By the Committee on Governmental Oversight and Accountability; and Senator Boyd

585-03626A-21 20211900c1

A bill to be entitled

An act relating to cybersecurity; amending s. 20.055, F.S.; requiring certain audit plans of an inspector general to include certain information; amending s. 282.0041, F.S.; revising and providing definitions; amending ss. 282.0051, 282.201, and 282.206, F.S.; revising provisions to replace references to information technology security with cybersecurity; amending s. 282.318, F.S.; revising provisions to replace references to information technology security and computer security with references to cybersecurity; revising a short title; providing that the Department of Management Services, acting through the Florida Digital Service, is the lead entity for the purpose of certain responsibilities; providing and revising requirements for the department, acting through the Florida Digital Service; providing that the state chief information security officer is responsible for state technology systems and shall be notified of certain incidents and threats; revising requirements for state agency heads; requiring the department, through the Florida Digital Service, to track the implementation by state agencies of certain plans; creating s. 282.319, F.S.; creating the Florida Cybersecurity Advisory Council within the Department of Management Services; providing the purpose of the council; requiring the council to provide certain assistance to the Florida Digital Service; providing for the membership of the council; providing for terms

of council members; providing that the Secretary of Management Services, or his or her designee, shall serve as the ex officio, nonvoting executive director of the council; providing that members shall serve without compensation but are entitled to reimbursement for per diem and travel expenses; requiring the council to meet at least quarterly for certain purposes; requiring the council to work with certain entities to identify certain local infrastructure sectors and critical cyber infrastructure; requiring the council to submit an annual report to the Legislature; providing an effective date.

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

Section 1. Paragraph (i) of subsection (6) of section 20.055, Florida Statutes, is amended to read:

20.055 Agency inspectors general.—

(6) In carrying out the auditing duties and responsibilities of this act, each inspector general shall review and evaluate internal controls necessary to ensure the fiscal accountability of the state agency. The inspector general shall conduct financial, compliance, electronic data processing, and performance audits of the agency and prepare audit reports of his or her findings. The scope and assignment of the audits shall be determined by the inspector general; however, the agency head may at any time request the inspector general to perform an audit of a special program, function, or organizational unit. The performance of the audit shall be under

the direction of the inspector general, except that if the inspector general does not possess the qualifications specified in subsection (4), the director of auditing shall perform the functions listed in this subsection.

(i) The inspector general shall develop long-term and annual audit plans based on the findings of periodic risk assessments. The plan, where appropriate, should include postaudit samplings of payments and accounts. The plan shall show the individual audits to be conducted during each year and related resources to be devoted to the respective audits. The plan shall include a specific cybersecurity audit plan. The Chief Financial Officer, to assist in fulfilling the responsibilities for examining, auditing, and settling accounts, claims, and demands pursuant to s. 17.03(1), and examining, auditing, adjusting, and settling accounts pursuant to s. 17.04, may use audits performed by the inspectors general and internal auditors. For state agencies under the jurisdiction of the Governor, the audit plans shall be submitted to the Chief Inspector General. The plan shall be submitted to the agency head for approval. A copy of the approved plan shall be submitted to the Auditor General.

Section 2. Present subsections (8) through (21) of section 282.0041, Florida Statutes, are redesignated as subsections (9) through (22), respectively, a new subsection (8) is added to that section, and present subsection (22) of that section is amended, to read:

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

(8) "Cybersecurity" means the protection afforded to an automated information system in order to attain the applicable

objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources.

~~(22) "Information technology security" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of data, information, and information technology resources.~~

Section 3. Paragraph (j) of subsection (1) of section 282.0051, Florida Statutes, is amended to read:

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

(1) The Florida Digital Service has been created within the department to propose 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:

(j) Provide operational management and oversight of the state data center established pursuant to s. 282.201, which includes:

1. Implementing industry standards and best practices for the state data center's facilities, operations, maintenance, planning, and management processes.

2. Developing and implementing cost-recovery mechanisms that recover the full direct and indirect cost of services through charges to applicable customer entities. Such cost-

recovery mechanisms must comply with applicable state and federal regulations concerning distribution and use of funds and must ensure that, for any fiscal year, no service or customer entity subsidizes another service or customer entity. The Florida Digital Service may recommend other payment mechanisms to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives. Such mechanism may be implemented only if specifically authorized by the Legislature.

