other sources, relating to protection from terrorism; (3) identifies and categorizes potential targets of acts of terrorism; and (4) reviews the use and efficacy of 911 systems and other emergency communication systems, including computer systems. (NRS 239C.160) This bill provides that the Commission also has certain duties regarding the cybersecurity of critical infrastructure.

**Section 8** of this bill requires the Commission to designate as critical infrastructure an entity, asset or system that is so vital that the incapacity or destruction thereof would have a debilitating impact on the economy or security of this State or the public health and safety of the citizens of this State. **Section 9** of this bill sets forth the certain considerations for the Commission when developing the requirements for cybersecurity plans. **Section 10** of this bill requires each owner or operator of critical infrastructure to ensure that a cybersecurity plan for the critical infrastructure is developed and implemented. **Section 10** also sets forth certain annual reporting requirements for an owner or operator of critical infrastructure.

**Section 11** of this bill requires that cybersecurity plans for critical infrastructure must be evaluated by: (1) the Commission if the owner or operator of the critical infrastructure is the State or a local government; or (2) an evaluator of cybersecurity if the owner or operator of the critical infrastructure is not the State or a local government. **Section 12** of this bill requires an evaluator of cybersecurity to submit to the Commission a written summary of each evaluation of a cybersecurity plan that is conducted by the evaluator.

**Section 13** of this bill authorizes the Commission to periodically review the development, implementation and evaluation of any cybersecurity plan and take certain actions if the Commission determines that the plan does not adequately address the risks of a cybersecurity plan.

**Section 14** of this bill requires the owner or operator of the critical infrastructure to immediately report any significant cybersecurity incident to the Commission.

**Section 15** of this bill prohibits the Commission from disclosing or authorizing or requiring the disclosure of any proprietary information or information indicating a weakness in the cybersecurity of the critical infrastructure except in certain circumstances.

**Section 17** of this bill requires that an evaluator of cybersecurity must be licensed by the Commission and requires the Commission to establish the qualifications and requirements for becoming a licensed evaluator of cybersecurity. **Section 21** of this bill requires the Commission to monitor the performance of every licensed evaluator of cybersecurity.

---

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

**Section 1.** 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. 2.** Chapter 239C of NRS is hereby amended by adding thereto the provisions set forth as sections 3 to 23, inclusive, of this act.

**Sec. 3.** ***As used in sections 3 to 23, inclusive, of this act, the words and terms defined in sections 4 to 7, inclusive, of this act have the meanings ascribed to them in those sections.***

**Sec. 4.** ***"Critical infrastructure" means an entity, asset or system, whether physical or virtual, that:***

***1. Is owned or operated by the State, a local government, a utility or any person; and***

***2. Has been designated by the Commission pursuant to section 8 of this act as critical infrastructure.***

**Sec. 5.** ***"Evaluator of cybersecurity" means a person licensed pursuant to section 17 of this act to evaluate the cybersecurity plans for critical infrastructure.***

**Sec. 6.** ***"Local government" means every political subdivision and every other governmental entity in this State.***

**Sec. 7.** ***1. "Utility" means any public or private entity that:***

***(a) Provides telecommunications service, water service, electric service or natural gas service to 500 or more service locations; or***

***(b) Operates any pipeline that is necessary to provide such service.***

***2. The term includes, without limitation:***

***(a) A governmental utility.***

***(b) A public utility that is regulated by the Public Utilities Commission of Nevada pursuant to chapter 704 of NRS.***

***(c) A rural electric cooperative established pursuant to chapter 81 of NRS.***

***(d) A cooperative association, nonprofit corporation, nonprofit association or provider of electric service which is declared to be a public utility pursuant to NRS 704.673 and which provides service only to its members.***

***(e) A community water system that is subject to the requirements of 42 U.S.C. § 300i-2.***

**Sec. 8.** ***1. The Commission shall designate as critical infrastructure an entity, asset or system in the State that is so vital that the incapacity or destruction thereof would have a debilitating***

*impact on the economy or security of the State or the public health and safety of the citizens of this State. In determining whether an entity, asset or system should be designated as critical infrastructure, the Commission must consider, without limitation:*

*(a) The relative size of the entity, asset or system;*

*(b) The number of persons who would be impacted if there was a cyberattack on the entity, asset or system; and*

*(c) Any interdependence of the entity, asset or system with other entities, assets or systems in this State.*

*2. If an entity, asset or system is designated as critical infrastructure by the Commission pursuant to subsection 1, the Commission must assign the entity, asset or system into one of the risk tiers of critical infrastructure established by the Commission pursuant to subsection 3.*

*3. The Commission shall establish and periodically update risk tiers of critical infrastructure that are based on:*

