228190

LEGISLATIVE ACTION

Senate	.	House
Comm: RCS	.	
03/04/2020	.	
	.	
	.	
	.	

The Committee on Appropriations (Hutson) recommended the following:

Senate Amendment (with title amendment)

Delete everything after the enacting clause and insert:

Section 1. Subsection (2) of section 20.22, Florida Statutes, is amended to read:

20.22 Department of Management Services.—There is created a Department of Management Services.

(2) The following divisions, ~~and~~ programs, and services within the Department of Management Services are established:

(a) Facilities Program.

(b) The Florida Digital Service ~~Division of State Technology, the director of which is appointed by the secretary of the department and shall serve as the state chief information officer~~. ~~The state chief information officer must be a proven, effective administrator who must have at least 10 years of executive-level experience in the public or private sector, preferably with experience in the development of information technology strategic planning and the development and implementation of fiscal and substantive information technology policy and standards.~~

(c) Workforce Program.

(d)1. Support Program.

2. Federal Property Assistance Program.

(e) Administration Program.

(f) Division of Administrative Hearings.

(g) Division of Retirement.

(h) Division of State Group Insurance.

(i) Division of Telecommunications.

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

110.205 Career service; exemptions.—

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

(e) The state chief information officer, the state chief data officer, and the state chief information security officer. ~~Unless otherwise fixed by law,~~ The Department of Management Services shall set the salary and benefits of these positions ~~this position~~ in accordance with the rules of the Senior


228190

Management Service.

Section 3. Section 282.0041, Florida Statutes, is amended to read:

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

(1) "Agency assessment" means the amount each customer entity must pay annually for services from the Department of Management Services and includes administrative and data center services costs.

(2) "Agency data center" means agency space containing 10 or more physical or logical servers.

(3) "Breach" has the same meaning as provided in s. 501.171.

(4) "Business continuity plan" means a collection of procedures and information designed to keep an agency's critical operations running during a period of displacement or interruption of normal operations.

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

(6) "Computing facility" or "agency computing facility" means agency space containing fewer than a total of 10 physical or logical servers, but excluding single, logical-server installations that exclusively perform a utility function such as file and print servers.

(7) "Customer entity" means an entity that obtains services from the Department of Management Services.

(8) "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted.


228190

(9) "Data governance" means the practice of organizing, classifying, securing, and implementing policies, procedures, and standards for the effective use of an organization's data.

(10) "Department" means the Department of Management Services.

(11)~~(10)~~ "Disaster recovery" means the process, policies, procedures, and infrastructure related to preparing for and implementing recovery or continuation of an agency's vital technology infrastructure after a natural or human-induced disaster.

(12) "Electronic" means technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(13) "Electronic credential" means an electronic representation of the identity of a person, an organization, an application, or a device.

(14) "Enterprise" means state agencies and the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services.

(15) "Enterprise architecture" means a comprehensive operational framework that contemplates the needs and assets of the enterprise to support interoperability.

(16)~~(11)~~ "Enterprise information technology service" means an information technology service that is used in all agencies or a subset of agencies and is established in law to be designed, delivered, and managed at the enterprise level.

(17)~~(12)~~ "Event" means an observable occurrence in a system or network.

(18)~~(13)~~ "Incident" means a violation or imminent threat of


228190

violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur.

(19)~~(14)~~ "Information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form.

(20)~~(15)~~ "Information technology policy" means a definite course or method of action selected from among one or more alternatives that guide and determine present and future decisions.

(21)~~(16)~~ "Information technology resources" has the same meaning as provided in s. 119.011.

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

(23) "Interoperability" means the technical ability to share and use data across and throughout the enterprise.

(24)~~(18)~~ "Open data" means data collected or created by a state agency, the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and

228190

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

(25) ~~(19)~~ "Performance metrics" means the measures of an organization's activities and performance.

(26) ~~(20)~~ "Project" means an endeavor that has a defined start and end point; is undertaken to create or modify a unique product, service, or result; and has specific objectives that, when attained, signify completion.

