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

585-03244A-23 20231708c1

A bill to be entitled

An act relating to cybersecurity; providing a short title; amending s. 110.205, F.S.; exempting certain personnel from the career service; amending s. 282.0041, F.S.; defining terms; revising the definition of the term "incident"; amending s. 282.0051, F.S.; requiring the Florida Digital Service to ensure that independent project oversight is performed in a certain manner and to take certain actions relating to the procurement of project oversight as a service; requiring the Florida Digital Service to provide certain reports by certain dates; requiring the Florida Digital Service to establish an operations committee for a certain purpose and composed of certain members; requiring the Governor to appoint a state chief information officer subject to confirmation by the Senate; requiring the state chief information officer to designate a state chief technology officer; providing duties of the state chief technology officer; amending s. 282.201, F.S.; requiring that the state data center be overseen by and accountable to the Department of Management Services in consultation with certain officers; providing requirements for certain state data center procurements; requiring the state chief information officer to assume responsibility for a certain contract; requiring that the Florida Digital Service be provided with full access to state data center infrastructure, systems, applications, and other means

of hosting, supporting, and managing certain data; requiring the state data center to submit a certain report to the department and the Florida Digital Service; amending s. 282.318, F.S.; requiring a state agency to report ransomware and cybersecurity incidents within a certain time period; requiring the Florida Digital Service to notify the Governor and Legislature of certain incidents; requiring that certain notification be provided in a secure environment; requiring the Florida Digital Service to provide cybersecurity briefings to certain legislative committees; authorizing the Florida Digital Service to respond to certain cybersecurity incidents; requiring a state agency head to designate a chief information security officer for the agency; revising the purpose of an agency's information security manager and the date by which he or she must be designated; revising the frequency of a comprehensive risk assessment; authorizing the department to facilitate and providing requirements for such assessment; authorizing certain legislative committees to hold closed meetings to receive certain briefings; requiring such committees to maintain the confidential and exempt status of certain records; amending s. 282.3185, F.S.; requiring a local government to report ransomware and cybersecurity incidents within a certain time period; requiring the Florida Digital Service to notify the Governor and Legislature of certain incidents; requiring that certain notification be provided in a

secure environment; amending s. 282.319, F.S.; revising the membership of the Florida Cybersecurity Advisory Council; creating s. 768.401, F.S.; providing that a county, municipality, or commercial entity that complies with certain requirements is not liable in connection with a cybersecurity incident; requiring certain entities to adopt certain revised frameworks or standards within a specified time period; providing that a private cause of action is not established; providing that certain failures are not evidence of negligence and do not constitute negligence per se; specifying that the defendant in certain actions has a certain burden of proof; providing an effective date.

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

Section 1. This act may be cited as the "Florida Cyber Protection Act."

Section 2. Paragraph (y) is added to subsection (2) of section 110.205, Florida Statutes, to read:

110.205 Career service; exemptions.—

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

(y) Personnel employed by or reporting to the state chief information security officer, the state chief data officer, a chief information security officer, and an agency information security manager.

Section 3. Present subsections (3) through (5), (6) through (19), and (20) through (38) of section 282.0041, Florida

Statutes, are redesignated as subsections (4) through (6), (8) through (21), and (24) through (42), respectively, new subsections (3), (7), (22), and (23) are added to that section, and present subsection (19) is amended, to read:

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

(3) "As a service" means the contracting with or outsourcing to a third-party of a defined role or function as a means of delivery.

(7) "Cloud provider" has the same meaning as provided in Special Publication 800-145 issued by the National Institute of Standards and Technology.

(21) ~~(19)~~ "Incident" means a violation or an imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices, or which may jeopardize the confidentiality, integrity, or availability of an information technology system or the information the system processes, stores, or transmits. An imminent threat of violation refers to a situation in which a state agency, county, or municipality has a factual basis for believing that a specific incident is about to occur.

