Senate Bill No. 12–Committee on Government Affairs

CHAPTER.....

AN ACT relating to governmental administration; creating and setting forth the composition of the Governor's Technology Office within the Office of the Governor; transferring the powers and duties of the Office of the Chief Information Officer within the Office of the Governor to the Governor's Technology Office; revising the classification and duties of the Deputy Chief of the Office of Information Security; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law creates the Office of the Chief Information Officer within the Office of the Governor, consisting of certain units, offices and other units, groups divisions or departments. (NRS 242.080) Existing law sets forth certain duties and responsibilities of the Office of the Chief Information Officer, including providing certain information services to state agencies, elected state officers and, under certain circumstances, agencies not under the control of the Governor and local government agencies. (NRS 242.131, 242.141)

Section 6 of this bill renames the Office of the Chief Information Officer as the Governor's Technology Office. **Sections 1, 3-5, 7, 9, 11-14, 16, 18 and 23-30** of this bill make conforming changes by applying various provisions of the Nevada Revised Statutes relating to the Office of the Chief Information Officer instead to the Governor's Technology Office.

Existing law provides that the Office of the Chief Information Officer is composed of: (1) the Administration Unit; (2) the Client Services Unit; (3) the Computing Services Unit; (4) the Network Services Unit, including a Network Transport Services Group and a Telecommunications Group; (5) the Office of Information Security; and (6) certain other units, groups, divisions or departments deemed necessary by the Chief Information Officer. (NRS 242.080) **Section 6** provides instead that the Governor's Technology Office is composed of: (1) the Director's Office; (2) the Client Services Division; (3) the Computing Services Division; (4) the Network Services Division, including a Network Transport Services Unit and a Unified Communications Unit; (5) the Office of Information Security; and (6) certain other units, groups, divisions or departments deemed necessary by the Chief Information Officer. **Sections 10, 17, 19-22 and 25** of this bill make conforming changes to apply various provisions of the Nevada Revised Statutes relating to the former units, groups, offices, divisions or departments of the Office of the Chief Information Officer instead to the units, groups, offices, divisions or departments of the Governor's Technology Office.

Existing law requires the Chief Information Officer to appoint a Deputy Chief of the Office of Information Security who is in the classified service of the State. (NRS 242.101) **Section 7** instead places the Deputy Chief of the Office of Information Security in the unclassified service of the State. **Section 31** of this bill clarifies that the person who is in the position of Deputy Chief of the Office on July 1, 2025, is in the classified service and must remain in the classified service until he or she vacates that position.

Existing law creates an Information Technology Advisory Board, which has various duties including: (1) advising the Office of the Chief Information Officer concerning issues relating to information technology; (2) periodically reviewing the Office's statewide strategic plans and standards manual for information technology;

(3) reviewing the Office's budget; and (4) consulting and coordinating with state agencies on certain regulations, policies, standards and guidelines. (NRS 242.122, 242.124, 242.125) **Section 8** of this bill replaces the Director of the Department of Administration as a member of the Advisory Board with the Chief Information Officer.

Existing law: (1) requires the Chief of the Office of Information Security to investigate and resolve certain breaches related to an information system of a state agency or elected official in certain circumstances; and (2) authorizes the Chief of the Office of Information Security to notify members of certain boards and commissions of a breach of certain information systems in certain circumstances. (NRS 242.183) **Section 9** instead: (1) requires the Deputy Chief of the Office of Information Security to investigate and resolve such breaches; and (2) authorizes the Deputy Chief to provide such notifications.

Senate Bill No. 431 of the 2023 Legislative Session eliminated the Division of Enterprise Information Technology Services of the Department of Administration and transferred the powers and duties of the Division to the Office of the Chief Information Officer. (Chapter 532, Statutes of Nevada 2023, at page 3544) Existing law defines the terms "Administrator," "Department" and "Division" as they relate to the former Division. (NRS 233F.015, 233F.055, 233F.059, 242.013, 242.031, 242.045) **Section 34** of this bill repeals these obsolete definitions. **Sections 2 and 15** of this bill make conforming changes to eliminate references to certain repealed definitions.

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. NRS 239.073 is hereby amended to read as follows:

239.073 1. The Committee to Approve Schedules for the Retention and Disposition of Official State Records, consisting of six members, is hereby created.