(27) ~~(21)~~ "Project oversight" means an independent review and analysis of an information technology project that provides information on the project's scope, completion timeframes, and budget and that identifies and quantifies issues or risks affecting the successful and timely completion of the project.

(28) ~~(22)~~ "Risk assessment" means the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

(29) ~~(23)~~ "Service level" means the key performance indicators (KPI) of an organization or service which must be regularly performed, monitored, and achieved.


228190

(30)~~(24)~~ "Service-level agreement" means a written contract between the Department of Management Services and a customer entity which specifies the scope of services provided, service level, the duration of the agreement, the responsible parties, and service costs. A service-level agreement is not a rule pursuant to chapter 120.

(31)~~(25)~~ "Stakeholder" means a person, group, organization, or state agency involved in or affected by a course of action.

(32)~~(26)~~ "Standards" means required practices, controls, components, or configurations established by an authority.

(33)~~(27)~~ "State agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. As used in part I of this chapter, except as otherwise specifically provided, the term does not include the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services.

(34)~~(28)~~ "SUNCOM Network" means the state enterprise telecommunications system that provides all methods of electronic or optical telecommunications beyond a single building or contiguous building complex and used by entities authorized as network users under this part.

(35)~~(29)~~ "Telecommunications" means the science and technology of communication at a distance, including electronic systems used in the transmission or reception of information.

(36)~~(30)~~ "Threat" means any circumstance or event that has the potential to adversely impact a state agency's operations or

228190

assets through an information system via unauthorized access, destruction, disclosure, or modification of information or denial of service.

(37) ~~(31)~~ "Variance" means a calculated value that illustrates how far positive or negative a projection has deviated when measured against documented estimates within a project plan.

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 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) ~~(1)~~ Develop and publish information technology policy for the management of the state's information technology resources.

(b) ~~(2)~~ 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


228190

be modernized to achieve cloud-first objectives ~~Establish and publish information technology architecture standards to provide for the most efficient use of the state's information technology resources and to ensure compatibility and alignment with the needs of state agencies~~. ~~The department shall assist state agencies in complying with the standards.~~

(c) ~~(3)~~ 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. ~~(a)~~ 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. ~~(b)~~ Methodologies for calculating acceptable variances in the projected versus actual scope, schedule, or cost of an information technology project.

3. ~~(c)~~ 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. ~~(d)~~ Content, format, and frequency of project updates.

(d) ~~(4)~~ 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


228190

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) ~~(5)~~ 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 1 of each even-numbered year ~~April 1~~ 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) ~~(6)~~ 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) ~~(7)~~ 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


228190

by state agencies.

(h) ~~(8)~~ Upon request, assist state agencies in the development of information technology-related legislative budget requests.

(i) ~~(9)~~ 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) ~~(10)~~ Provide operational management and oversight of the state data center established pursuant to s. 282.201, which includes:

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

2. ~~(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 Florida Digital Service may recommend other payment mechanisms to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives. Such mechanism may be implemented only if specifically authorized by the Legislature.

3. ~~(c)~~ Developing and implementing appropriate operating

228190

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

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

b.~~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.

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

d.~~4.~~ Requiring customer entities to validate that sufficient funds exist in the appropriate data processing appropriation category or will be transferred into the appropriate data processing appropriation category before implementation of a customer entity's request for a change in the type or level of service provided, if such change results in a net increase to the customer entity's cost for that fiscal year.

e.~~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.


228190

f.~~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 sub-subparagraph d. ~~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.

g.~~7.~~ Standardizing and consolidating procurement and contracting practices.

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

5.~~(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.

(k) 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


228190

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.

~~(f) Conducting an annual market analysis to determine whether the state's approach to the provision of data center services is the most effective and cost-efficient manner by which its customer entities can acquire such services, based on federal, state, and local government trends; best practices in service provision; and the acquisition of new and emerging technologies. The results of the market analysis shall assist the state data center in making adjustments to its data center service offerings.~~

(l) ~~(11)~~ 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.

(m) ~~(12)~~ 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.


