By Senator Harrell

31-00757A-25 2025770__

A bill to be entitled

An act relating to cybersecurity; amending s. 110.205, F.S.; exempting the state chief technology officer from the Career Service System; amending s. 282.0041, F.S.; revising definitions of the terms "data" and "open data"; defining the terms "enterprise digital data"; amending s. 282.0051, F.S.; revising the purpose of the Florida Digital Service; revising the timeframes for the Florida Digital Service to issue certain reports to the Governor and the Legislature; requiring that, by a specified date, an annual report on specified alternative standards be provided to the Governor and the Legislature; requiring the Florida Digital Service to support state agencies with the use of electronic credentials in compliance with specified standards; requiring the state chief information officer, in consultation with the Secretary of Management Services, to designate a state chief technology officer; providing requirements for such position; providing the responsibilities of the state chief technology officer; amending s. 282.318, F.S.; revising the standards and processes for assessing state agency cybersecurity risks of the Department of Management Services, acting through the Florida Digital Service; requiring state agencies to report all ransomware and cybersecurity incidents to the Cybersecurity Operations Center and the Cybercrime Office; requiring the Cybersecurity Operations Center to notify the state chief information officer and the

state chief information security officer immediately of a reported incident; requiring the state chief information officer, in consultation with the state chief information security officer, to notify the Legislature of certain reported incidents within a specified timeframe; revising the timeframe during which the Cybersecurity Operations Center is required to provide a consolidated incident report to the Governor, the Legislature, and the Florida Cybersecurity Advisory Council; revising the name of an Emergency Support Function from ESF-Cyber to ESF-20; revising the specified date by which a state agency head must designate an information security manager; requiring that the agency strategic cybersecurity plan take the statewide cybersecurity strategic plan into consideration; requiring that such agency operational cybersecurity program include a certain set of measures for a specified purpose; requiring agency heads to require that enterprise digital data be maintained in accordance with specified provisions; providing construction; authorizing designated members of the Legislature and designated members of legislative staff to attend portions of meetings where material exempt from public disclosure is discussed, under certain circumstances; amending s. 282.3185, F.S.; revising the timeframes in which a local government must report a discovery of all ransomware incidents and certain cybersecurity incidents; requiring the Cybersecurity Operations

Center to notify immediately the state chief information officer and the state chief information security officer of a reported incident; requiring the state chief information officer, in consultation with the state chief information security officer, to notify the Legislature of incidents of certain severity levels within a specified timeframe; revising the timeframe during which the Cybersecurity Operations Center is required to provide a quarterly consolidated incident report to the Legislature and the Florida Cybersecurity Advisory Council; amending s. 282.319, F.S.; revising the membership of the Florida Cybersecurity Advisory Council; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Paragraph (e) of subsection (2) of section 110.205, Florida Statutes, is amended to read:

110.205 Career service; exemptions.—

(2) EXEMPT POSITIONS.—The exempt positions that are not covered by this part include the following:

(e) The state chief information officer, the state chief data officer, the state chief technology officer, and the state chief information security officer. The Department of Management Services shall set the salary and benefits of these positions in accordance with the rules of the Senior Management Service.

Section 2. Present subsections (17) through (38) of section 282.0041, Florida Statutes, are redesignated as subsections (18)

through (39), respectively, a new subsection (17) is added to that section, and subsection (9) and present subsection (24) of that section are amended, to read:

282.0041 Definitions.—As used in this chapter, the term:

(9) "Data" means information in a specific representation, usually a sequence of symbols that have meaning. The term includes, but is not limited to, numbers, text, images, audio, and video. The term also includes raw material that is processed and interpreted to gain insights and make decisions ~~a subset of structured information in a format that allows such information to be electronically retrieved and transmitted~~.

(17) "Enterprise digital data" means information in electronic form which is deemed to be data owned by a state agency and held for state purposes by the state agency. For the purposes of this subsection, the term "state agency" includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

(25)~~(24)~~ "Open data" is a subset of "data" and means data collected or created by a state agency, the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services, and structured in a way that enables the data to be fully discoverable and usable by the public. The term does not include data that are restricted from public disclosure based on federal or state laws and regulations, including, but not limited to, those related to privacy, confidentiality, security, personal health, business or trade secret information, and exemptions from state public records laws; or data for which a state agency, the Department of Legal Affairs, the Department of Financial Services, or the

Department of Agriculture and Consumer Services is statutorily authorized to assess a fee for its distribution.