*(a) The degree of threat of a cyberattack on the critical infrastructure;*

*(b) The vulnerability of the critical infrastructure to a cyberattack;*

*(c) The extent of the consequences to or impact on the economy and security of the State and the public health and safety of the citizens of this State if there is a cyberattack on the critical infrastructure; and*

*(d) Any other factor that the Commission determines to be relevant.*

*4. The Commission must:*

*(a) Publish a list of critical infrastructure that has been designated as such by the Commission; and*

*(b) Inform the owner or operator of the critical infrastructure of the risk tier in which the critical infrastructure has been assigned.*

**Sec. 9.** *1. For each risk tier established pursuant to section 8 of this act, the Commission shall:*

*(a) Identify specific cybersecurity risks; and*

*(b) Develop and periodically update a framework that sets forth the requirements for cybersecurity plans for critical infrastructure in that risk tier.*

*2. When developing and updating the framework for a risk tier, the Commission shall:*

*(a) Consult with and solicit input from, without limitation, organizations, businesses, individuals and governmental agencies that promote or provide expertise in cybersecurity;*

*(b) Consider:*

***(1) The extent to which the framework minimizes the risks of a successful cyberattack;***

***(2) The cost-effectiveness of the framework;***

***(3) Whether the framework includes outcome-based metrics that measure the practical effectiveness of a cybersecurity plan;***

***(4) Whether the framework includes independent practical assessments or evaluations of cybersecurity plans that are implemented, including, without limitation, the simulation of cyberattacks and any other method of testing for vulnerabilities of critical infrastructure;***

***(5) Whether the framework includes cybersecurity training or other awareness measures for employees and contractors of owners or operators of critical infrastructure; and***

***(6) Incorporating into the framework any appropriate cybersecurity measures or techniques proposed by the National Institute of Standards and Technology of the United States Department of Commerce.***

**Sec. 10.** ***1. The owner or operator of the critical infrastructure shall ensure that a cybersecurity plan is developed and implemented for the critical infrastructure that meets the requirements for the risk tier in which the Commission has designated the critical infrastructure. The owner or operator of the critical infrastructure shall submit to the Commission a written copy of the cybersecurity plan and any significant changes that are made to the plan.***

***2. A cybersecurity plan must be:***

***(a) On file at the main office of the owner or operator of the critical infrastructure.***

***(b) Signed and attested to by the owner or operator of the critical infrastructure or an employee of the owner or operator of the critical infrastructure that has authority for implementing the cybersecurity plan.***

***(c) Available for inspection upon request by the Commission or an evaluator of cybersecurity.***

***3. Except as otherwise provided in this subsection, a summary of each cybersecurity plan must be made available to the public. The summary must be in the form prescribed by the Commission and must not contain any proprietary information or information that indicates any critical weakness of the cybersecurity of the critical infrastructure.***

***4. Pursuant to the schedule established by the Commission pursuant to section 11 of this act, the owner or operator of the critical infrastructure shall ensure that the cybersecurity plan is evaluated:***

*(a) If the critical infrastructure is owned by the State or a local government, by the Commission.*

*(b) If the critical infrastructure is not owned by the State or a local government, by an evaluator of cybersecurity.*

*5. The owner or operator of the critical infrastructure shall on an annual basis report to the Commission whether:*

*(a) The cybersecurity plan is up to date and currently being implemented;*

*(b) The Commission or an evaluator of cybersecurity, as applicable, has evaluated the plan pursuant to the schedule and requirements of the Commission; and*

*(c) The Commission or evaluator of cybersecurity, as applicable, that evaluated the plan concluded that the risk of a cyberattack on the critical infrastructure has been mitigated or the cybersecurity plan has been amended based on the recommendations of the Commission or evaluator of cybersecurity.*

**Sec. 11.** *The cybersecurity plans of critical infrastructure must be evaluated:*

*1. By the Commission pursuant to the schedule adopted by the Commission if the critical infrastructure is owned by the State or a local government.*

*2. By an evaluator of cybersecurity at least once each year if the critical infrastructure is not owned by the State or a local government.*

**Sec. 12.** *1. When the Commission or an evaluator of cybersecurity evaluates a cybersecurity plan pursuant to section 10 of this act, the evaluation must be based on outcome-based metrics that measure the practical effectiveness of the cybersecurity measures included in the plan.*

*2. An evaluator of cybersecurity who conducts an evaluation of a cybersecurity plan pursuant to section 10 of this act must submit to the Commission a written summary of the evaluation, including, without limitation, the findings of the evaluator of cybersecurity regarding the effectiveness of the cybersecurity plan.*

**Sec. 13.** *1. The Commission may review the development, implementation and evaluation of any cybersecurity plan. If the Commission determines after conducting such a review that the risks of a successful cyberattack on critical infrastructure are not adequately addressed by a cybersecurity plan, the Commission may:*