3. Developing and implementing appropriate operating guidelines and procedures necessary for the state data center to perform its duties pursuant to s. 282.201. The guidelines and procedures must comply with applicable state and federal laws, regulations, and policies and conform to generally accepted governmental accounting and auditing standards. The guidelines and procedures must include, but need not be limited to:

a. Implementing a consolidated administrative support structure responsible for providing financial management, procurement, transactions involving real or personal property, human resources, and operational support.

b. Implementing an annual reconciliation process to ensure that each customer entity is paying for the full direct and indirect cost of each service as determined by the customer entity’s use of each service.

c. Providing rebates that may be credited against future billings to customer entities when revenues exceed costs.

d. Requiring customer entities to validate that sufficient funds exist in the appropriate data processing appropriation category or will be transferred into the appropriate data

processing appropriation category before implementation of a customer entity's request for a change in the type or level of service provided, if such change results in a net increase to the customer entity's cost for that fiscal year.

e. By November 15 of each year, providing to the Office of Policy and Budget in the Executive Office of the Governor and to the chairs of the legislative appropriations committees the projected costs of providing data center services for the following fiscal year.

f. Providing a plan for consideration by the Legislative Budget Commission if the cost of a service is increased for a reason other than a customer entity's request made pursuant to sub-subparagraph d. Such a plan is required only if the service cost increase results in a net increase to a customer entity for that fiscal year.

g. Standardizing and consolidating procurement and contracting practices.

4. In collaboration with the Department of Law Enforcement, developing and implementing a process for detecting, reporting, and responding to cybersecurity ~~information technology security~~ incidents, breaches, and threats.

5. Adopting rules relating to the operation of the state data center, including, but not limited to, budgeting and accounting procedures, cost-recovery methodologies, and operating procedures.

Section 4. Paragraph (g) of subsection (1) of section 282.201, Florida Statutes, is amended to read:

282.201 State data center.—The state data center is established within the department. The provision of data center

services must comply with applicable state and federal laws, regulations, and policies, including all applicable security, privacy, and auditing requirements. The department shall appoint a director of the state data center, preferably an individual who has experience in leading data center facilities and has expertise in cloud-computing management.

(1) STATE DATA CENTER DUTIES.—The state data center shall:

(g) In its procurement process, show preference for cloud-computing solutions that minimize or do not require the purchasing, financing, or leasing of state data center infrastructure, and that meet the needs of customer agencies, that reduce costs, and that meet or exceed the applicable state and federal laws, regulations, and standards for cybersecurity ~~information technology security~~.

Section 5. Subsection (2) of section 282.206, Florida Statutes, is amended to read:

282.206 Cloud-first policy in state agencies.—

(2) In its procurement process, each state agency shall show a preference for cloud-computing solutions that either minimize or do not require the use of state data center infrastructure when cloud-computing solutions meet the needs of the agency, reduce costs, and meet or exceed the applicable state and federal laws, regulations, and standards for cybersecurity ~~information technology security~~.

Section 6. Section 282.318, Florida Statutes, is amended to read:

282.318 Cybersecurity ~~Security of data and information technology~~.—

(1) This section may be cited as the "State Cybersecurity

Act." ~~"Information Technology Security Act."~~

(2) As used in this section, the term "state agency" has the same meaning as provided in s. 282.0041, except that the term includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

(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 and determining appropriate security measures. 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 ~~information technology security, to include cybersecurity, and adopting~~ rules that mitigate risks; safeguard state agency digital assets, ~~an agency's~~ data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework ~~and to mitigate risks~~. 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 ~~information technology security~~ 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 ~~the strategic issues of information technology security policy, risk management, training, incident management, and disaster recovery planning~~.

(c) Develop and publish for use by state agencies a cybersecurity governance ~~an information technology security~~ 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 ~~information technology security~~ 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 ~~computer security~~ incident response teams and describing their responsibilities for responding to cybersecurity ~~information technology security~~ incidents, including breaches of personal information containing confidential or exempt data.