Section 3. Subsection (1) of section 282.0051, Florida Statutes, is amended, and paragraph (c) is added to subsection (2) of that section, to read:

282.0051 Department of Management Services; Florida Digital Service; powers, duties, and functions.—

(1) The Florida Digital Service is established ~~has been created~~ within the department to lead the creation of enterprise information technology and cybersecurity standards, to propose and evaluate innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support the cloud-first policy as specified in s. 282.206. The department, through the Florida Digital Service, shall have the following powers, duties, and functions:

(a) Develop and publish information technology policy for the management of the state's information technology resources.

(b) Develop an enterprise architecture that:

1. Acknowledges the unique needs of the entities within the enterprise in the development and publication of standards and terminologies to facilitate digital interoperability;

2. Supports the cloud-first policy as specified in s. 282.206; and

3. Addresses how information technology infrastructure may be modernized to achieve cloud-first objectives.

(c) Establish project management and oversight standards with which state agencies must comply when implementing

information technology projects. The department, acting through the Florida Digital Service, shall provide training opportunities to state agencies to assist in the adoption of the project management and oversight standards. To support data-driven decisionmaking, the standards must include, but are not limited to:

1. Performance measurements and metrics that objectively reflect the status of an information technology project based on a defined and documented project scope, cost, and schedule.

2. Methodologies for calculating acceptable variances in the projected versus actual scope, schedule, or cost of an information technology project.

3. Reporting requirements, including requirements designed to alert all defined stakeholders that an information technology project has exceeded acceptable variances defined and documented in a project plan.

4. Content, format, and frequency of project updates.

5. Technical standards to ensure an information technology project complies with the enterprise architecture.

(d) Perform project oversight on all state agency information technology projects that have total project costs of $10 million or more and that are funded in the General Appropriations Act or any other law. The department, acting through the Florida Digital Service, shall report, by the 30th day after the end of each quarter, ~~at least quarterly~~ to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department identifies as high-risk due to the project exceeding acceptable variance

ranges defined and documented in a project plan. The report must include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project, and a recommendation for corrective actions required, including suspension or termination of the project.

(e) Identify opportunities for standardization and consolidation of information technology services that support interoperability and the cloud-first policy, as specified in s. 282.206, and business functions and operations, including administrative functions such as purchasing, accounting and reporting, cash management, and personnel, and that are common across state agencies. The department, acting through the Florida Digital Service, shall biennially on January 31 ~~1~~ of each even-numbered year provide recommendations for standardization and consolidation to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(f) Establish best practices for the procurement of information technology products and cloud-computing services in order to reduce costs, increase the quality of data center services, or improve government services.

(g) Develop standards for information technology reports and updates, including, but not limited to, operational work plans, project spend plans, and project status reports, for use by state agencies.

(h) Upon request, assist state agencies in the development of information technology-related legislative budget requests.

(i) Conduct annual assessments of state agencies to determine compliance with all information technology standards

and guidelines developed and published by the department and provide results of the assessments to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(j) Conduct a market analysis not less frequently than every 3 years beginning in 2021 to determine whether the information technology resources within the enterprise are utilized in the most cost-effective and cost-efficient manner, while recognizing that the replacement of certain legacy information technology systems within the enterprise may be cost prohibitive or cost inefficient due to the remaining useful life of those resources; whether the enterprise is complying with the cloud-first policy specified in s. 282.206; and whether the enterprise is utilizing best practices with respect to information technology, information services, and the acquisition of emerging technologies and information services. Each market analysis shall be used to prepare a strategic plan for continued and future information technology and information services for the enterprise, including, but not limited to, proposed acquisition of new services or technologies and approaches to the implementation of any new services or technologies. Copies of each market analysis and accompanying strategic plan must be submitted to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives not later than December 31 of each year that a market analysis is conducted.

(k) Recommend other information technology services that should be designed, delivered, and managed as enterprise information technology services. Recommendations must include

the identification of existing information technology resources associated with the services, if existing services must be transferred as a result of being delivered and managed as enterprise information technology services.

(l) In consultation with state agencies, propose a methodology and approach for identifying and collecting both current and planned information technology expenditure data at the state agency level.

(m)1. Notwithstanding any other law, provide project oversight on any information technology project of the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services which has a total project cost of $20 million or more. Such information technology projects must also comply with the applicable information technology architecture, project management and oversight, and reporting standards established by the department, acting through the Florida Digital Service.

2. When performing the project oversight function specified in subparagraph 1., report, by the 30th day after the end of each quarter, ~~at least quarterly~~ to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department, acting through the Florida Digital Service, identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in the project plan. The report shall include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project and a recommendation for corrective actions required, including suspension or termination of the project.

