COMMITTEE/SUBCOMMITTEE ACTION

ADOPTED	___ (Y/N)
ADOPTED AS AMENDED	___ (Y/N)
ADOPTED W/O OBJECTION	___ (Y/N)
FAILED TO ADOPT	___ (Y/N)
WITHDRAWN	___ (Y/N)
OTHER	_____

Committee/Subcommittee hearing bill: State Administration & Technology Appropriations Subcommittee
Representative Giallombardo offered the following:

Amendment

Remove lines 94-691 and insert:

Section 2. Subsections (3) through (5), (6) through (16), and (17) through (38) of section 282.0041, Florida Statutes, are renumbered as subsections (4) through (6), (8) through (18), and (20) through (41), respectively, and new subsections (3), (7), and (19) are added to that section 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" means an entity that provides cloud-computing services.

(8) "Criminal Justice Agency" has the same meaning as defined in 943.045 (11).

(19) "Enterprise digital data" means information held by a state agency in electronic form that is deemed to be data owned by the state and held for state purposes by the state agency. Enterprise digital data must be maintained in accordance with chapter 119. This subsection may not be construed to create, modify, abrogate, or expand an exemption from public records requirements under s. 119.07(1) or s. 24(a), Art. I of the State Constitution.

Section 3. Subsection (6) of section 282.0051, Florida Statutes, is renumbered as subsection (5), subsections (1) and (4) and present subsection (5) are amended, and paragraph (c) is added to subsection (2) of that section, to read:

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

(1) The Florida Digital Service is established ~~has been created~~ within the department to lead enterprise information technology and cybersecurity efforts, to propose and evaluate innovative solutions pursuant to interagency agreements that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support the

cloud-first policy as specified in s. 282.206. The department, through the Florida Digital Service, shall have the following powers, duties, and functions:

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

(b) Develop an enterprise architecture that:

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

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

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

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

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

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

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

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

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

(d) Perform project oversight on all state agency information technology projects that have total project costs of $10 million or more and that are funded in the General Appropriations Act or any other law. The department, acting through the Florida Digital Service, shall report 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.

(i) ~~(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.

(j)~~(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.

(k)~~(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.

(l)~~(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 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.

(m) ~~(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.

(n) ~~(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.

(o) ~~(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 (l) ~~(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.

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

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

(r) ~~(s)~~ Ensure that enterprise information technology solutions are capable of utilizing an electronic credential and comply with the enterprise architecture standards.

(2)

(c) The state chief information officer, in consultation with the Secretary of Management Services, shall designate a state chief technology officer who shall be responsible for all of the following:

1. Establishing and maintaining an enterprise architecture framework that ensures information technology investments align with the state's strategic objectives and initiatives pursuant to paragraph (1)(b).

2. Conducting comprehensive evaluations of potential technological solutions and cultivating strategic partnerships, internally with state enterprise agencies and externally with the private sector, to leverage collective expertise, foster collaboration, and advance the state's technological capabilities.

3. Supervising program management of enterprise information technology initiatives pursuant to paragraphs (1)(c), (d), and (l); providing advisory support and oversight for technology-related projects; and continuously identifying and recommending best practices to optimize outcomes of technology projects and enhance the enterprise's technological efficiency and effectiveness.

(4) For information technology projects that have a total project 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.

Section 4. Subsection (1) of section 282.00515, Florida Statutes, is amended to read:

282.00515 Duties of Cabinet agencies.—

(1) The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services shall adopt the standards established in s. 282.0051(1)(b), (c), and <u>(q)</u> ~~(r)~~ and (3)(e) or adopt alternative standards based on best practices and industry standards that allow for open data interoperability.

Section 5. Section 5. Subsection (10) of section 282.318, Florida Statutes, is renumbered as subsection (11), subsection (3) and paragraph (a) of subsection (4) are amended, and a new subsection (10) is added to that section, to read:

282.318 Cybersecurity.—

(3) The ~~department, acting through the~~ Florida Digital Service~~,~~ is the lead entity responsible for leading enterprise information technology and cybersecurity efforts, 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 Cybersecurity Operations Center shall immediately notify the state chief information officer and the state chief information security officer ~~shall be notified~~ of all confirmed or suspected incidents or threats of state agency information technology resources. The state chief information officer, in consultation with the state chief information security officer, ~~and~~ must report such incidents or threats to ~~the state chief information officer and~~ the Governor.