2. The Committee consists of:

(a) The Secretary of State;

(b) The Attorney General;

(c) The Director of the Department of Administration;

(d) The State Library, Archives and Public Records Administrator;

(e) The Chief of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor; and

(f) One member who is a representative of the general public appointed by the Governor.

➥ All members of the Committee, except the representative of the general public, are ex officio members of the Committee.

3. The Secretary of State or a person designated by the Secretary of State shall serve as Chair of the Committee. The State Library, Archives and Public Records Administrator shall serve as

Secretary of the Committee and prepare and maintain the records of the Committee.

4. The Committee shall meet at least quarterly and may meet upon the call of the Chair.

5. An ex officio member of the Committee may designate a person to represent the ex officio member at any meeting of the Committee. The person designated may exercise all the duties, rights and privileges of the member that the person represents.

6. The Committee may adopt rules and regulations for its management.

Sec. 2. NRS 242.011 is hereby amended to read as follows:

242.011 As used in this chapter, unless the context otherwise requires, the words and terms defined in NRS ~~[242.013]~~ ***242.015*** to 242.068, inclusive, have the meanings ascribed to them in those sections.

Sec. 3. NRS 242.017 is hereby amended to read as follows:

242.017 "Chief" or "Chief Information Officer" means the Chief of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor.

Sec. 4. NRS 242.062 is hereby amended to read as follows:

242.062 "Office" means the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor.

Sec. 5. NRS 242.071 is hereby amended to read as follows:

242.071 1. The Legislature hereby determines and declares that the creation of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor is necessary for the coordinated, orderly and economical processing of data and information in State Government, to ensure economical use of information systems and to prevent the unnecessary proliferation of equipment and personnel among the various state agencies.

2. The purposes of the Office are:

(a) To perform information services for state agencies.

(b) To provide technical advice but not administrative control of the information systems within the state agencies and, as authorized, of local governmental agencies.

Sec. 6. NRS 242.080 is hereby amended to read as follows:

242.080 1. The ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ is hereby created within the Office of the Governor.

2. The Office consists of the Chief ***Information Officer*** and:

(a) The ~~[Administration Unit.]~~ ***Director's Office.*** The Chief is the head of the ~~[Administration Unit.]~~ ***Director's Office.***

(b) The Client Services ~~[Unit.]~~ ***Division.***

(c) The Computing Services ~~[Unit.]~~ ***Division.***

(d) The Network Services ~~[Unit.]~~ ***Division.***

(e) The Office of Information Security.

(f) Other units, groups, divisions or departments deemed necessary by the Chief to the extent such functions are supported by the appropriations allocated to the functions of the Office.

3. A Network Transport Services ~~[Group]~~ ***Unit*** and a ~~[Telecommunications Group]~~ ***Unified Communications Unit*** are hereby created within the Network Services ~~[Unit]~~ ***Division*** of the Office.

Sec. 7. NRS 242.101 is hereby amended to read as follows:

242.101 1. The Chief Information Officer shall:

(a) Appoint a Deputy Chief of the Office of Information Security who is in the ~~[classified]~~ ***unclassified*** service of the State;

(b) Administer the provisions of this chapter and other provisions of law relating to the duties of the ***Governor's Technology*** Office ***;*** ~~[of the Chief Information Officer;]~~

(c) Employ, within the limits of the approved budget of the Office, such other staff as is necessary for the performance of the duties of the Office; and

(d) Carry out other duties and exercise other powers specified by law.

2. The Chief may form committees to establish standards and determine criteria for evaluation of policies relating to informational services.

Sec. 8. NRS 242.122 is hereby amended to read as follows:

242.122 1. There is hereby created an Information Technology Advisory Board. The Board consists of:

(a) One member appointed by the Majority Floor Leader of the Senate from the membership of the Senate Standing Committee on Finance.

(b) One member appointed by the Speaker of the Assembly from the membership of the Assembly Standing Committee on Ways and Means.

(c) Two representatives of using agencies which are major users of the services of the Office. The Governor shall appoint the two representatives. Each such representative serves for a term of 4 years. For the purposes of this paragraph, an agency is a "major user" if it is among the top five users of the services of the Office, based on the amount of money paid by each agency for the services of the Office during the immediately preceding biennium.

