ASSEMBLY BILL NO. 1–SELECT COMMITTEE
ON HEALTH AND WELLNESS

PREFILED NOVEMBER 12, 2025

Referred to Select Committee on Health and Wellness

SUMMARY—Revises provisions relating to governmental administration. (BDR 19-22)

FISCAL NOTE: Effect on Local Government: May have Fiscal Impact.
Effect on the State: Contains Appropriation not included in Executive Budget.

~

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

AN ACT relating to governmental administration; creating and setting forth the duties of the Security Operations Center within the Office of Information Security and Cyber Defense within the Governor's Technology Office within the Office of the Governor; creating the Account for the Security Operations Center and prescribing the use of money in the Account; requiring the Security Operations Center to prepare an annual report that assesses the effectiveness of the Security Operations Center; requiring the Security Operations Center, to the extent funding is available, to develop the Cybersecurity Talent Pipeline Program; revising the purpose of the Governor's Technology Office; authorizing the board of trustees of a school district to use the services and equipment of the Governor's Technology Office; making various other changes relating to the cybersecurity of governmental entities; making appropriations; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law provides that the Governor's Technology Office within the Office of the Governor 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 Cyber Defense; and (6) certain other units, groups, divisions or departments deemed necessary by the Chief Information

Officer. (NRS 242.080) **Section 13** of this bill creates the Security Operations Center in the Office of Information Security and Cyber Defense.

Existing law: (1) requires the Governor's Technology Office to provide certain state agencies and elected officers with all their required design of information systems; (2) authorizes certain other state agencies to negotiate with the Office for its services or the use of its equipment; and (3) authorizes, upon request, the Office to provide certain services to state agencies not under the control of the Governor and local governmental agencies. (NRS 242.131, 242.141) **Section 16** of this bill requires the Security Operations Center to provide each state agency and elected state officers with cybersecurity services, including real-time monitoring of cyberinfrastructure, threat mitigation, incident response and cybersecurity enforcement. **Sections 16 and 30** of this bill reorganize provisions that authorize certain state agencies and local governmental agencies to use the equipment and services of the Governor's Technology Office. **Section 16** also requires any local governmental agency which has agreed to use the equipment or services of the Governor's Technology Office to apply to the Chief to withdraw from such use. **Section 10** of this bill revises the definition of "local governmental agency" to include the board of trustees of a school district, which has the effect of authorizing the board of trustees of a school district to use the services of the Governor's Technology Office pursuant to **section 16**. **Section 11** of this bill amends the definition of "using agency" so that the term includes any state agency, elected state officer or local governmental agency that uses the services or equipment of the Office.

Section 2 of this bill requires the Security Operations Center to develop certain policies and procedures to: (1) combat the increasing threats to using agencies posed by cybercriminals; (2) protect sensitive data in the possession of a using agency; and (3) ensure a coordinated and rapid response to any cybersecurity incident that affects a using agency. **Section 3** of this bill provides that if a using agency does not comply with the cybersecurity policies and protocols developed by the Security Operations Center, the Chief may impose additional oversight or audit requirements on the using agency relating to cybersecurity.

Section 4 of this bill creates the Account for the Security Operations Center in the State General Fund to be administered by the Chief. **Section 4** requires the money in the Account to be used for the purposes of supporting and carrying out the duties of the Security Operations Center. **Section 4** also authorizes the Security Operations Center to serve as a fiscal agent to pool federal grant funds for the purposes of cybersecurity support and infrastructure development.

Section 5 of this bill requires the Security Operations Center to collaborate with the Office of Information Security and Cyber Defense to enhance communication and coordination of incident responses to cyber threats or cyberattacks on information systems.

Section 6 of this bill requires the Security Operations Center to prepare and submit an annual report to the Governor, Attorney General and the Director of the Legislative Counsel Bureau for transmission to the Legislature that includes certain information relating to the duties of the Security Operations Center.