(n) If an information technology project implemented by a state agency must be connected to or otherwise accommodated by an information technology system administered by the Department of Financial Services, the Department of Legal Affairs, or the Department of Agriculture and Consumer Services, consult with these departments regarding the risks and other effects of such projects on their information technology systems and work cooperatively with these departments regarding the connections, interfaces, timing, or accommodations required to implement such projects.

(o) If adherence to standards or policies adopted by or established pursuant to this section causes conflict with federal regulations or requirements imposed on an entity within the enterprise and results in adverse action against an entity or federal funding, work with the entity to provide alternative standards, policies, or requirements that do not conflict with the federal regulation or requirement. The department, acting through the Florida Digital Service, shall annually report, by January 31, such alternative standards to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(p)1. Establish an information technology policy for all information technology-related state contracts, including state term contracts for information technology commodities, consultant services, and staff augmentation services. The information technology policy must include:

a. Identification of the information technology product and service categories to be included in state term contracts.

b. Requirements to be included in solicitations for state

term contracts.

c. Evaluation criteria for the award of information technology-related state term contracts.

d. The term of each information technology-related state term contract.

e. The maximum number of vendors authorized on each state term contract.

f. At a minimum, a requirement that any contract for information technology commodities or services meet the National Institute of Standards and Technology Cybersecurity Framework.

g. For an information technology project wherein project oversight is required pursuant to paragraph (d) or paragraph (m), a requirement that independent verification and validation be employed throughout the project life cycle with the primary objective of independent verification and validation being to provide an objective assessment of products and processes throughout the project life cycle. An entity providing independent verification and validation may not have technical, managerial, or financial interest in the project and may not have responsibility for, or participate in, any other aspect of the project.

2. Evaluate vendor responses for information technology-related state term contract solicitations and invitations to negotiate.

3. Answer vendor questions on information technology-related state term contract solicitations.

4. Ensure that the information technology policy established pursuant to subparagraph 1. is included in all solicitations and contracts that are administratively executed

by the department.

(q) Recommend potential methods for standardizing data across state agencies which will promote interoperability and reduce the collection of duplicative data.

(r) Recommend open data technical standards and terminologies for use by the enterprise.

(s) Support state agencies with the use of ~~Ensure that enterprise information technology solutions are capable of utilizing an~~ electronic credentials in compliance ~~credential and comply~~ with the enterprise architecture standards.

(2)

(c) The state chief information officer, in consultation with the Secretary of Management Services, shall designate a state chief technology officer who must have significant and substantive experience in information technology, operational technology, technology-related projects, and enterprise architecture. The state chief technology officer is responsible for all of the following:

1. Conducting comprehensive evaluations of potential technological solutions and cultivating strategic partnerships with state enterprise agencies and to leverage the state's technological capabilities.

2. Supporting program management of enterprise information technology initiatives; providing advisory support for technology-related projects; and continuously identifying and recommending best practices to optimize outcomes of technology projects and enhance the enterprise's technological efficiency and effectiveness.

Section 4. Subsection (3), paragraphs (a) and (c) of

subsection (4), and subsection (6) of section 282.318, Florida Statutes, are amended, and paragraph (j) is added to subsection (4) of that section, to read:

282.318 Cybersecurity.—

(3) The department, acting through the Florida Digital Service, is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks, including threats to enterprise digital data, and determining appropriate security measures that comply with all national and state data compliance security standards. Such standards and processes must be consistent with generally accepted technology best practices, including the National Institute for Standards and Technology Cybersecurity Framework, for cybersecurity. The department, acting through the Florida Digital Service, shall adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework. The department, acting through the Florida Digital Service, shall also:

(a) Designate an employee of the Florida Digital Service as the state chief information security officer. The state chief information security officer must have experience and expertise in security and risk management for communications and information technology resources. The state chief information security officer is responsible for the development, operation, and oversight of cybersecurity for state technology systems. The state chief information security officer shall be notified of all confirmed or suspected incidents or threats of state agency

information technology resources and must report such incidents or threats to the state chief information officer and the Governor.

(b) Develop, and annually update by February 1, a statewide cybersecurity strategic plan that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for a cyber incident.

(c) Develop and publish for use by state agencies a cybersecurity governance framework that, at a minimum, includes guidelines and processes for:

1. Establishing asset management procedures to ensure that an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

3. Completing comprehensive risk assessments and cybersecurity audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the department.

4. Identifying protection procedures to manage the protection of an agency's information, data, and information technology resources.

5. Establishing procedures for accessing information and data to ensure the confidentiality, integrity, and availability

of such information and data.

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.