(22) "Independent" means, for an entity providing independent verification and validation, having no technical, managerial, or financial interest in the relevant technology project; no relationship to the relevant agency; and no responsibility for or participation in any aspect of the project, which includes project oversight by the Florida Digital Service.

(23) "Independent verification and validation" means third-

party support services that provide a completely independent and impartial assessment of the progress and work products of a technology project from concept to business case and throughout the project life cycle.

Section 4. 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 is ~~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:

(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) Ensure that independent ~~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 is performed and in compliance with applicable state and federal law.

1. The department may not be considered independent for purposes of project oversight under this paragraph on a project for which the department has provided or may be asked to provide any operational or technical support, including, but not limited to, providing advice or conducting any review.

2. The department shall establish an appropriate contract

vehicle to facilitate procurement of project oversight as a service by the enterprise and ensure that the contract vehicle includes offerings that incorporate the ability to comply with applicable state and federal law, including any independent verification and validation requirements. An entity that provides project oversight as a service must provide a project oversight report to the department.

3. An agency may request the department to procure project oversight as a service for a project that is subject to this paragraph. Such procurement by the department does not violate the requirement that the project oversight must be independent.

4. The department, acting through the Florida Digital Service, shall at least quarterly review received project oversight reports and, upon acceptance of the contents of such reports, provide the reports to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

5. The department, acting through the Florida Digital Service, shall report 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 15 ~~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 15th 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 by January 15 report 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) Ensure that enterprise information technology solutions are capable of utilizing an electronic credential and comply with the enterprise architecture standards.

(t) Establish an operations committee that shall meet as necessary for the purpose of developing collaborative efforts between agencies and other governmental entities relating to cybersecurity issues, including the coordination of preparedness and response efforts relating to cybersecurity incidents and issues relating to the interoperability of agency projects. The Secretary of Management Services shall serve as the executive director of the committee. The committee shall be composed of the following members:

1. The state chief information officer, or his or her designee.

2. The Attorney General, or his or her designee.

3. The Secretary of State, or his or her designee.

4. The executive director of the Department of Law Enforcement, or his or her designee.

5. The Secretary of Transportation, or his or her designee.

6. The director of the Division of Emergency Management, or his or her designee.

7. The Secretary of Health Care Administration, or his or her designee.

8. The Commissioner of Education, or his or her designee.

9. The executive director of the Department of Highway Safety and Motor Vehicles, or his or her designee.

10. The chair of the Public Service Commission, or his or her designee.

11. The director of the Florida State Guard, or his or her

designee.

12. The Adjutant General of the Florida National Guard, or his or her designee.

13. Any other agency head appointed by the Governor.

(2)(a) The Governor shall appoint ~~Secretary of Management Services shall designate~~ a state chief information officer, subject to confirmation by the Senate, who shall administer the Florida Digital Service. The state chief information officer, before ~~prior to~~ appointment, must have at least 5 years of experience in the development of information system strategic planning and development or information technology policy, and, preferably, have leadership-level experience in the design, development, and deployment of interoperable software and data solutions.

(b) The state chief information officer~~, in consultation with the Secretary of Management Services,~~ shall designate a state chief data officer. The chief data officer must be a proven and effective administrator who must have significant and substantive experience in data management, data governance, interoperability, and security.

(c) The state chief information officer shall designate a state chief technology officer who shall be responsible for:

1. Exploring technology solutions to meet the enterprise need;

2. The deployments of adopted enterprise solutions;

3. Compliance with the cloud-first policy specified in s. 282.206;

4. Recommending best practices to increase the likelihood of technology project success;

5. Developing strategic partnerships with the private sector; and

6. Directly supporting enterprise cybersecurity and data interoperability initiatives.

The state chief technology officer may acquire cloud migration as a service to comply with this section as it pertains to the implementation across the enterprise of the cloud-first policy.

(3) The department, acting through the Florida Digital Service and from funds appropriated to the Florida Digital Service, shall:

(a) Create~~, not later than December 1, 2022,~~ and maintain a comprehensive indexed data catalog in collaboration with the enterprise that lists the data elements housed within the enterprise and the legacy system or application in which these data elements are located. The data catalog must, at a minimum, specifically identify all data that is restricted from public disclosure based on federal or state laws and regulations and require that all such information be protected in accordance with s. 282.318.