Section 7 of this bill provides that the provisions of the Nevada Revised Statutes relating to information services do not impair or affect existing agreements with a federally recognized Indian tribe and that any interlocal agreement entered into must respect the sovereign governance of the tribe and provide for jointly agreed upon data protocols.

To the extent that funding is available, **section 8** of this bill requires the Security Operations Center, in collaboration with the Nevada System of Higher Education, to develop the Cybersecurity Talent Pipeline Program.

Section 9 of this bill amends the definition of "information service," as provided by the Office to a using agency, to include the real-time monitoring of

cyberinfrastructure, threat mitigation, incident response and cybersecurity enforcement.

Existing law makes certain legislative determinations and declarations relating to the purpose of the Governor's Technology Office. (NRS 242.071) **Section 12** of this bill revises these determinations and declarations to include performing information services for using agencies.

Existing law provides that certain documents assembled, maintained, overseen or prepared by the Governor's Technology Office to mitigate, prevent or respond to acts of terrorism are confidential. (NRS 242.105) **Section 14** of this bill provides that certain documents relating to the cybersecurity of a using agency are also confidential.

Existing law requires the Chief to adopt certain regulations relating to information systems of certain state agencies. (NRS 242.111) **Section 15** of this bill instead requires the Chief to adopt certain regulations relating to information systems of using agencies.

Existing law requires the Chief to advise using agencies regarding the policy for information services of the Executive Branch of Government. (NRS 242.151) **Section 17** of this bill requires the Chief to instead advise the using agencies of the policy for information services of the Governor's Technology Office.

Existing law provides that all equipment of an agency or elected state officer which is owned or leased by the State must be under the managerial control of the Office. (NRS 242.161) **Section 18** of this bill: (1) provides instead that all equipment of a using agency which is owned or leased by the State must be under the managerial control of the Office; (2) prohibits the Security Operations Center from assuming operational control of the equipment or software systems of a using agency; and (3) requires the Security Operations Center to provide to a using agency standards and policies for the equipment or software systems to be deployed by the Security Operations Center, which must be agreed upon in writing before the Security Operations Center provides services.

Section 19 of this bill provides that the Office is responsible for any application of an information system which it furnishes to using agencies.

Section 20 of this bill requires: (1) any using agency which uses the equipment or services of the Office to adhere to the regulations, standards, practices, policies and conventions of the Office; and (2) each using agency to report certain information relating to certain suspected incidents to the Office of Information Security and Cyber Defense and the Security Operations Center.

Existing law requires the Deputy Director of the Office of Information Security and Cyber Defense to 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. (NRS 242.183) **Section 21** of this bill requires instead that the Deputy Director, in consultation with the Security Operations Center, investigate and resolve any breach of an information system of a using agency.

Existing law authorizes the Governor to proclaim the existence of a state of emergency or a declaration of disaster if the Governor in his or her proclamation finds that certain events, including a technological or man-made emergency or disaster of major proportions, have actually occurred in this State and that the safety and welfare of the inhabitants of this State require such a proclamation. (NRS 414.070) If the Governor has made such a proclamation concerning a critical cybersecurity incident, **section 21** authorizes the Governor to authorize the information technology personnel of using agencies of the Executive Branch to report directly to the Chief.

Existing law provides that the amount receivable from a state agency or officer or local governmental agency which uses the services of the Governor's Technology Office must be determined by the Chief. (NRS 242.191) **Section 22** of

this bill provides instead that the amount receivable from a using agency which uses the services or equipment of the Office must be determined by the Chief.

Section 23 of this bill requires each using agency using the services or equipment of the Office to pay a fee for such use to the Fund for Information Services.

Section 24 of this bill makes an appropriation to the Office of Finance in the Office of the Governor for the Governor's Technology Office within the Office of the Governor for investments related to cybersecurity. **Sections 25-27** of this bill make appropriations to the Office of Finance in the Office of the Governor for a loan to the Governor's Technology Office within the Office of the Governor to cover a shortfall in revenues for certain divisions and offices within the Governor's Technology Office.