7. Establishing agency cybersecurity incident response teams and describing their responsibilities for responding to cybersecurity incidents, including breaches of personal information containing confidential or exempt data.

8. Recovering information and data in response to a cybersecurity incident. The recovery may include recommended improvements to the agency processes, policies, or guidelines.

9. Establishing a cybersecurity incident reporting process that includes procedures for notifying the department and the Department of Law Enforcement of cybersecurity incidents.

a. The level of severity of the cybersecurity incident is defined by the National Cyber Incident Response Plan of the United States Department of Homeland Security as follows:

(I) Level 5 is an emergency-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country’s, state’s, or local government’s residents.

(II) Level 4 is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties.

(III) Level 3 is a high-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security;

economic security; civil liberties; or public confidence.

(IV) Level 2 is a medium-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(V) Level 1 is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

b. The cybersecurity incident reporting process must specify the information that must be reported by a state agency following a cybersecurity incident or ransomware incident, which, at a minimum, must include the following:

(I) A summary of the facts surrounding the cybersecurity incident or ransomware incident.

(II) The date on which the state agency most recently backed up its data; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.

(III) The types of data compromised by the cybersecurity incident or ransomware incident.

(IV) The estimated fiscal impact of the cybersecurity incident or ransomware incident.

(V) In the case of a ransomware incident, the details of the ransom demanded.

c.(I) A state agency shall report all ransomware incidents and ~~any~~ cybersecurity incidents ~~incident determined by the state agency to be of severity level 3, 4, or 5~~ to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible but no later than 48 hours

after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required in sub-subparagraph b.

(II) The Cybersecurity Operations Center shall immediately notify the state chief information officer and the state chief information security officer of a reported incident. The state chief information officer, in consultation with the state chief information security officer, shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a state agency's incident report. The notification must include a high-level description of the incident and the likely effects.

d. ~~A state agency shall report a cybersecurity incident determined by the state agency to be of severity level 1 or 2 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible. The report must contain the information required in sub-subparagraph b.~~

~~e.~~ The Cybersecurity Operations Center shall provide a consolidated incident report by the 30th day after the end of each quarter to the Governor, ~~on a quarterly basis to~~ the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any agency, network information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities

as required in s. 282.319(9).

10. Incorporating information obtained through detection and response activities into the agency's cybersecurity incident response plans.

11. Developing agency strategic and operational cybersecurity plans required pursuant to this section.

12. Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources that align with the state agency risk management strategy and that protect the confidentiality, integrity, and availability of information and data.

13. Establishing procedures for procuring information technology commodities and services that require the commodity or service to meet the National Institute of Standards and Technology Cybersecurity Framework.

14. Submitting after-action reports following a cybersecurity incident or ransomware incident. Such guidelines and processes for submitting after-action reports must be developed and published by December 1, 2022.

(d) Assist state agencies in complying with this section.

(e) In collaboration with the Cybercrime Office of the Department of Law Enforcement, annually provide training for state agency information security managers and computer security incident response team members that contains training on cybersecurity, including cybersecurity threats, trends, and best practices.

(f) Annually review the strategic and operational cybersecurity plans of state agencies.

(g) Annually provide cybersecurity training to all state

agency technology professionals and employees with access to highly sensitive information which develops, assesses, and documents competencies by role and skill level. The cybersecurity training curriculum must include training on the identification of each cybersecurity incident severity level referenced in sub-subparagraph (c)9.a. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(h) Operate and maintain a Cybersecurity Operations Center led by the state chief information security officer, which must be primarily virtual and staffed with tactical detection and incident response personnel. The Cybersecurity Operations Center shall serve as a clearinghouse for threat information and coordinate with the Department of Law Enforcement to support state agencies and their response to any confirmed or suspected cybersecurity incident.

(i) Lead an Emergency Support Function, ESF-20 ~~ESF CYBER~~, under the state comprehensive emergency management plan as described in s. 252.35.

(4) Each state agency head shall, at a minimum:

(a) Designate an information security manager to administer the cybersecurity program of the state agency. This designation must be provided annually in writing to the department by January 31 ~~1~~. A state agency's information security manager, for purposes of these information security duties, shall report directly to the agency head.

(c) Submit to the department annually by July 31, the state agency's strategic and operational cybersecurity plans developed

pursuant to rules and guidelines established by the department, through the Florida Digital Service.

1. The state agency strategic cybersecurity plan must cover a 3-year period and, at a minimum, define security goals, intermediate objectives, and projected agency costs for the strategic issues of agency information security policy, risk management, security training, security incident response, and disaster recovery. The plan must take ~~be based on~~ the statewide cybersecurity strategic plan created by the department into consideration and include performance metrics that can be objectively measured to reflect the status of the state agency's progress in meeting security goals and objectives identified in the agency's strategic information security plan.