(b) Develop and publish~~, not later than December 1, 2022,~~ in collaboration with the enterprise, a data dictionary for each agency that reflects the nomenclature in the comprehensive indexed data catalog.

(c) Adopt, by rule, standards that support the creation and deployment of an application programming interface to facilitate integration throughout the enterprise.

(d) Adopt, by rule, standards necessary to facilitate a secure ecosystem of data interoperability that is compliant with

the enterprise architecture.

(e) Adopt, by rule, standards that facilitate the deployment of applications or solutions to the existing enterprise system in a controlled and phased approach.

(f) After submission of documented use cases developed in conjunction with the affected agencies, assist the affected agencies with the deployment, contingent upon a specific appropriation therefor, of new interoperable applications and solutions:

1. For the Department of Health, the Agency for Health Care Administration, the Agency for Persons with Disabilities, the Department of Education, the Department of Elderly Affairs, and the Department of Children and Families.

2. To support military members, veterans, and their families.

(4) For information technology projects that have ~~a~~ total project costs ~~cost~~ of $10 million or more:

(a) State agencies must provide the Florida Digital Service with written notice of any planned procurement of an information technology project.

(b) The Florida Digital Service must participate in the development of specifications and recommend modifications to any planned procurement of an information technology project by state agencies so that the procurement complies with the enterprise architecture.

(c) The Florida Digital Service must participate in post-award contract monitoring.

(5) The department, acting through the Florida Digital Service, may not retrieve or disclose any data without a shared-

data agreement in place between the department and the enterprise entity that has primary custodial responsibility of, or data-sharing responsibility for, that data.

(6) The department, acting through the Florida Digital Service, shall adopt rules to administer this section.

Section 5. Section 282.201, Florida Statutes, is amended to read:

282.201 State data center.—The state data center is established within the department and shall be overseen by and accountable to the department in consultation with the state chief information officer, the state chief data officer, the state chief information security officer, and the state chief technology officer. Any procurement or purchase of enterprise architecture which is comparable to a project that would be subject to requirements under s. 282.0051(4) if the total project cost was $10 million or more and which may be consumed by an enterprise must be provided to the department and the Florida Digital Service for review before publication. 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 Florida Digital Service ~~department~~ shall appoint a director of the state data center 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:

(a) Offer, develop, and support the services and applications defined in service-level agreements executed with its customer entities.

(b) Maintain performance of the state data center by

ensuring proper data backup; data backup recovery; disaster recovery; and appropriate security, power, cooling, fire suppression, and capacity.

(c) Develop and implement business continuity and disaster recovery plans, and annually conduct a live exercise of each plan.

(d) Enter into a service-level agreement with each customer entity to provide the required type and level of service or services. If a customer entity fails to execute an agreement within 60 days after commencement of a service, the state data center may cease service. A service-level agreement may not have a term exceeding 3 years and at a minimum must:

1. Identify the parties and their roles, duties, and responsibilities under the agreement.

2. State the duration of the contract term and specify the conditions for renewal.

3. Identify the scope of work.

4. Identify the products or services to be delivered with sufficient specificity to permit an external financial or performance audit.

5. Establish the services to be provided, the business standards that must be met for each service, the cost of each service by agency application, and the metrics and processes by which the business standards for each service are to be objectively measured and reported.

6. Provide a timely billing methodology to recover the costs of services provided to the customer entity pursuant to s. 215.422.

7. Provide a procedure for modifying the service-level

agreement based on changes in the type, level, and cost of a service.

8. Include a right-to-audit clause to ensure that the parties to the agreement have access to records for audit purposes during the term of the service-level agreement.

9. Provide that a service-level agreement may be terminated by either party for cause only after giving the other party and the department notice in writing of the cause for termination and an opportunity for the other party to resolve the identified cause within a reasonable period.