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

Section 1. Chapter 242 of NRS is hereby amended by adding thereto the provisions set forth as sections 2 to 8, inclusive, of this act.

Sec. 2. ***1. The Security Operations Center shall develop policies and procedures to:***

(a) Combat the increasing threats to using agencies posed by cybercriminals;

(b) Protect sensitive data in the possession of a using agency; and

(c) Ensure a coordinated and rapid response to any cybersecurity incident that affects a using agency.

2. The policies and procedures developed pursuant to subsection 1 must include, without limitation:

(a) A requirement that a using agency notify the Security Operations Center of any specific or immediate threat to the cybersecurity of an information system operated or maintained by the using agency;

(b) A requirement that the Security Operations Center notify the appropriate law enforcement agency and prosecuting attorney and any other appropriate public or private entity of any specific threat to the cybersecurity of an information system of which the Security Operations Center has been notified;

(c) A strategy for developing ongoing programs for professional development in cybersecurity for the employees of a using agency; and

(d) The use of security orchestration automation and response systems to automate repetitive tasks, enhance operational efficiency and standardize procedures and responses for the various information technology support of using agencies.

Sec. 3. *If a using agency does not comply with the cybersecurity policies and protocols developed by the Security Operations Center pursuant to section 2 of this act, the Chief may impose additional oversight or audit requirements on the using agency relating to cybersecurity.*

Sec. 4. *1. The Account for the Security Operations Center is hereby created in the State General Fund. The Chief must administer the Account.*

2. The money in the Account must only be used for the purposes of supporting and carrying out the duties of the Security Operations Center.

3. The Chief may apply for and accept federal grants for the purposes of this section.

4. The Security Operations Center may serve as a fiscal agent to pool federal grant funds for the purposes of cybersecurity support and infrastructure development. The Security Operations Center may establish criteria for using agencies to access shared resources which must ensure equitable distribution of the resources and maximize competiveness for federal opportunities.

5. All interest earned on the money in the Account, after deducting any applicable charges, must be credited to the Account.

6. All claims against the Account must be paid as other claims against the State are paid.

7. Any money remaining in the Account at the end of a fiscal year does not revert to the State General Fund and must be carried forward to the next fiscal year.

Sec. 5. *The Security Operations Center shall collaborate with the Office of Information Security and Cyber Defense created by NRS 242.080 to enhance communication and coordination of incident responses to cyber threats or cyberattacks on information systems and to provide each using agency information relating to emerging cyber threats and best practices for cybersecurity.*

Sec. 6. *1. On or before January 1 of each year, the Security Operations Center shall prepare a report assessing the effectiveness of the Security Operations Center relating to its duties. The report must include, without limitation:*

(a) A summary of the progress made by the Security Operations Center during the immediately preceding year in performing its duties and exercising such powers as are conferred upon it;

(b) A general description of any threats or attacks responded to by the Security Operations Center during the immediately preceding year, and a summary of the response to the threat;

(c) A summary of the goals and objectives of the Security Operations Center for the upcoming year;

(d) A summary of any issues presenting challenges to the Security Operations Center; and

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

2. The report required pursuant to subsection 1 must be submitted not later than July 1 of each year to the Governor, Attorney General and Director of the Legislative Counsel Bureau for transmission to the Legislature.

Sec. 7. ***Nothing in this chapter shall be construed to impair or affect existing agreements with a federally recognized Indian tribe. Any interlocal agreement entered into with the governing body of an Indian tribe, group of tribes, organized segment of a tribe or any organization representing two or more such entities must respect sovereign governance and provide for jointly agreed upon data protocols.***

Sec. 8. ***To the extent that funding is available:***

1. The Security Operations Center shall, in collaboration with the Nevada System of Higher Education, develop the Cybersecurity Talent Pipeline Program. The Program must develop a system for the career development of students in the field of computer science or cybersecurity.

2. The Program must provide opportunities for students within the Nevada System of Higher Education who are majoring in a field related to cybersecurity to obtain working experience in the Security Operations Center.