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

9. Establishing a cybersecurity ~~an information technology security~~ incident reporting process that includes procedures and tiered reporting timeframes for notifying the department and the Department of Law Enforcement of cybersecurity ~~information technology security~~ incidents. The tiered reporting timeframes shall be based upon the level of severity of the cybersecurity ~~information technology security~~ incidents being reported.

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

11. Developing agency strategic and operational cybersecurity ~~information technology security~~ 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.

(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 ~~information technology security~~, including cybersecurity~~,~~ threats, trends, and best practices.

(f) Annually review the strategic and operational cybersecurity ~~information technology security~~ plans of state ~~executive branch~~ agencies.

(g) Provide cybersecurity training to all state agency technology professionals which develops, assesses, and documents competencies by role and skill level. 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 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 ~~information technology security~~ program of the state agency. This designation must be provided annually in writing to the department by January 1. A state agency's information security manager, for purposes of these information security duties, shall report directly to the agency head.

(b) In consultation with the department, through the Florida Digital Service, and the Cybercrime Office of the Department of Law Enforcement, establish an agency cybersecurity ~~computer security incident~~ response team to respond to a cybersecurity ~~an information technology security~~ incident. The agency cybersecurity ~~computer security incident~~ response team shall convene upon notification of a cybersecurity ~~an information technology security~~ incident and must immediately report all confirmed or suspected incidents to the state chief information security officer, or his or her designee, and comply with all applicable guidelines and processes established pursuant to paragraph (3)(c).

(c) Submit to the department annually by July 31, the state agency's strategic and operational cybersecurity ~~information technology security~~ plans developed pursuant to rules and guidelines established by the department, through the Florida Digital Service.

1. The state agency strategic cybersecurity ~~information technology security~~ 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 be based on the statewide cybersecurity ~~information technology security~~ strategic plan created by the department 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 ~~information technology security~~ plan must include a progress report that objectively measures progress made towards the prior operational cybersecurity ~~information technology security~~ 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.

(d) Conduct, and update every 3 years, a comprehensive risk assessment, which may be completed by a private sector vendor, to determine the security threats to the data, information, and information technology resources, including mobile devices and print environments, of the agency. The risk assessment must

comply with the risk assessment methodology developed by the department and is confidential and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Florida Digital Service within the department, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General. If a private sector vendor is used to complete a comprehensive risk assessment, it must attest to the validity of the risk assessment findings.

(e) Develop, and periodically update, written internal policies and procedures, which include procedures for reporting cybersecurity ~~information technology security~~ incidents and breaches to the Cybercrime Office of the Department of Law Enforcement and the Florida Digital Service within the department. Such policies and procedures must be consistent with the rules, guidelines, and processes established by the department to ensure the security of the data, information, and information technology resources of the agency. The internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service within the department, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(f) Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by the department to address identified risks to the data,

information, and information technology resources of the agency. The department, through the Florida Digital Service, shall track implementation by state agencies upon development of such remediation plans in coordination with agency inspectors general.

(g) Ensure that periodic internal audits and evaluations of the agency's cybersecurity ~~information technology security~~ program for the data, information, and information technology resources of the agency are conducted. The results of such audits and evaluations are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service within the department, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

(h) Ensure that the ~~information technology security and~~ cybersecurity requirements in both the written specifications for the solicitation, contracts, and service-level agreement of information technology and information technology resources and services meet or exceed the applicable state and federal laws, regulations, and standards for ~~information technology security and~~ cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework. Service-level agreements must identify service provider and state agency responsibilities for privacy and security, protection of government data, personnel background screening, and security deliverables with associated frequencies.

(i) Provide ~~information technology security and~~ cybersecurity awareness training to all state agency employees

in the first 30 days after commencing employment concerning cybersecurity ~~information technology security~~ risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. 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.

(j) Develop a process for detecting, reporting, and responding to threats, breaches, or cybersecurity ~~information technology security~~ incidents which is consistent with the security rules, guidelines, and processes established by the department through the Florida Digital Service.

1. All cybersecurity ~~information technology security~~ incidents and breaches must be reported to the Florida Digital Service within the department and the Cybercrime Office of the Department of Law Enforcement and must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c).