2. The state agency operational cybersecurity plan must include a set of measures that objectively assess the performance of the agency's cybersecurity program in accordance with its risk management plan ~~progress report that objectively measures progress made towards the prior operational cybersecurity plan and a project plan that includes activities, timelines, and deliverables for security objectives that the state agency will implement during the current fiscal year~~.

(j) Require that enterprise digital data be maintained in accordance with chapter 119. This paragraph may not be construed to create, modify, abrogate, or expand an exemption from public records requirements under s. 119.07(1) or s. 24(a), Art. I of the State Constitution.

(6)(a) Those portions of a public meeting as specified in s. 286.011 which would reveal records which are confidential and exempt under subsection (5) are exempt from s. 286.011 and s.

24(b), Art. I of the State Constitution. No exempt portion of an exempt meeting may be off the record. All exempt portions of such meeting shall be recorded and transcribed. Such recordings and transcripts are confidential and exempt from disclosure under s. 119.07(1) and s. 24(a), Art. I of the State Constitution unless a court of competent jurisdiction, after an in camera review, determines that the meeting was not restricted to the discussion of data and information made confidential and exempt by this section. In the event of such a judicial determination, only that portion of the recording and transcript which reveals nonexempt data and information may be disclosed to a third party.

(b) If authorized in writing by the President of the Senate or the Speaker of the House of Representatives, as applicable, designated members of the Legislature and legislative staff may attend those portions of a meeting which are exempt under paragraph (a).

Section 5. Subsection (5) of section 282.3185, Florida Statutes, is amended to read:

282.3185 Local government cybersecurity.—

(5) INCIDENT NOTIFICATION.—

(a) A local government shall provide notification of a cybersecurity incident or ransomware incident to the Cybersecurity Operations Center, Cybercrime Office of the Department of Law Enforcement, and sheriff who has jurisdiction over the local government in accordance with paragraph (b). The notification must include, at a minimum, the following information:

1. A summary of the facts surrounding the cybersecurity

incident or ransomware incident.

2. The date on which the local government most recently backed up its data; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.

3. The types of data compromised by the cybersecurity incident or ransomware incident.

4. The estimated fiscal impact of the cybersecurity incident or ransomware incident.

5. In the case of a ransomware incident, the details of the ransom demanded.

6. A statement requesting or declining assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government.

(b)1. A local government shall report all ransomware incidents and any cybersecurity incident determined by the local government to be of severity level 3, 4, or 5 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 12 ~~48~~ hours after discovery of the cybersecurity incident and no later than 6 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a).

2. The Cybersecurity Operations Center shall immediately notify the state chief information officer and state chief information security officer of a reported incident. The state chief information officer, in consultation with the state chief

information security officer, shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a local government's incident report. The notification must include a high-level description of the incident and the likely effects.

(c) A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government. The report must ~~shall~~ contain the information required in paragraph (a).

(d) The Cybersecurity Operations Center shall provide a consolidated incident report by the 30th day after the end of each quarter ~~on a quarterly basis~~ to the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any local government, network information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

Section 6. Subsection (4) of section 282.319, Florida Statutes, is amended to read:

282.319 Florida Cybersecurity Advisory Council.—

(4) The council shall be composed ~~comprised~~ of the following members:

(a) The Lieutenant Governor, or his or her designee.

(b) The state chief information officer.

(c) The state chief information security officer.

(d) The director of the Division of Emergency Management, or his or her designee.

(e) A representative of the computer crime center of the Department of Law Enforcement, appointed by the executive director of the Department of Law Enforcement.

(f) A representative of the Florida Fusion Center of the Department of Law Enforcement, appointed by the executive director of the Department of Law Enforcement.

(g) No more than two representatives from local government, appointed by the Governor ~~The Chief Inspector General~~.

(h) A representative from the Public Service Commission.

(i) No more than ~~Up to~~ two representatives from institutions of higher education located in this state, appointed by the Governor.

(j) Three representatives from critical infrastructure sectors, one of whom must be from a water treatment facility, appointed by the Governor.

(k) Four representatives of the private sector with senior level experience in cybersecurity or software engineering from within the finance, energy, health care, and transportation sectors, appointed by the Governor.

(l) Two representatives with expertise on emerging technology, with one appointed by the President of the Senate and one appointed by the Speaker of the House of Representatives.

(m) The Chief Inspector General, who shall serve as an ex-officio, nonvoting member of the council.

Section 7. This act shall take effect July 1, 2025.