228190

(n)1.~~(13)(a)~~ 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 $25 million or more and which impacts one or more other agencies. 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.~~(b)~~ When performing the project oversight function specified in subparagraph 1. ~~paragraph (a)~~, 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.

(o)~~(14)~~ 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


228190

cooperatively with these departments regarding the connections, interfaces, timing, or accommodations required to implement such projects.

(p) ~~(15)~~ 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 ~~a state agency~~ and results in adverse action against an entity ~~the state agency~~ or federal funding, work with the entity ~~state agency~~ to provide alternative standards, policies, or requirements that do not conflict with the federal regulation or requirement. The department, acting through the Florida Digital Service, shall annually report such alternative standards to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(q)1. ~~(16)(a)~~ 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. ~~1.~~ Identification of the information technology product and service categories to be included in state term contracts.

b. ~~2.~~ Requirements to be included in solicitations for state term contracts.

c. ~~3.~~ Evaluation criteria for the award of information technology-related state term contracts.

d. ~~4.~~ The term of each information technology-related state term contract.

e. ~~5.~~ The maximum number of vendors authorized on each state term contract.


228190

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

3.~~(c)~~ Answer vendor questions on information technology-related state term contract solicitations.

4.~~(d)~~ Ensure that the information technology policy established pursuant to subparagraph 1. ~~paragraph (a)~~ is included in all solicitations and contracts that are administratively executed by the department.

(r)~~(17)~~ Recommend potential methods for standardizing data across state agencies which will promote interoperability and reduce the collection of duplicative data.

(s)~~(18)~~ Recommend open data technical standards and terminologies for use by the enterprise ~~state agencies~~.

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

(2)(a) The Secretary of Management Services shall designate a state chief information officer, who shall administer the Florida Digital Service. The state chief information officer, 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


228190

substantive experience in data management, data governance, interoperability, and security.

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

(a) Create, not later than October 1, 2021, 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 October 1, 2021, 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

228190

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) Upon the adoption of the enterprise architecture standards in rule, the department, acting through the Florida Digital Service, may develop a process to:

(a) Receive written notice from the entities within the enterprise of any planned procurement of an information technology project that is subject to enterprise architecture standards.

(b) Participate in the development of specifications and recommend modifications to any planned procurement by state agencies so that the procurement complies with the enterprise architecture.

(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.

~~(19) Adopt rules to administer this section.~~

Section 5. Section 282.00515, Florida Statutes, is amended


228190

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 (s) and (3)(e) ~~s. 282.0051(2), (3), and (7)~~ or adopt alternative standards based on best practices and industry standards that allow for open data interoperability.

(2) If the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services adopts alternative standards in lieu of the enterprise architecture standards adopted pursuant to s. 282.0051, such department must notify the Governor, the President of the Senate, and the Speaker of the House of Representatives in writing of the adoption of the alternative standards and provide a justification for adoption of the alternative standards and explain how the agency will achieve open data interoperability.

(3) The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services~~, and~~ may contract with the department to provide or perform any of the services and functions described in s. 282.0051 ~~for the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services~~.

(4)(a) Nothing in this section or in s. 282.0051 requires the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services to integrate with information technology outside its own


228190

department or with the Florida Digital Service.

(b) 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 Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services.

Section 6. Paragraph (a) of subsection (3), paragraphs (d), (e), (g), and (j) of subsection (4), and subsection (5) of section 282.318, Florida Statutes, are amended to read:

282.318 Security of data and information technology.—

(3) The department is responsible for establishing standards and processes consistent with generally accepted best practices for information technology security, to include cybersecurity, and adopting rules that safeguard an agency's data, information, and information technology resources to ensure availability, confidentiality, and integrity and to mitigate risks. The department shall also:

(a) Designate an employee of the Florida Digital Service as the ~~a~~ state chief information security officer. The state chief information security officer ~~who~~ must have experience and expertise in security and risk management for communications and information technology resources.

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

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


228190

comply with the risk assessment methodology developed by the department and is confidential and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Florida Digital Service ~~Division of State Technology~~ 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.