2. For cybersecurity ~~information technology security~~ breaches, state agencies shall provide notice in accordance with s. 501.171.

(5) Portions of records held by a state agency which contain network schematics, hardware and software configurations, or encryption, or which identify detection, investigation, or response practices for suspected or confirmed cybersecurity ~~information technology security~~ incidents, including suspected or confirmed breaches, are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State

Constitution, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

(a) Data or information, whether physical or virtual; or

(b) Information technology resources, which includes:

1. Information relating to the security of the agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or

2. Security information, whether physical or virtual, which relates to the agency's existing or proposed information technology systems.

(6) The portions of risk assessments, evaluations, external audits, and other reports of a state agency's cybersecurity ~~information technology security~~ program for the data, information, and information technology resources of the state agency which are held by a state agency are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution if the disclosure of such portions of records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

(a) Data or information, whether physical or virtual; or

(b) Information technology resources, which include:

1. Information relating to the security of the agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or

2. Security information, whether physical or virtual, which relates to the agency's existing or proposed information

technology systems.

For purposes of this subsection, "external audit" means an audit that is conducted by an entity other than the state agency that is the subject of the audit.

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

(8) The portions of records made confidential and exempt in subsections (5), (6), and (7) shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service within the department, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. Such portions of records may be made available to a local government, another state agency, or a federal agency for cybersecurity ~~information technology security~~ purposes or in furtherance of the state agency's official

duties.

(9) The exemptions contained in subsections (5), (6), and (7) apply to records held by a state agency before, on, or after the effective date of this exemption.

(10) Subsections (5), (6), and (7) are subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2025, unless reviewed and saved from repeal through reenactment by the Legislature.

(11) The department shall adopt rules relating to cybersecurity ~~information technology security~~ and to administer this section.

Section 7. Section 282.319, Florida Statutes, is created to read:

282.319 Florida Cybersecurity Advisory Council.—

(1) The Florida Cybersecurity Advisory Council, an advisory council as defined in s. 20.03(7), is created within the department. Except as otherwise provided in this section, the advisory council shall operate in a manner consistent with s. 20.052.

(2) The purpose of the council is to assist state agencies in protecting their information technology resources from cyber threats and incidents.

(3) The council shall assist the Florida Digital Service in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force created under chapter 2019-118, Laws of Florida.

(4) The council shall be 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.

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

(g) The Chief Inspector General.

(h) A representative from the Public Service Commission.

(i) 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 which 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.

(5) Members shall serve for a term of 4 years; however, for the purpose of providing staggered terms, the initial appointments of members made by the Governor shall be for a term

of 2 years. A vacancy shall be filled for the remainder of the unexpired term in the same manner as the initial appointment. All members of the council are eligible for reappointment.

(6) The Secretary of Management Services, or his or her designee, shall serve as the ex officio, nonvoting executive director of the council.

(7) Members of the council shall serve without compensation but are entitled to receive reimbursement for per diem and travel expenses pursuant to s. 112.061.

(8) The council shall meet at least quarterly to:

(a) Review existing state agency cybersecurity policies.

(b) Assess ongoing risks to state agency information technology.

(c) Recommend a reporting and information sharing system to notify state agencies of new risks.

(d) Recommend data breach simulation exercises.

(e) Assist the Florida Digital Service in developing cybersecurity best practice recommendations for state agencies which include recommendations regarding:

1. Continuous risk monitoring.

2. Password management.

3. Protecting data in legacy and new systems.

(f) Examine inconsistencies between state and federal law regarding cybersecurity.

(9) The council shall work with the National Institute of Standards and Technology and other federal agencies, private sector businesses, and private cybersecurity experts:

(a) For critical infrastructure not covered by federal law, to identify which local infrastructure sectors are at the

greatest risk of cyber attacks and need the most enhanced cybersecurity measures.

(b) To use federal guidance to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage or unauthorized cyber access to the infrastructure could reasonably result in catastrophic consequences.

(10) Beginning June 30, 2022, and each June 30 thereafter, the council shall submit to the President of the Senate and the Speaker of the House of Representatives any legislative recommendations considered necessary by the council to address cybersecurity.

Section 8. This act shall take effect July 1, 2021.