Sec. 9. NRS 242.055 is hereby amended to read as follows:

242.055 "Information service" means any service ***provided by the Office to a using agency*** relating to the creation, maintenance, operation, security validation, testing, continuous monitoring or use of an information system. ***The term includes, without limitation, the real-time monitoring of cyberinfrastructure, threat mitigation, incident response and cybersecurity enforcement.***

Sec. 10. NRS 242.061 is hereby amended to read as follows:

242.061 "Local governmental agency" means ~~[any]~~ ***:***

1. Any branch, agency, bureau, board, commission, department or division of a county, incorporated city or town in this State ~~[.]~~ ***; or***

2. The board of trustees of a school district.

Sec. 11. NRS 242.068 is hereby amended to read as follows:

242.068 "Using agency" means ~~[an agency of the State which has a function requiring the use of information technology, information services or an information system.]~~ ***:***

1. A state agency or elected state officer who is required to use the services and equipment of the Office pursuant to subsection 1 of NRS 242.131.

2. Any other state agency or local governmental agency that has negotiated with the Office for its services or equipment pursuant to subsection 2 of NRS 242.131.

Sec. 12. 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 within the Office of the Governor is necessary for the ***secure,*** coordinated, orderly and economical processing of data and information in State Government, to ensure ***the secure and*** 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]~~ ***using*** agencies.

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

Sec. 13. NRS 242.080 is hereby amended to read as follows:

242.080 1. The Governor's Technology Office is hereby created within the Office of the Governor.

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

(a) The Director's Office. The Chief is the head of the Director's Office.

(b) The Client Services Division.

(c) The Computing Services Division.

(d) The Network Services Division.

(e) The Office of Information Security and Cyber Defense.

(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 Unit and a Unified Communications Unit are hereby created within the Network Services Division of the Office.

4. The Security Operations Center is hereby created within the Office of Information Security and Cyber Defense.

Sec. 14. NRS 242.105 is hereby amended to read as follows:

242.105 1. Except as otherwise provided in subsection 3, records and portions of records that are assembled, maintained, overseen or prepared by the Office to mitigate, prevent or respond to ***cybersecurity incidents or*** acts of terrorism, the public disclosure of which would, in the determination of the Chief, create a substantial likelihood of threatening the ***cybersecurity of a using agency or the*** safety of the general public are confidential and not subject to inspection by the general public to the extent that such records and portions of records consist of or include:

(a) Information regarding the infrastructure and security of information systems, including, without limitation:

(1) Access codes, passwords and programs used to ensure the security of an information system;

(2) Access codes used to ensure the security of software applications;

(3) Procedures and processes used to ensure the security of an information system; and

(4) Plans used to re-establish security and service with respect to an information system after security has been breached or service has been interrupted.

(b) Assessments and plans that relate specifically and uniquely to the vulnerability of an information system or to the measures which will be taken to respond to such vulnerability, including, without limitation, any compiled underlying data necessary to prepare such assessments and plans.

(c) The results of tests of the security of an information system, insofar as those results reveal specific vulnerabilities relative to the information system.

2. The Chief shall maintain or cause to be maintained a list of each record or portion of a record that the Chief has determined to be confidential pursuant to subsection 1. The list described in this subsection must be prepared and maintained so as to recognize the existence of each such record or portion of a record without revealing the contents thereof.

3. At least once each biennium, the Chief shall review the list described in subsection 2 and shall, with respect to each record or portion of a record that the Chief has determined to be confidential pursuant to subsection 1:

(a) Determine that the record or portion of a record remains confidential in accordance with the criteria set forth in subsection 1;

(b) Determine that the record or portion of a record is no longer confidential in accordance with the criteria set forth in subsection 1; or

(c) If the Chief determines that the record or portion of a record is obsolete, cause the record or portion of a record to be disposed of in the manner described in NRS 239.073 to 239.125, inclusive.