10. Provide for mediation of disputes by the Division of Administrative Hearings pursuant to s. 120.573.

(e) For purposes of chapter 273, be the custodian of resources and equipment located in and operated, supported, and managed by the state data center.

(f) Assume administrative access rights to resources and equipment, including servers, network components, and other devices, consolidated into the state data center.

1. Upon consolidation, a state agency shall relinquish administrative rights to consolidated resources and equipment. State agencies required to comply with federal and state criminal justice information security rules and policies shall retain administrative access rights sufficient to comply with the management control provisions of those rules and policies; however, the state data center shall have the appropriate type or level of rights to allow the center to comply with its duties pursuant to this section. The Department of Law Enforcement shall serve as the arbiter of disputes pertaining to the appropriate type and level of administrative access rights

pertaining to the provision of management control in accordance with the federal criminal justice information guidelines.

2. The state data center shall provide customer entities with access to applications, servers, network components, and other devices necessary for entities to perform business activities and functions, and as defined and documented in a service-level agreement.

(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.

(h) Assist customer entities in transitioning from state data center services to the Northwest Regional Data Center or other third-party cloud-computing services procured by a customer entity or by the Northwest Regional Data Center on behalf of a customer entity.

(2) USE OF THE STATE DATA CENTER.—The following are exempt from the use of the state data center: the Department of Law Enforcement, the Department of the Lottery's Gaming System, Systems Design and Development in the Office of Policy and Budget, the regional traffic management centers as described in s. 335.14(2) and the Office of Toll Operations of the Department of Transportation, the State Board of Administration, state attorneys, public defenders, criminal conflict and civil regional counsel, capital collateral regional counsel, and the Florida Housing Finance Corporation.

(3) AGENCY LIMITATIONS.—Unless exempt from the use of the

state data center pursuant to this section or authorized by the Legislature, a state agency may not:

(a) Create a new agency computing facility or data center, or expand the capability to support additional computer equipment in an existing agency computing facility or data center; or

(b) Terminate services with the state data center without giving written notice of intent to terminate services 180 days before such termination.

(4) DEPARTMENT RESPONSIBILITIES.—The department shall provide operational management and oversight of the state data center, which includes:

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

(b) 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 department 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 mechanisms may be implemented only if specifically authorized by the Legislature.

(c) Developing and implementing appropriate operating guidelines and procedures necessary for the state data center to

perform its duties pursuant to subsection (1). 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:

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

2. 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.

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

4. Requiring customer entities to validate that sufficient funds exist 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.

5. 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.

6. 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

subparagraph 4. Such a plan is required only if the service cost increase results in a net increase to a customer entity for that fiscal year.

7. Standardizing and consolidating procurement and contracting practices.

(d) In collaboration with the Department of Law Enforcement and the Florida Digital Service, developing and implementing a process for detecting, reporting, and responding to cybersecurity incidents, breaches, and threats.

(e) 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.

(5) NORTHWEST REGIONAL DATA CENTER CONTRACT.—In order for the department to carry out its duties and responsibilities relating to the state data center, the state chief information officer shall assume responsibility for the contract entered into by the secretary of the department ~~shall contract by July 1, 2022,~~ with the Northwest Regional Data Center pursuant to s. 287.057(11). The contract shall provide that the Northwest Regional Data Center will manage the operations of the state data center and provide data center services to state agencies. Notwithstanding the terms of the contract, the Northwest Regional Data Center must provide the Florida Digital Service with access to information regarding the operations of the state data center.

(a) The department shall provide contract oversight, including, but not limited to, reviewing invoices provided by the Northwest Regional Data Center for services provided to

state agency customers.

(b) The department shall approve or request updates to invoices within 10 business days after receipt. If the department does not respond to the Northwest Regional Data Center, the invoice will be approved by default. The Northwest Regional Data Center must submit approved invoices directly to state agency customers.