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

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

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

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities,

constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

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

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

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

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

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

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

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

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

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

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

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

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

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

b. The cybersecurity incident reporting process must specify the information that must be reported by a state agency

following a cybersecurity incident or ransomware incident, which, at a minimum, must include the following:

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

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

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

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

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

c.(I) A state agency shall report all ransomware incidents and ~~any~~ cybersecurity incidents ~~incident determined by the state agency to be of severity level 3, 4, or 5~~ to the Cybersecurity Operations Center ~~and the Cybercrime Office of the Department of Law Enforcement~~ as soon as possible but no later than 12 ~~48~~ hours after discovery of the cybersecurity incident and no later than 6 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in sub-subparagraph b.

(II) The Cybersecurity Operations Center shall:

(A) Immediately notify the Cybercrime Office of the

Department of Law Enforcement of a reported incident and provide to the Cybercrime Office of the Department of Law Enforcement regular reports on the status of the incident. The department will preserve forensic data to support a subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office of the Department of Law Enforcement upon the office's request as long as the investigation does not impede remediation of the incident and that there is no risk to the public and no risk to critical state functions.

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

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

d.~~e.~~ The Cybersecurity Operations Center shall provide a consolidated incident report by the 30th day after the end of

each quarter ~~on a quarterly basis~~ to the Governor, the Attorney General, the executive director of the Department of Law Enforcement, the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any agency, network information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

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

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

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

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

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

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

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

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

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

(h) Operate and maintain a Cybersecurity Operations Center led by the state chief information security officer, which must

be primarily virtual and staffed with tactical detection and incident response personnel. The Cybersecurity Operations Center shall serve as a clearinghouse for threat information and coordinate with the Department of Law Enforcement to support state agencies and their response to any confirmed or suspected cybersecurity incident.

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

(j) During a cyber incident or as otherwise agreed to in writing by the state agency that holds the particular enterprise data, have the authority to obtain immediate and complete access to state agency accounts and instances that hold enterprise digital data and to direct, in consultation with the state agency that holds the particular enterprise digital data, measures to assess, monitor, and protect the security of enterprise digital data. The department is not authorized to view, modify, transfer, or otherwise duplicate enterprise digital data except as required to respond to a cyber incident or as agreed to in writing by the state agency that holds the particular enterprise digital data. All criminal justice entities are exempt from section (j).

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

(a) Designate an information security manager to ensure compliance with cybersecurity governance and with the state's

enterprise security program and incident response plan. The information security manager must coordinate with the agency's information security personnel and the Cybersecurity Operations Center to ensure that the unique needs of the agency are met ~~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.

Section 6. Paragraph (d) of subsection (5) of section 282.3185, Florida Statutes, is redesignated as paragraph (c), and paragraph (b) and present paragraph (c) of that subsection 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 incident determined by the local government to be of severity level 3, 4, or 5 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center~~, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government~~ as soon as possible but no later than 12 ~~48~~ hours after discovery of the cybersecurity incident and no later than 6 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a).

2. The Cybersecurity Operations Center shall:

a. Immediately notify the Cybercrime Office of the Department of Law Enforcement and provide to the Cybercrime Office of the Department of Law Enforcement and the sheriff who has jurisdiction over the local government regular reports on the status of the incident, preserve forensic data to support a subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office of the Department of Law Enforcement upon the office's request. Except that the Department of Law Enforcement will coordinate the response of all incidents in which a law enforcement agency is the subject of the incident and will provide the Cybersecurity Operations Center with updates.

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

(c) A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of

Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a). The Cybersecurity Operations Center shall immediately notify the Cybercrime Office of the Department of Law Enforcement and the sheriff who has jurisdiction over the local government of a reported incident and provide regular reports on the status of the cybersecurity incident, preserve forensic data to support a subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office of the Department of Law Enforcement upon request if the investigation does not impede remediation of the cybersecurity incident and that there is no risk to the public and no risk to critical state functions.