(d) The ~~[Director]~~ ***Chief*** of the ~~[Department]~~ ***Office*** or his or her designee.

(e) The Attorney General or his or her designee.

(f) Five persons appointed by the Governor as follows:

(1) Three persons who represent a city or county in this State, at least one of whom is engaged in information technology or information security; and

(2) Two persons who represent the information technology industry but who:

(I) Are not employed by this State;

(II) Do not hold any elected or appointed office in State Government;

(III) Do not have an existing contract or other agreement to provide information services, systems or technology to an agency of this State; and

(IV) Are independent of and have no direct or indirect pecuniary interest in a corporation, association, partnership or other business organization which provides information services, systems or technology to an agency of this State.

2. Each person appointed pursuant to paragraph (f) of subsection 1 serves for a term of 4 years. No person so appointed may serve more than 2 consecutive terms.

3. At the first regular meeting of each calendar year, the members of the Board shall elect a Chair by majority vote.

Sec. 9. NRS 242.183 is hereby amended to read as follows:

242.183 1. The ***Deputy*** Chief of the Office of Information Security shall investigate and resolve any breach of an information system of a state agency or elected officer that uses the equipment or services of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ or an application of such an information system or unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of such an information system.

2. The Chief Information Officer or ***Deputy*** Chief of the Office of Information Security, at his or her discretion, may inform members of the Technological Crime Advisory Board created by NRS 205A.040, the Nevada Commission on Homeland Security created by NRS 239C.120 and the Information Technology Advisory Board created by NRS 242.122 of any breach of an information system of a state agency or elected officer or application of such an information system or unauthorized acquisition of computerized data or information that materially compromises the security, confidentiality or integrity of such an information system.

Sec. 10. NRS 242.191 is hereby amended to read as follows:

242.191 1. Except as otherwise provided in subsection 3, the amount receivable from a state agency or officer or local governmental agency which uses the services of the Office must be determined by the Chief in each case and include:

(a) The annual expense, including depreciation, of operating and maintaining the Network Services ~~[Unit,]~~ ***Division,*** distributed among the agencies in proportion to the services performed for each agency.

(b) A service charge in an amount determined by distributing the monthly installment for the construction costs of the computer facility among the agencies in proportion to the services performed for each agency.

2. The Chief shall prepare and submit monthly to the state agencies and officers and local governmental agencies for which services of the Office have been performed an itemized statement of the amount receivable from each state agency or officer or local governmental agency.

3. The Chief may authorize, if in his or her judgment the circumstances warrant, a fixed cost billing, including a factor for depreciation, for services rendered to a state agency or officer or local governmental agency.

Sec. 11. NRS 205.4765 is hereby amended to read as follows:

205.4765 1. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization:

(a) Modifies;

(b) Damages;

(c) Destroys;

(d) Discloses;

(e) Uses;

(f) Transfers;

(g) Conceals;

(h) Takes;

(i) Retains possession of;

(j) Copies;

(k) Obtains or attempts to obtain access to, permits access to or causes to be accessed; or

(l) Enters,

➥ data, a program or any supporting documents which exist inside or outside a computer, system or network is guilty of a misdemeanor.

2. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization:

(a) Modifies;
(b) Destroys;
(c) Uses;
(d) Takes;
(e) Damages;
(f) Transfers;
(g) Conceals;
(h) Copies;
(i) Retains possession of; or
(j) Obtains or attempts to obtain access to, permits access to or causes to be accessed,

➥ equipment or supplies that are used or intended to be used in a computer, system or network is guilty of a misdemeanor.

3. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization:
(a) Destroys;
(b) Damages;
(c) Takes;
(d) Alters;
(e) Transfers;
(f) Discloses;
(g) Conceals;
(h) Copies;
(i) Uses;
(j) Retains possession of; or
(k) Obtains or attempts to obtain access to, permits access to or causes to be accessed,

➥ a computer, system or network is guilty of a misdemeanor.

4. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization:
(a) Obtains and discloses;
(b) Publishes;
(c) Transfers; or
(d) Uses,

➥ a device used to access a computer, network or data is guilty of a misdemeanor.

5. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization introduces, causes to be introduced or attempts to introduce a computer contaminant into a computer, system or network is guilty of a misdemeanor.