(6) FLORIDA DIGITAL SERVICE ACCESS.—The state data center, and any successor entity assuming the responsibilities of the state data center, including, but not limited to, the Northwest Regional Data Center, shall provide the Florida Digital Service with full access to any infrastructure, system, application, or other means that hosts, supports, or manages data in the custody of an enterprise. For any such infrastructure, system, application, or other means, the state data center or a successor entity shall fully integrate with the Cybersecurity Operations Center.

(7) STATE DATA CENTER REPORT.—Subject to s. 119.0725, the state data center and any successor entity must submit to the department and the Florida Digital Service a quarterly report that provides, relating to infrastructure servicing enterprise customers and data, the number of:

(a) Technology assets which are within 1 year of end of life as defined by the manufacturer.

(b) Technology assets which are beyond end of life as defined by the manufacturer.

(c) Technology assets which are within 2 years of being unsupported by the manufacturer.

(d) Technology assets which are currently unsupported by

the manufacturer.

(e) Workloads which are hosted by a commercial cloud service provider as defined in the National Institute of Standards and Technology publication 500-292.

(f) Workloads which are not hosted by a commercial entity which is a cloud service provider as defined in the National Institute of Standards and Technology publication 500-292.

(g) Service level disruptions and average duration of disruption.

Section 6. Present subsection (10) of section 282.318, Florida Statutes, is redesignated as subsection (11), a new subsection (10) is added to that section, and subsections (3) and (4) of that section are amended, 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 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 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 Florida Digital Service, the Cybersecurity Operations Center, and the Cybercrime Office of the Department of Law Enforcement as soon as possible but no later than 4 ~~48~~ hours after discovery of the cybersecurity incident and no later than 2 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in sub-subparagraph b. The Florida Digital Service shall notify the Governor, the President of the Senate, and the Speaker of the House of Representatives of any incident discovered by a state agency but not timely reported under this sub-sub-subparagraph.

(II) The Cybersecurity Operations Center 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 and must be provided in a secure environment.

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.~~

~~c.~~ The Cybersecurity Operations Center shall provide a consolidated incident report by the 15th 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 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 CYBER and digital, under the state comprehensive emergency management plan as described in s. 252.35.

(j) Provide cybersecurity briefings to the members of any legislative committee or subcommittee responsible for policy matters relating to cybersecurity.

(k) Have the authority to respond to any state agency cybersecurity incident.

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

(a) Designate a chief information security officer to integrate the agency's technical and operational cybersecurity efforts with the Cybersecurity Operations Center. This designation must be provided annually in writing to the Florida Digital Service by January 1. An agency's chief information security officer shall report to the agency's chief information officer. An agency may request the department to procure a chief information security officer as a service to fulfill the agency's duties under this paragraph.

(b) ~~(a)~~ Designate an information security manager to ensure compliance with cybersecurity governance, manage risk, and ensure compliance with the state's incident response plan ~~administer the cybersecurity program of the state agency~~. This designation must be provided annually in writing to the department by January 15 ~~1~~. A state agency's information security manager, for purposes of these information security duties, shall report directly to the agency head.

(c) ~~(b)~~ In consultation with the department, through the Florida Digital Service, and the Cybercrime Office of the Department of Law Enforcement, and incorporating the resources of the Florida State Guard as appropriate, establish an agency cybersecurity response team to respond to a cybersecurity incident. The agency cybersecurity response team shall convene

upon notification of a cybersecurity 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).

(d) ~~(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 be based on the statewide cybersecurity 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 plan must include a 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.

(e) ~~(d)~~ Conduct, and update annually by April 30 ~~every 3 years~~, a comprehensive risk assessment, which may be facilitated by the department or 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 criteria, methodology, and scope developed by the state chief information security officer. The risk assessment findings must be signed by the agency head or the agency head's designee and the Florida Digital Service. 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.

(f) ~~(e)~~ Develop, and periodically update, written internal policies and procedures, which include procedures for reporting cybersecurity 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.

(g) ~~(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.

(h) ~~(g)~~ Ensure that periodic internal audits and evaluations of the agency's cybersecurity 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.