4. On or before February 15 of each year, the Chief shall:

(a) Prepare a report setting forth a detailed description of each record or portion of a record determined to be confidential pursuant to this section, if any, accompanied by an explanation of why each such record or portion of a record was determined to be confidential; and

(b) Submit a copy of the report to the Director of the Legislative Counsel Bureau for transmittal to:

(1) If the Legislature is in session, the standing committees of the Legislature which have jurisdiction of the subject matter; or

(2) If the Legislature is not in session, the Legislative Commission.

5. As used in this section, "act of terrorism" has the meaning ascribed to it in NRS 239C.030.

Sec. 15. NRS 242.111 is hereby amended to read as follows:

242.111 The Chief shall adopt regulations necessary for the administration of this chapter, including:

1. The policy for the information systems of ~~[the Executive Branch of Government, excluding the Nevada System of Higher Education and the Nevada Criminal Justice Information System,]~~ ***using agencies,*** as that policy relates, but is not limited, to such items as standards for systems and programming and criteria for selection, location and use of information systems to meet the requirements of ~~[state]~~ ***using*** agencies and officers ~~[at]~~ ***in*** the ~~[least cost to]~~ ***best interests of*** the State ~~[;]~~ ***and using agencies;***

2. The procedures of the Office in providing information services, which may include provision for the performance, by ~~[an]~~ ***a using*** agency which uses the services or equipment of the Office, of preliminary procedures, such as data recording and verification, within the ***using*** agency;

3. The effective administration of the Office, including, without limitation, security to prevent unauthorized access to information systems and plans for the recovery of systems and applications after they have been disrupted;

4. The development of standards to ensure the security of the information systems of the ~~[Executive Branch of Government;]~~ ***using agencies;***

5. Specifications and standards for the employment of all personnel of the Office; and

6. The policies and procedures necessary to coordinate the cybersecurity activities of state agencies and local governments.

Sec. 16. NRS 242.131 is hereby amended to read as follows:

242.131 1. The Office shall provide state agencies and elected state officers with all their required design of information systems. ***The Security Operations Center shall provide each state agency and elected state officer with cybersecurity services, including, without limitation, real-time monitoring of cyberinfrastructure, threat mitigation, incident response and cybersecurity enforcement.*** All agencies and officers must use those services and equipment, except as otherwise provided in subsection 2.

2. The following agencies may negotiate with the Office for its services ***, including, without limitation, cybersecurity services,***

including, without limitation, real-time monitoring of cyberinfrastructure, threat mitigation, incident response and cybersecurity enforcement, or the use of its equipment, subject to the provisions of this chapter, and the Office shall provide those services and the use of that equipment as may be mutually agreed:

(a) The Court Administrator;

(b) The Department of Motor Vehicles;

(c) The Department of Public Safety;

(d) The Department of Transportation;

(e) The Employment Security Division of the Department of Employment, Training and Rehabilitation;

(f) The Department of Wildlife;

(g) The Housing Division of the Department of Business and Industry;

(h) The Legislative Counsel Bureau;

(i) The State Controller;

(j) The Nevada Gaming Control Board and Nevada Gaming Commission; ~~[and]~~

(k) The Nevada System of Higher Education ~~[.]~~ ***; and***

(l) Any local governmental agency.

3. Any state agency or elected state officer who uses the services of the Office and desires to withdraw substantially from that use must apply to the Chief for approval. The application must set forth justification for the withdrawal. If the Chief denies the application, the agency or officer must:

(a) If the Legislature is in regular or special session, obtain the approval of the Legislature by concurrent resolution.

(b) If the Legislature is not in regular or special session, obtain the approval of the Interim Finance Committee. The Chief shall, within 45 days after receipt of the application, forward the application together with his or her recommendation for approval or denial to the Interim Finance Committee. The Interim Finance Committee has 45 days after the application and recommendation are submitted to its Secretary within which to consider the application. Any application which is not considered by the Committee within the 45-day period shall be deemed approved.