6. If the violation of any provision of this section:
(a) Was committed to devise or execute a scheme to defraud or illegally obtain property;

(b) Caused response costs, loss, injury or other damage in excess of $500; or

(c) Caused an interruption or impairment of a public service, including, without limitation, a governmental operation, a system of public communication or transportation or a supply of water, gas or electricity,

➥ the person is guilty of a category C felony and shall be punished as provided in NRS 193.130, and may be further punished by a fine of not more than $100,000. In addition to any other penalty, the court shall order the person to pay restitution.

7. The provisions of this section do not apply to a person performing any testing, including, without limitation, penetration testing, of an information system of an agency that uses the equipment or services of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor that is authorized by the Chief ~~[of that Office]~~ ***Information Officer*** or the head of the Office of Information Security of the ***Governor's Technology*** Office **.** ~~[of the Chief Information Officer.]~~ As used in this subsection:

(a) "Information system" has the meaning ascribed to it in NRS 242.057.

(b) "Penetration testing" has the meaning ascribed to it in NRS 242.171.

Sec. 12. NRS 205A.040 is hereby amended to read as follows:

205A.040 1. The Technological Crime Advisory Board is hereby created.

2. The Board consists of 13 members as follows:

(a) The Attorney General.

(b) The Chief ***Information Officer*** of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor.

(c) One member of the Senate appointed by the Majority Leader of the Senate.

(d) One member of the Assembly appointed by the Speaker of the Assembly.

(e) Nine other persons appointed by the Governor as follows:

(1) Two or more persons who represent major sectors of the economy of this State that are impacted significantly by technological crimes.

(2) One or more persons who are employees of a law enforcement agency of this State.

(3) One or more persons who are employees of a public educational institution within this State.

(4) One or more persons who are residents of this State and who are employed by the Federal Government.

3. Each member of the Board who is appointed to the Board serves for a term of 4 years. A vacancy on the Board in an appointed position must be filled in the same manner as the original appointment. A member may be reappointed to the Board.

4. The members of the Board shall elect a Chair and Vice Chair by majority vote. After the initial election, the Chair and Vice Chair shall hold office for a term of 1 year beginning on July 1 of each year. If the position of Chair or Vice Chair becomes vacant, the members of the Board shall elect a Chair or Vice Chair, as appropriate, from among its members for the remainder of the unexpired term.

5. The members of the Board:

(a) Serve without compensation; and

(b) May, upon written request, receive the per diem allowance and travel expenses provided for state officers and employees generally while engaged in the business of the Board.

6. A member of the Board who is an officer or employee of this State or a political subdivision of this State must be relieved from duties without loss of regular compensation so that the officer or employee may prepare for and attend meetings of the Board and perform any work necessary to carry out the duties of the Board in the most timely manner practicable. A state agency or political subdivision of this State shall not require an officer or employee who is a member of the Board to make up the time the officer or employee is absent from work to carry out duties as a member of the Board or use annual vacation or compensatory time for the absence.

Sec. 13. NRS 205A.050 is hereby amended to read as follows:

205A.050 1. The Board shall meet at least once every quarter and at the times and places specified by a call of the Chair or a majority of the members of the Board.

2. Except as otherwise provided in subsection 3, a member of the Board may designate in writing a person to represent him or her at a meeting of the Board if it is impractical for the member of the Board to attend the meeting. A representative who has been so designated:

(a) Shall be deemed to be a member of the Board for the purpose of determining a quorum at the meeting; and

(b) May vote on any matter that is voted on by the regular members of the Board at the meeting.

3. The Attorney General may designate a representative to serve in his or her place on the Board or attend a meeting of the

Board in his or her place. The Chief ***Information Officer*** of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor may designate a representative to serve in his or her place on the Board or attend a meeting of the Board in his or her place.

4. Seven members of the Board constitute a quorum. Except as otherwise provided in NRS 205A.070 and 205A.080, a quorum may exercise all the power and authority conferred on the Board.

5. Notwithstanding any other provision of law, a member of the Board:

(a) Is not disqualified from public employment or holding a public office because of membership on the Board; and

(b) Does not forfeit public office or public employment because of membership on the Board.

Sec. 14. NRS 205A.060 is hereby amended to read as follows:

205A.060 The Board shall:

1. Facilitate cooperation between state, local and federal officers in detecting, investigating and prosecuting technological crimes.