*(a) Enter into discussions with the owner or operator of the critical infrastructure and any governmental agency with regulatory authority over the owner or operator of the critical infrastructure regarding the further development and*

*implementation of a plan to minimize the risk of a successful cyberattack on the critical infrastructure; and*

*(b) Provide technical assistance, or facilitate the provision of technical assistance, to the owner or operator of the critical infrastructure regarding minimizing the risk of a successful cyberattack on the critical infrastructure.*

*2. If, after taking the steps described in subsection 1, the Commission determines that the risk of a successful cyberattack on the critical infrastructure is still not being adequately addressed, the Commission may:*

*(a) Issue a public statement that the risk of a successful cyberattack on the critical infrastructure is not being adequately addressed; and*

*(b) Except as otherwise provided in section 16 of this act, take any other appropriate actions that are intended to encourage the owner or operator of the critical infrastructure to further develop and implement a cybersecurity plan to minimize the risk of a successful cyberattack on the critical infrastructure.*

**Sec. 14.** *1. The owner or operator of the critical infrastructure must immediately report a significant cybersecurity incident, including, without limitation, a cybersecurity attack, to the Commission.*

*2. The Commission, in cooperation with the Attorney General, shall adopt regulations establishing standards and procedures for reporting any significant cybersecurity incident.*

**Sec. 15.** *1. Except as otherwise provided in subsection 2, when carrying out its powers and duties pursuant to sections 3 to 23, inclusive, of this act, the Commission shall not disclose, or authorize or require the disclosure of, any proprietary information or specific information indicating that there is a weakness in the cybersecurity of the critical infrastructure. Except as otherwise provided in subsection 2, the records and portions of records that are assembled, maintained, overseen or prepared by the Commission to mitigate, prevent or respond to cyberattacks are confidential and not public records.*

*2. The Commission may disclose, or authorize the disclosure of, any information if:*

*(a) Disclosure is required pursuant to federal law;*

*(b) The Commission determines that disclosure is necessary to prevent or mitigate the effects of a cyberattack;*

*(c) The Commission determines that disclosure will further the functions of a governmental agency; or*

*(d) The information is requested by a legislative committee having jurisdiction over issues related to cybersecurity.*

**Sec. 16.** *1. A governmental agency with regulatory authority over the owner or operator of the critical infrastructure, including, without limitation, the Commission, may not take any civil or disciplinary action against the owner or operator of the critical infrastructure for failing or refusing to take any action required by the provisions of sections 3 to 23, inclusive, of this act.*

*2. Injunctive relief requiring the owner or operator of the critical infrastructure to take any action required by the provisions of sections 3 to 23, inclusive, of this act may not be granted.*

*3. The owner or operator of the critical infrastructure may appeal any decision or order of the Commission by requesting a hearing pursuant to the provisions of NRS 233B.121 to 233B.150, inclusive.*

**Sec. 17.** *1. A person shall not conduct an evaluation of critical infrastructure that is required pursuant to section 11 of this act unless the person is licensed as an evaluator of cybersecurity by the Commission.*

*2. The Commission shall establish by regulation:*

*(a) The qualifications to obtain a license as an evaluator of cybersecurity.*

*(b) The annual fee that must be paid for a license as an evaluator of cybersecurity. The Commission shall establish the amount of the annual fee such that the total amount of licensing fees collected must pay for the annual expenses of the Commission to carry out the provisions of sections 3 to 23, inclusive, of this act.*

*(c) The requirements and fees for renewal of a license as an evaluator of cybersecurity.*

*(d) Adopt and amend rules of professional conduct appropriate to establish and maintain a high standard of quality, integrity and dignity in the profession of evaluator of cybersecurity.*

*3. A current or former member or employee of the Commission may not obtain a license as an evaluator of cybersecurity for at least 1 year after the termination of the member's or employee's service or period of employment.*

**Sec. 18.** *1. In addition to any other requirements set forth in this chapter and any regulations adopted thereto, an applicant for the issuance of a license as an evaluator of cybersecurity shall:*

*(a) Include the social security number of the applicant in the application submitted to the Commission.*

*(b) Submit to the Commission the statement prescribed by the Division of Welfare and Supportive Services of the Department of Health and Human Services pursuant to NRS 425.520. The statement must be completed and signed by the applicant.*

*2. The Commission shall include the statement required pursuant to subsection 1 in:*

*(a) The application or any other forms that must be submitted for the issuance or renewal of the license; or*

*(b) A separate form prescribed by the Commission.*

*3. A license may not be issued or renewed by the Commission if the applicant:*

*(a) Fails to submit the statement required pursuant to subsection 1; or*

*(b) Indicates on the statement submitted pursuant to subsection 1 that the applicant is subject to a court order for the support of a child and is not in compliance with the order or a plan approved by the district attorney or other public agency enforcing the order for the repayment of the amount owed pursuant to the order.*