(e) Develop, and periodically update, written internal policies and procedures, which include procedures for reporting information technology security incidents and breaches to the Cybercrime Office of the Department of Law Enforcement and the Florida Digital Service ~~Division of State Technology~~ 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 ~~Division of State Technology~~ within the department, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(g) Ensure that periodic internal audits and evaluations of the agency's information technology security program for the data, information, and information technology resources of the agency are conducted. The results of such audits and evaluations


228190

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 ~~Division of State Technology~~ within the department, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

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

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

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

3. Records held by a state agency which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents, including suspected or confirmed breaches, are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

a. Data or information, whether physical or virtual; or

b. Information technology resources, which includes:


228190

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

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

Such records shall be available to the Auditor General, the Florida Digital Service ~~Division of State Technology~~ 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. Such records may be made available to a local government, another state agency, or a federal agency for information technology security purposes or in furtherance of the state agency's official duties. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.

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


228190

unauthorized access to or the unauthorized modification, disclosure, or destruction of:

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

(b) Information technology resources, which include:

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

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

Such portions of records shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service ~~Division of State Technology~~ within the department, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. Such portions of records may be made available to a local government, another state agency, or a federal agency for information technology security purposes or in furtherance of the state agency's official duties. For purposes of this subsection, "external audit" means an audit that is conducted by an entity other than the state agency that is the subject of the audit. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.


228190

Section 7. Subsection (4) of section 287.0591, Florida Statutes, is amended to read:

287.0591 Information technology.—

(4) If the department issues a competitive solicitation for information technology commodities, consultant services, or staff augmentation contractual services, the Florida Digital Service ~~Division of State Technology~~ within the department shall participate in such solicitations.

Section 8. Paragraph (a) of subsection (3) of section 365.171, Florida Statutes, is amended to read:

365.171 Emergency communications number E911 state plan.—

(3) DEFINITIONS.—As used in this section, the term:

(a) "Office" means the Division of Telecommunications ~~State Technology~~ within the Department of Management Services, as designated by the secretary of the department.

Section 9. Paragraph (s) of subsection (3) of section 365.172, Florida Statutes, is amended to read:

365.172 Emergency communications number "E911."—

(3) DEFINITIONS.—Only as used in this section and ss. 365.171, 365.173, 365.174, and 365.177, the term:

(s) "Office" means the Division of Telecommunications ~~State Technology~~ within the Department of Management Services, as designated by the secretary of the department.

Section 10. Paragraph (a) of subsection (1) of section 365.173, Florida Statutes, is amended to read:

365.173 Communications Number E911 System Fund.—

(1) REVENUES.—

(a) Revenues derived from the fee levied on subscribers under s. 365.172(8) must be paid by the board into the State

228190

Treasury on or before the 15th day of each month. Such moneys must be accounted for in a special fund to be designated as the Emergency Communications Number E911 System Fund, a fund created in the Division of Telecommunications ~~State Technology~~, or other office as designated by the Secretary of Management Services.

Section 11. Subsection (5) of section 943.0415, Florida Statutes, is amended to read:

943.0415 Cybercrime Office.—There is created within the Department of Law Enforcement the Cybercrime Office. The office may:

(5) Consult with the Florida Digital Service ~~Division of State Technology~~ within the Department of Management Services in the adoption of rules relating to the information technology security provisions in s. 282.318.

Section 12. Effective January 1, 2021, section 559.952, Florida Statutes, is created to read:

559.952 Financial Technology Sandbox.—

(1) SHORT TITLE.—This section may be cited as the "Financial Technology Sandbox."

(2) CREATION OF THE FINANCIAL TECHNOLOGY SANDBOX.—There is created the Financial Technology Sandbox within the Office of Financial Regulation to allow financial technology innovators to test new products and services in a supervised, flexible regulatory sandbox using exceptions to specified general law and waivers of the corresponding rule requirements under defined conditions. The creation of a supervised, flexible regulatory sandbox provides a welcoming business environment for technology innovators and may lead to significant business growth.