2. Establish, support and assist in the coordination of activities between two multiagency task forces on technological crime, one based in Reno and one based in Las Vegas, consisting of investigators and forensic examiners who are specifically trained to investigate technological crimes.

3. Coordinate and provide training and education for members of the general public, private industry and governmental agencies, including, without limitation, law enforcement agencies, concerning the statistics and methods of technological crimes and how to prevent, detect and investigate technological crimes.

4. Assist the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor in securing governmental information systems against illegal intrusions and other criminal activities.

5. Evaluate and recommend changes to the existing civil and criminal laws relating to technological crimes in response to current and projected changes in technology and law enforcement techniques.

6. Distribute money deposited pursuant to NRS 179.1233 into the Account for the Technological Crime Advisory Board in accordance with the provisions of NRS 205A.090.

7. Authorize the payment of expenses incurred by the Board in carrying out its duties pursuant to this chapter.

Sec. 15. NRS 233F.010 is hereby amended to read as follows:

233F.010 As used in this chapter, unless the context otherwise requires, the words and terms defined in NRS ~~[233F.015]~~ ***233F.020*** to 233F.065, inclusive, have the meanings ascribed to them in those sections.

Sec. 16. NRS 233F.035 is hereby amended to read as follows:

233F.035 "Chief" means the Chief Information Officer ***of the Governor's Technology Office*** within the Office of the Governor.

Sec. 17. NRS 233F.0593 is hereby amended to read as follows:

233F.0593 "Network Transport Services ~~[Group"]~~ ***Unit"*** means the Network Transport Services ~~[Group]~~ ***Unit*** of the Network Services ~~[Unit]~~ ***Division*** of the Office.

Sec. 18. NRS 233F.0595 is hereby amended to read as follows:

233F.0595 "Office" means the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor.

Sec. 19. NRS 233F.065 is hereby amended to read as follows:

233F.065 ~~["Telecommunications Group"]~~ ***"Unified Communications Unit"*** means the ~~[Telecommunications Group]~~ ***Unified Communications Unit*** of the Network Services ~~[Unit]~~ ***Division*** of the Office.

Sec. 20. NRS 233F.117 is hereby amended to read as follows:

233F.117 If a state agency other than the Network Transport Services ~~[Group]~~ ***Unit*** adds equipment which extends the state communications system to another location, the extension, if approved by the Chief, becomes part of the state communications system. An approved extension of the system is subject to the provisions of this chapter relating to the system.

Sec. 21. NRS 233F.260 is hereby amended to read as follows:

233F.260 The Board shall provide advice to the ~~[Telecommunications Group]~~ ***Unified Communications Unit*** on the use of telecommunications by the State Government, including:

1. The development of policies, standards, plans and designs;
2. The procurement of systems, facilities and services;
3. The integration of telecommunications systems with other state and local governmental systems; and
4. New technology that may become or is available.

Sec. 22. NRS 233F.270 is hereby amended to read as follows:

233F.270 1. The ~~[Telecommunications Group,]~~ ***Unified Communications Unit,*** with the advice of the Board, shall:

(a) Plan, carry out and administer a state telecommunications system. When available at a competitive cost, the ~~[Telecommunications Group]~~ ***Unified Communications Unit*** shall use the facilities of telephone companies providing local exchange service.

(b) Make arrangements for the installation of a central telephone switchboard or switchboards to serve the state offices in one or more buildings as may be practical or feasible.

2. The system must be integrated and may include services between the State and any cities, counties and schools.

3. The Office may consider for the system all the telecommunications requirements of the State and its political subdivisions.

Sec. 23. NRS 408.55028 is hereby amended to read as follows:

408.55028 1. The Telecommunications Advisory Council is hereby created.

2. The Council consists of seven members appointed by the Governor. The Governor shall appoint to the Council:

(a) One member from the Office of Science, Innovation and Technology in the Office of the Governor;

(b) One member from the Department of Transportation;

(c) One member from the Department of Education;

(d) One member from the Nevada Office of Rural Health;

(e) One member from the Department of Public Safety;

(f) One member from the Nevada System of Higher Education; and

(g) One member from the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor.

3. The member appointed from the Office of Science, Innovation and Technology in the Office of the Governor shall serve as the Chair of the Council.