*4. If an applicant indicates on the statement submitted pursuant to subsection 1 that the applicant is subject to a court order for the support of a child and is not in compliance with the order or a plan approved by the district attorney or other public agency enforcing the order for the repayment of the amount owed pursuant to the order, the Commission shall advise the applicant to contact the district attorney or other public agency enforcing the order to determine the actions that the applicant may take to satisfy the arrearage.*

**Sec. 19.** *1. If the Commission receives a copy of a court order issued pursuant to NRS 425.450 that provides for the suspension of all professional, occupational and recreational licenses, certificates and permits issued to a person who is a holder of a license as an evaluator of cybersecurity, the Commission shall deem the license issued to that person to be suspended at the end of the 30th day after the date on which the court order was issued unless the Commission receives a letter issued to the holder of the license by the district attorney or other public agency pursuant to NRS 425.550 stating that the holder of the license has complied with the subpoena or warrant or has satisfied the arrearage pursuant to NRS 425.560.*

*2. The Commission shall reinstate a license that has been suspended by a district court pursuant to NRS 425.540 if the Commission receives a letter issued by the district attorney or other public agency pursuant to NRS 425.550 to the person whose license was suspended stating that the person whose license was suspended has complied with the subpoena or warrant or has satisfied the arrearage pursuant to NRS 425.560.*

**Sec. 20.** *1. In addition to any other requirements set forth in sections 3 to 23, inclusive, of this act or by regulation, an applicant for the renewal of a license as an evaluator of cybersecurity must indicate in the application submitted to the*

*Commission whether the applicant has a state business registration. If the applicant has a state business registration, the applicant must include in the application the business identification number assigned by the Secretary of State upon compliance with the provisions of chapter 76 of NRS.*

*2. A license as an evaluator of cybersecurity may not be renewed if:*

*(a) The applicant fails to submit the information required by subsection 1; or*

*(b) The State Controller has informed the Commission pursuant to subsection 5 of NRS 353C.1965 that the applicant owes a debt to an agency that has been assigned to the State Controller for collection and the applicant has not:*

*(1) Satisfied the debt;*

*(2) Entered into an agreement for the payment of the debt pursuant to NRS 353C.130; or*

*(3) Demonstrated that the debt is not valid.*

*3. As used in this section:*

*(a) "Agency" has the meaning ascribed to it in NRS 353C.020.*

*(b) "Debt" has the meaning ascribed to it in NRS 353C.040.*

**Sec. 21.** *1. The Commission shall monitor the performance of every evaluator of cybersecurity to ensure that the evaluator of cybersecurity complies with the provisions of sections 3 to 23, inclusive, of this act, and any regulations adopted pursuant thereto. The Commission may review the work of any evaluator of cybersecurity to determine if the evaluator has complied with the provisions of sections 3 to 23, inclusive, of this act, and any regulations adopted pursuant thereto.*

*2. If the Commission finds that an evaluator of cybersecurity has not complied with any provision of sections 3 to 23, inclusive, of this act, or any regulation adopted pursuant thereto, the Commission may suspend or revoke the license of the evaluator of cybersecurity.*

*3. If the Commission suspends or revokes a license of an evaluator of cybersecurity, the licensee may request that the Commission hold a hearing pursuant to the provisions of NRS 233B.121 to 233B.150, inclusive. The decision of the Commission is a final decision for purposes of judicial review.*

**Sec. 22.** *The Commission may apply for and accept any gift, donation, bequest, grant or other source of money to carry out the provisions of sections 3 to 23, inclusive, of this act.*

**Sec. 23.** *The Commission shall adopt any regulations necessary to carry out the provisions of sections 3 to 23, inclusive, of this act.*

**Sec. 24.** The provisions of NRS 354.599 do not apply to any additional expenses of a local government that are related to the provisions of this act.

**Sec. 25.** 1. This act becomes effective on:

(a) July 1, 2017, for the purpose of adopting regulations and performing any other preparatory administrative tasks necessary to carry out the provisions of this act; and

(b) On January 1, 2018, for all other purposes.

2. Sections 18 and 19 of this act expire by limitation on the date on which the provisions of 42 U.S.C. § 666 requiring each state to establish procedures under which the state has authority to withhold or suspend, or to restrict the use of professional, occupational and recreational licenses of persons who:

(a) Have failed to comply with a subpoena or warrant relating to a proceeding to determine the paternity of a child or to establish or enforce an obligation for the support of a child; or

(b) Are in arrears in the payment for the support of one or more children,

➥ are repealed by the Congress of the United States.

㉚