(i) ~~(h)~~ Ensure that the cybersecurity requirements in 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 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.

(j) ~~(i)~~ Provide cybersecurity awareness training to all state agency employees within 30 days after commencing employment, and annually thereafter, concerning cybersecurity 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.

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

1. All cybersecurity incidents and ransomware incidents must be reported by state agencies. Such reports must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c).

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

(l) ~~(k)~~ Submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, an after-action report that summarizes the incident, the incident’s resolution, and any insights gained as a result of the incident.

(10) Any legislative committee or subcommittee responsible for policy matters relating to cybersecurity may hold meetings closed by the respective legislative body under the rules of such legislative body at which such committee or subcommittee is briefed on records made confidential and exempt under subsections (5) and (6). The committee or subcommittee must maintain the confidential and exempt status of such records.

Section 7. Paragraphs (b) and (c) of subsection (5) of section 282.3185, Florida Statutes, are amended to read:

282.3185 Local government cybersecurity.—

(5) INCIDENT NOTIFICATION.—

(b)1. A local government shall report all ransomware incidents and ~~any~~ cybersecurity incidents ~~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 Florida Digital Service, 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 4 ~~48~~ hours after discovery of the cybersecurity incident and no later than 2 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a). The Florida Digital Service shall notify the Governor, the President of the Senate, and the Speaker of the House of Representatives of any incident discovered by a local government but not timely reported under this subparagraph.

2. The Cybersecurity Operations Center 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 and must be provided in a secure environment.

~~(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 shall contain the information required in paragraph (a).~~

Section 8. Paragraph (j) of subsection (4) of section 282.319, Florida Statutes, is amended to read:

282.319 Florida Cybersecurity Advisory Council.—

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

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

Section 9. Section 768.401, Florida Statutes, is created to read:

768.401 Limitation on liability for cybersecurity incidents.—

(1) A county or municipality that substantially complies with s. 282.3185 is not liable in connection with a cybersecurity incident.

(2) A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information

is not liable in connection with a cybersecurity incident if the entity substantially complies with s. 501.171, if applicable, and has:

(a) Adopted a cybersecurity program that substantially aligns with the current version of any of the following standards:

1. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

2. NIST special publication 800-171.

3. NIST special publications 800-53 and 800-53A.

4. The Federal Risk and Authorization Management Program security assessment framework.

5. CIS Critical Security Controls.

6. The International Organization for Standardization/International Electrotechnical Commission 27000-series family of standards; or

(b) If regulated by the state or Federal Government, or both, or if otherwise subject to the requirements of any of the following laws and regulations, substantially complied its cybersecurity program to the current version of the following, as applicable:

1. The security requirements of the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. part 164 subpart C.

2. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended.

3. The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

4. The Health Information Technology for Economic and Clinical Health Act, 45 C.F.R. part 162.

(3) The scale and scope of compliance with a standard, law, or regulation under paragraph (2)(a) or paragraph (2)(b) by a covered entity, as applicable, is appropriate if it is based on all of the following factors:

(a) The size and complexity of the covered entity;

(b) The nature and scope of the activities of the covered entity; and

(c) The sensitivity of the information to be protected.

(4) Any commercial entity covered by subsection (2) that substantially complies with a combination of industry-recognized cybersecurity frameworks or standards, including the payment card industry data security standard, to gain the presumption against liability pursuant to subsection (2) must, upon the revision of two or more of the frameworks or standards with which the entity complies, adopt the revised frameworks or standards within 1 year after the latest publication date stated in the revisions.

(5) This section does not establish a private cause of action. Failure of a county, municipality, or commercial entity to substantially implement a cybersecurity program that is in compliance with this section is not evidence of negligence and does not constitute negligence per se.

(6) In an action in connection with a cybersecurity incident, if the defendant is an entity covered by subsection (1) or subsection (2), the defendant has the burden of proof to establish substantial compliance.

Section 10. This act shall take effect July 1, 2023.