4. The Council shall meet as necessary at the call of the Chair.

5. The Director of the Office of Science, Innovation and Technology in the Office of the Governor shall provide staff support to the Council.

6. A majority of the members of the Council constitutes a quorum for the transaction of business.

7. The members of the Council receive no compensation for their services, but are entitled to be reimbursed for all travel and other expenses actually and necessarily incurred by them in the performance of their duties, within the limits of money available to the Council.

8. The members of the Council may request assistance from technical advisors as the Council deems necessary.

9. The Council shall:

(a) Provide information, advice, strategic plans, priorities and recommendations to assist the Department in administering access to rights-of-way to telecommunications providers for statewide telecommunications purposes;

(b) Assist the Department in valuing in-kind compensation pursuant to NRS 408.5501 to 408.55029, inclusive, and approve or deny any valuation thereof;

(c) Seek input from telecommunications providers and the public relating to broadband access;

(d) Coordinate and exchange information with other entities of this State and its political subdivisions relating to technology and telecommunications;

(e) Approve or deny any agreement between the Department and a telecommunications provider proposed pursuant to NRS 408.5502, if the Council finds that the agreement is competitively neutral and nondiscriminatory; and

(f) Provide other assistance as requested by the Department.

Sec. 24. NRS 439.942 is hereby amended to read as follows:

439.942 1. The Division may establish a secure Internet website which makes certain information available for a website client to conduct an investigation into the background and personal history of a person that is required pursuant to the provisions of this chapter or chapter 62B, 63, 424, 427A, 432, 432A, 432B, 433, 433B, 435 or 449 of NRS.

2. To become a website client, a person or governmental entity must:

(a) Create an account on the Internet website;

(b) Comply with NRS 439.942 to 439.948, inclusive, and any regulations adopted pursuant thereto governing use of the Internet website; and

(c) Designate a website client administrator who is responsible for:

(1) Determining the persons who are authorized to use the Internet website;

(2) Providing the Division with the names of the persons who are authorized to use the Internet website;

(3) Ensuring that only those authorized persons have access to the Internet website; and

(4) Notifying the Division of any change in the persons who are authorized to use the Internet website.

3. Authorized employees of the Division and of the Department of Public Safety may be designated to serve as administrators of the Internet website with access to all the data and information on the Internet website.

4. Except as otherwise provided in this section and NRS 239.0115, information collected, maintained, stored, backed up or on file on the Internet website is confidential, not subject to subpoena or discovery and is not subject to inspection by the general public.

5. The Division shall ensure that any information collected, maintained and stored on the Internet website is protected adequately from fire, theft, loss, destruction, other hazards and unauthorized access, and is backed-up in a manner that ensures proper confidentiality and security.

6. The Internet website must be maintained in accordance with any requirements of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor established for use of the equipment or services of the Office pursuant to NRS 242.181.

Sec. 25. NRS 459.742 is hereby amended to read as follows:

459.742 The Commission, in carrying out its duties and within the limits of legislative appropriations and other available money, may:

1. Enter into contracts, leases or other agreements or transactions;

2. Provide grants of money to local emergency planning committees to improve their ability to respond to emergencies involving hazardous materials;

3. Assist with the development of comprehensive plans for responding to such emergencies in this State;

4. Provide technical assistance and administrative support to the ~~[Telecommunications Group]~~ ***Unified Communications Unit*** of the Network Services ~~[Unit]~~ ***Division*** of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor for the development of systems for communication during such emergencies;

5. Provide technical and administrative support and assistance for training programs;

6. Develop a system to provide public access to data relating to hazardous materials;

7. Support any activity or program eligible to receive money from the Contingency Account for Hazardous Materials;

8. Approve programs developed to address planning for and responding to emergencies involving hazardous materials; and

9. Coordinate the activities administered by state agencies to carry out the provisions of this chapter, 42 U.S.C. §§ 11001 et seq. and 49 U.S.C. §§ 5101 et seq.

Sec. 26. 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, 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 Office of the Military and the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor 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. 27. NRS 493.118 is hereby amended to read as follows:

493.118 1. The Department shall, to the extent that money is available for this purpose, establish and maintain a registry of unmanned aerial vehicles that are operated by public agencies in this State. The Department shall include on its Internet website the information that is maintained in the registry.