4. ***Any local governmental agency which has entered into an agreement to use the equipment or services of the Office and desires to withdraw substantially from that use must apply to the Chief for approval. The application must set forth the justification for the withdrawal.***

5. If the demand for services or use of equipment exceeds the capability of the Office to provide them, the Office may contract with other agencies or independent contractors to furnish the

required services or use of equipment and is responsible for the administration of the contracts.

Sec. 17. NRS 242.151 is hereby amended to read as follows:

242.151 The Chief shall advise the using agencies regarding:

1. The policy for information services of the ~~[Executive Branch of Government,]~~ ***Office,*** as that policy relates, but is not limited, to such items as standards for systems and programming and criteria for the selection, location and use of information systems in order that the requirements of ~~[state agencies and officers]~~ ***using agencies*** may be met ~~[at the least cost to]~~ ***in the best interests of*** the State;

2. The procedures in performing information services; and

3. The effective administration and use of the computer facility, including security to prevent unauthorized access to data, information and plans for the recovery of systems and applications after they have been disrupted.

Sec. 18. NRS 242.161 is hereby amended to read as follows:

242.161 1. All equipment of ~~[an agency or elected state officer]~~ ***a using agency*** which is owned or leased by the State must be under the managerial control of the Office, except the equipment of the agencies and officers specified in subsection 2 of NRS 242.131.

2. The Office may permit ~~[an]~~ ***a using*** agency which is required to use such equipment to operate it on the ***using*** agency's premises.

3. The Security Operations Center shall not assume operational control of the equipment or software systems of a using agency. Before providing services, the Security Operations Center shall provide to the using agency standards and policies for the equipment or software systems to be deployed by the Security Operations Center, which must be agreed upon in writing.

Sec. 19. NRS 242.171 is hereby amended to read as follows:

242.171 1. The Office is responsible for:

(a) The applications of information systems;

(b) Designing and placing those information systems in operation;

(c) Any application of an information system which it furnishes to ~~[state]~~ ***using*** agencies ~~[and officers]~~ after negotiation; and

(d) The security validation, testing, including, without limitation, penetration testing, and continuous monitoring of information systems,

➥ for using agencies **.** ~~[and for state agencies and officers which use the equipment or services of the Office pursuant to subsection 2 of NRS 242.131.]~~

2. The Chief shall review and approve or disapprove, pursuant to standards for justifying cost, any application of an information

system having an estimated developmental cost of $50,000 or more. No using agency may commence development work on any such applications until approval and authorization have been obtained from the Chief.

3. As used in this section, "penetration testing" means a method of evaluating the security of an information system or application of an information system by simulating unauthorized access to the information system or application.

Sec. 20. NRS 242.181 is hereby amended to read as follows:

242.181 1. Any ~~[state agency or elected state officer]~~ ***using agency*** which uses the equipment or services of the Office shall adhere to the regulations, standards, practices, policies and conventions of the Office.

2. Each ~~[state]~~ ***using*** agency ~~[or elected state officer described in subsection 1]~~ shall report any suspected incident of:

(a) ~~[Unauthorized access to an information system or application of an information system of the Office used by the state agency or elected state officer; and]~~ ***A data breach;***

(b) ***A distributed denial of service incident;***

(c) A ransomware incident;

(d) Any other incident that disrupts the delivery or essential services for more than 1 business day or directly affects life or property; or

(e) Noncompliance with the regulations, standards, practices, policies and conventions of the Office that is identified by the Office as security-related,

➥ to the Office of Information Security and Cyber Defense of the Office ***and the Security Operations Center*** within 24 hours after discovery of the suspected incident. If the Office of Information Security and Cyber Defense ***, in consultation with the Security Operations Center,*** determines that an incident of unauthorized access or noncompliance occurred, it shall immediately report the incident to the Chief. The Chief shall assist in the investigation and resolution of any such incident.

3. ***A report submitted by a using agency pursuant to subsection 2 must contain the following information:***

(a) The date and time of the incident;

(b) The type of incident;

(c) The type of information system or data affected by the incident;

(d) The known and projected impact of the incident to the using agency;

(e) Whether law enforcement, a regulatory body or any other entity that could be affected by the incident has been notified, as applicable; and

(f) Any additional resources needed by the using agency to respond to the incident, as applicable.