2. A public agency shall, for each unmanned aerial vehicle the public agency intends to operate, submit to the Department, on a form provided by the Department, for inclusion in the registry:

(a) The name of the public agency;

(b) The name and contact information of each operator of the unmanned aerial vehicle;

(c) Sufficient information to identify the unmanned aerial vehicle; and

(d) A statement describing the use of the unmanned aerial vehicle by the public agency.

3. The Department shall, on or before February 1 of each year, prepare and submit to the Director of the Legislative Counsel Bureau for submission to the Legislature, or to the Legislative Commission when the Legislature is not in regular session, a report outlining the activities of public agencies with respect to the operation of unmanned aerial vehicles in this State.

4. The Department shall adopt regulations prescribing the public purposes for which a public agency may operate an unmanned aerial vehicle that is registered with the Department pursuant to this section, including, without limitation:

(a) The provision of fire services.

(b) The provision of emergency medical services.

(c) The protection of a critical facility that is public property.

(d) Search and rescue operations conducted for persons and property in distress.

5. The regulations adopted by the Department pursuant to subsection 4 must include provisions that:

(a) Authorize, as a public purpose, a public agency to operate an unmanned aerial vehicle that is registered with the Department in order to conduct a scheduled inspection to ensure compliance with building or fire codes or laws, ordinances, regulations or rules adopting or establishing building or fire codes that are enforced by the public agency.

(b) Prohibit a public agency from collecting any photograph, image or recording through the operation of an unmanned aerial vehicle during a scheduled inspection described in paragraph (a). If any photograph, image or recording is collected in violation of such a regulation or if any other information is collected through the operation of an unmanned aerial vehicle during such a scheduled inspection, the photograph, image, recording or other information:

(1) Is not admissible and must not be disclosed in any judicial, administrative or other adjudicatory proceeding other than a proceeding relating to the purpose of the scheduled inspection; and

(2) May not be used to establish reasonable suspicion or probable cause as the basis for the investigation or prosecution of a crime or other offense.

6. In addition to the regulations adopted pursuant to subsection 4, the Department shall adopt regulations to establish:

(a) A list of countries, businesses and entities from which a public agency or law enforcement agency shall not purchase or

acquire any unmanned aerial vehicle or other equipment or service relating to the operation of an unmanned aerial vehicle; and

(b) A list of unmanned aerial vehicles and other related equipment or services that a public agency or law enforcement agency shall not operate, purchase or acquire.

7. The lists established pursuant to subsection 6 must include, without limitation:

(a) Any country, business or entity identified by the Secretary of Defense of the United States Department of Defense pursuant to Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116-283, any amendments thereto or any subsequent federal law establishing such a list;

(b) Any unmanned aerial vehicle or other equipment or service relating to the operation of an unmanned aerial vehicle sold, manufactured or distributed by an entity identified by the Secretary of Defense of the United States Department of Defense pursuant to Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116-283, any amendments thereto or any subsequent federal law establishing such a list;

(c) Any hardware, software, vendor or service prohibited from being used by a state agency in Nevada by a regulation, guideline or policy adopted by the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor pursuant to NRS 242.111 and 242.115; and

(d) Any other unmanned aerial vehicle or other equipment or service relating to the operation of an unmanned aerial vehicle, as determined by the Department.

Sec. 28. NRS 603A.210 is hereby amended to read as follows:

603A.210 1. A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

2. If a data collector is a governmental agency and maintains records which contain personal information of a resident of this State, the data collector shall, to the extent practicable, with respect to the collection, dissemination and maintenance of those records, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the National Institute of

Standards and Technology of the United States Department of Commerce.

3. A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

4. If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a resident of this State which are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this section.

5. The Office of Information Security of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor shall create, maintain and make available to the public a list of controls and standards with which the State is required to comply pursuant to any federal law, regulation or framework that also satisfy the controls and standards set forth in subsection 2.

Sec. 29. NRS 603A.215 is hereby amended to read as follows:

603A.215 1. If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its successor organization.

2. A data collector doing business in this State to whom subsection 1 does not apply shall not:

(a) Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission; or

(b) Move any data storage device containing personal information beyond the logical or physical controls of the data collector, its data storage contractor or, if the data storage device is used by or is a component of a multifunctional device, a person who assumes the obligation of the data collector to protect personal

information, unless the data collector uses encryption to ensure the security of the information.