4. The Chief may establish a uniform reporting system if the Office and Security Operations Center are organizationally collocated.

5. The Office shall provide services to each ~~[state]~~ ***using*** agency ~~[and elected state officer described in subsection 1]~~ uniformly with respect to degree of service, priority of service, availability of service and cost of service.

Sec. 21. NRS 242.183 is hereby amended to read as follows:

242.183 1. The Deputy Director of the Office of Information Security and Cyber Defense ***, in consultation with the Security Operations Center,*** shall investigate and resolve any breach of an information system of a ~~[state]~~ ***using*** agency ~~[or elected officer that uses the equipment or services of the Governor's Technology Office]~~ 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 Director of the Office of Information Security and Cyber Defense, at his or her discretion, may inform members of 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]~~ ***using*** 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.

3. If a state of emergency or declaration of disaster is proclaimed by the Governor pursuant to NRS 414.070 concerning a critical cybersecurity incident, the Governor may authorize the information technology personnel of using agencies of the Executive Branch to report directly to the Chief.

Sec. 22. 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]~~ ***using*** agency ~~[or officer or local governmental agency]~~ which uses the services ***or equipment*** 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 Division ~~[,]~~ ***and the cybersecurity services provided by the Security Operations Center,*** 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]~~ ***using*** agencies for which services of the Office have been performed an itemized statement of the amount receivable from each ~~[state]~~ ***using*** 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]~~ ***using*** agency ***.*** ~~[or officer or local governmental agency.]~~

Sec. 23. NRS 242.211 is hereby amended to read as follows:

242.211 1. The Fund for Information Services is hereby created as an internal service fund. Money from the Fund must be paid out on claims as other claims against the State are paid. The claims must be made in accordance with budget allotments and are subject to postaudit examination and approval.

2. All operating, maintenance, rental, repair and replacement costs of equipment and all salaries of personnel assigned to the Office must be paid from the Fund.

3. Each ***using*** agency using the services ***or equipment*** of the Office shall pay a fee for that use to the Fund, which must be set by the Chief in an amount sufficient to reimburse the Office for the entire cost of providing those services, including overhead. Each using agency shall budget for those services. All fees, proceeds from the sale of equipment and any other money received by the Office must be deposited with the State Treasurer for credit to the Fund.

Sec. 24. 1. There is hereby appropriated from the State General Fund to the Office of Finance in the Office of the Governor for the Governor's Technology Office within the Office of the Governor for investments related to cybersecurity the following sums:

For the Fiscal Year 2025-2026 ..... $6,573,067

For the Fiscal Year 2026-2027 ..... $3,420,682

2. Any balance of the sums appropriated by subsection 1 remaining at the end of the respective fiscal years must not be committed for expenditure after June 30 of the respective fiscal years by the entity to which the appropriation is made or any entity to which money from the appropriation is granted or otherwise transferred in any manner, and any portion of the appropriated money remaining must not be spent for any purpose after September 18, 2026, and September 17, 2027, respectively, by either the entity to which the money was appropriated or the entity

to which the money was subsequently granted or transferred, and must be reverted to the State General Fund on or before September 18, 2026, and September 17, 2027, respectively.

Sec. 25. 1. There is hereby appropriated from the State General Fund to the Office of Finance in the Office of the Governor for a loan to the Governor's Technology Office within the Office of the Governor to cover a shortfall in revenues for the Client Services Division within the Governor's Technology Office the following sums:

For the Fiscal Year 2025-2026 ..... $1,005,840

For the Fiscal Year 2026-2027 ..... $1,359,317

2. The amounts appropriated by subsection 1 are loans. Commencing on July 1, 2027, the Chief Information Officer shall use revenues from intergovernmental transfers to repay the loan in annual installments to the State Treasurer for deposit in the State General Fund. Each annual installment must be 25 percent of the loan, and the loan must be fully repaid not later than the end of Fiscal Year 2030-2031.

3. Any balance of the sums appropriated by subsection 1 remaining at the end of the respective fiscal years must not be committed for expenditure after June 30 of the respective fiscal years by the entity to which the appropriation is made or any entity to which money from the appropriation is granted or otherwise transferred in any manner, and any portion of the appropriated money remaining must not be spent for any purpose after September 18, 2026, and September 17, 2027, respectively, by either the entity to which the money was appropriated or the entity to which the money was subsequently granted or transferred, and must be reverted to the State General Fund on or before September 18, 2026, and September 17, 2027, respectively.

Sec. 26. 1. There is hereby appropriated from the State General Fund to the Office of Finance in the Office of the Governor for a loan to the Governor's Technology Office within the Office of the Governor to cover a shortfall in revenues for the Computing Services Division within the Governor's Technology Office the following sums:

For the Fiscal Year 2025-2026 ..... $1,063,637

For the Fiscal Year 2026-2027 ..... $1,063,637

2. The amounts appropriated by subsection 1 are loans. Commencing on July 1, 2027, the Chief Information Officer shall use revenues from intergovernmental transfers to repay the loan in annual installments to the State Treasurer for deposit in the State General Fund. Each annual installment must be 25 percent of the loan, and the loan must be fully repaid not later than the end of Fiscal Year 2030-2031.

3. Any balance of the sums appropriated by subsection 1 remaining at the end of the respective fiscal years must not be committed for expenditure after June 30 of the respective fiscal years by the entity to which the appropriation is made or any entity to which money from the appropriation is granted or otherwise transferred in any manner, and any portion of the appropriated money remaining must not be spent for any purpose after September 18, 2026, and September 17, 2027, respectively, by either the entity to which the money was appropriated or the entity to which the money was subsequently granted or transferred, and must be reverted to the State General Fund on or before September 18, 2026, and September 17, 2027, respectively.

Sec. 27. 1. There is hereby appropriated from the State General Fund to the Office of Finance in the Office of the Governor for a loan to the Governor's Technology Office within the Office of the Governor to cover a shortfall in revenues for the Office of Information Security and Cyber Defense within the Governor's Technology Office the following sums:

For the Fiscal Year 2025-2026 ..... $184,018

For the Fiscal Year 2026-2027 ..... $70,431

2. The amounts appropriated by subsection 1 are loans. Commencing on July 1, 2027, the Chief Information Officer shall use revenues from intergovernmental transfers to repay the loan in annual installments to the State Treasurer for deposit in the State General Fund. Each annual installment must be 25 percent of the loan, and the loan must be fully repaid not later than the end of Fiscal Year 2030-2031.

3. Any balance of the sums appropriated by subsection 1 remaining at the end of the respective fiscal years must not be committed for expenditure after June 30 of the respective fiscal years by the entity to which the appropriation is made or any entity to which money from the appropriation is granted or otherwise transferred in any manner, and any portion of the appropriated money remaining must not be spent for any purpose after September 18, 2026, and September 17, 2027, respectively, by either the entity to which the money was appropriated or the entity to which the money was subsequently granted or transferred, and must be reverted to the State General Fund on or before September 18, 2026, and September 17, 2027, respectively.

Sec. 28. The provisions 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. 29. Notwithstanding the provisions of NRS 218D.430 and 218D.435, a committee may vote on this act before the expiration of the period prescribed for the return of a fiscal note in

NRS 218D.475. This section applies retroactively from and after November 13, 2025.

Sec. 30. NRS 242.141 is hereby repealed.

Sec. 31. This act becomes effective upon passage and approval.

TEXT OF REPEALED SECTION

242.141 Services provided for agencies not under Governor's control and local governmental agencies. To facilitate the economical processing of data or information throughout the State Government, the Office may provide service for agencies not under the control of the Governor, upon the request of any such agency. The Office may provide services, including, without limitation, purchasing services, to a local governmental agency upon request, if provision of such services will result in reduced costs to the State for equipment and services.

㉚