3. A data collector shall not be liable for damages for a breach of the security of the system data if:

(a) The data collector is in compliance with this section; and

(b) The breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents.

4. The requirements of this section do not apply to:

(a) A telecommunication provider acting solely in the role of conveying the communications of other persons, regardless of the mode of conveyance used, including, without limitation:

(1) Optical, wire line and wireless facilities;

(2) Analog transmission; and

(3) Digital subscriber line transmission, voice over Internet protocol and other digital transmission technology.

(b) Data transmission over a secure, private communication channel for:

(1) Approval or processing of negotiable instruments, electronic fund transfers or similar payment methods; or

(2) Issuance of reports regarding account closures due to fraud, substantial overdrafts, abuse of automatic teller machines or related information regarding a customer.

5. As used in this section:

(a) "Data storage device" means any device that stores information or data from any electronic or optical medium, including, but not limited to, computers, cellular telephones, magnetic tape, electronic computer drives and optical computer drives, and the medium itself.

(b) "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using:

(1) An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data;

(2) Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology; and

(3) Any other technology or method identified by the Office of Information Security of the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor in regulations adopted pursuant to NRS 603A.217.

(c) "Facsimile" means an electronic transmission between two dedicated fax machines using Group 3 or Group 4 digital formats that conform to the International Telecommunications Union T.4 or T.38 standards or computer modems that conform to the International Telecommunications Union T.31 or T.32 standards. The term does not include onward transmission to a third device after protocol conversion, including, but not limited to, any data storage device.

(d) "Multifunctional device" means a machine that incorporates the functionality of devices, which may include, without limitation, a printer, copier, scanner, facsimile machine or electronic mail terminal, to provide for the centralized management, distribution or production of documents.

(e) "Payment card" has the meaning ascribed to it in NRS 205.602.

(f) "Telecommunication provider" has the meaning ascribed to it in NRS 704.027.

Sec. 30. NRS 603A.217 is hereby amended to read as follows:

603A.217 Upon receipt of a well-founded petition, the ***Governor's Technology*** Office ~~[of the Chief Information Officer]~~ within the Office of the Governor may, pursuant to chapter 233B of NRS, adopt regulations which identify alternative methods or technologies which may be used to encrypt data pursuant to NRS 603A.215.

Sec. 31. Notwithstanding any provision of law to the contrary, a person who has been appointed to or is otherwise incumbent in the position of Deputy Chief of the Office of Information Security as of July 1, 2025, is in the classified service of the State and must remain in the classified service of the State until he or she vacates the position.

Sec. 32. The Legislative Counsel shall:

1. In preparing the reprint and supplements to the Nevada Revised Statutes, appropriately change any references to an officer, agency or other entity whose name is changed or whose responsibilities are transferred pursuant to the provisions of this act to refer to the appropriate officer, agency or other entity.

2. In preparing supplements to the Nevada Administrative Code, appropriately change any references to an officer, agency or other entity whose name is changed or whose responsibilities are

transferred pursuant to the provisions of this act to refer to the appropriate officer, agency or other entity.

Sec. 33. 1. Any administrative regulations adopted by an officer or an agency whose name has been changed or whose responsibilities have been transferred pursuant to the provisions of this act to another officer or agency remain in force until amended by the officer or agency to which the responsibility for the adoption of the regulations has been transferred.

2. Any contracts or other agreements entered into by an officer or agency whose name has been changed or whose responsibilities have been transferred pursuant to the provisions of this act to another officer or agency are binding upon the officer or agency to which the responsibility for the administration of the provisions of the contract or other agreement has been transferred. Such contracts and other agreements may be enforced by the officer or agency to which the responsibility for the enforcement of the provisions of the contract or other agreement has been transferred.

3. Any action taken by an officer or agency whose name has been changed or whose responsibilities have been transferred pursuant to the provisions of this act to another officer or agency remains in effect as if taken by the officer or agency to which the responsibility for the enforcement of such actions has been transferred.

Sec. 34. NRS 233F.015, 233F.055, 233F.059, 242.013, 242.031 and 242.045 are hereby repealed.

Sec. 35. This act becomes effective on July 1, 2025.

20 ~~~~~ 25