(3) DEFINITIONS.—As used in this section, the term:


228190

(a) "Business entity" means a domestic corporation or other organized domestic entity with a physical presence, other than that of a registered office or agent or virtual mailbox, in this state.

(b) "Commission" means the Financial Services Commission.

(c) "Consumer" means a person in this state, whether a natural person or a business organization, who purchases, uses, receives, or enters into an agreement to purchase, use, or receive an innovative financial product or service made available through the Financial Technology Sandbox.

(d) "Control person" means an individual, a partnership, a corporation, a trust, or other organization that possesses the power, directly or indirectly, to direct the management or policies of a company, whether through ownership of securities, by contract, or through other means. A person is presumed to control a company if, with respect to a particular company, that person:

1. Is a director, a general partner, or an officer exercising executive responsibility or having similar status or functions;

2. Directly or indirectly may vote 10 percent or more of a class of a voting security or sell or direct the sale of 10 percent or more of a class of voting securities; or

3. In the case of a partnership, may receive upon dissolution or has contributed 10 percent or more of the capital.

(e) "Corresponding rule requirements" means the commission rules, or portions thereof, which implement the general laws enumerated in paragraph (4)(a).

228190

(f) "Financial product or service" means a product or service related to a consumer finance loan, as defined in s. 516.01, or a money transmitter or payment instrument seller, as those terms are defined in s. 560.103, including mediums of exchange that are in electronic or digital form, which is subject to the general laws enumerated in paragraph (4)(a) and corresponding rule requirements and which is under the jurisdiction of the office.

(g) "Financial Technology Sandbox" means the program created by this section which allows a licensee to make an innovative financial product or service available to consumers during a sandbox period through exceptions to general laws and waivers of corresponding rule requirements.

(h) "Innovative" means new or emerging technology, or new uses of existing technology, which provide a product, service, business model, or delivery mechanism to the public and which are not known to have a comparable offering in this state outside the Financial Technology Sandbox.

(i) "Licensee" means a business entity that has been approved by the office to participate in the Financial Technology Sandbox.

(j) "Office" means, unless the context clearly indicates otherwise, the Office of Financial Regulation.

(k) "Sandbox period" means the initial 24-month period in which the office has authorized a licensee to make an innovative financial product or service available to consumers, and any extension granted pursuant to subsection (7).

(4) EXCEPTIONS TO GENERAL LAW AND WAIVERS OF RULE REQUIREMENTS.—

228190

(a) Notwithstanding any other law, upon approval of a Financial Technology Sandbox application, the following provisions and corresponding rule requirements are not applicable to the licensee during the sandbox period:

1. Section 516.03(1), except for the application fee, the investigation fee, the requirement to provide the social security numbers of control persons, evidence of liquid assets of at least $25,000, and the office's authority to investigate the applicant's background. The office may prorate the license renewal fee for an extension granted under subsection (7).

2. Section 516.05(1) and (2), except that the office shall investigate the applicant's background.

3. Section 560.109, only to the extent that the section requires the office to examine a licensee at least once every 5 years.

4. Section 560.118(2).

5. Section 560.125(1), only to the extent that subsection would prohibit a licensee from engaging in the business of a money transmitter or payment instrument seller during the sandbox period.

6. Section 560.125(2), only to the extent that subsection would prohibit a licensee from appointing an authorized vendor during the sandbox period. Any authorized vendor of such a licensee during the sandbox period remains liable to the holder or remitter.

7. Section 560.128.

8. Section 560.141, except for s. 560.141(1)(a)1., 3., 7.-10. and (b), (c), and (d).

9. Section 560.142(1) and (2), except that the office may

prorate, but may not entirely eliminate, the license renewal fees in s. 560.143 for an extension granted under subsection (7).

10. Section 560.143(2), only to the extent necessary for proration of the renewal fee under subparagraph 9.

11. Section 560.204(1), only to the extent that subsection would prohibit a licensee from engaging in, or advertising that it engages in, the selling or issuing of payment instruments or in the activity of a money transmitter during the sandbox period.

12. Section 560.205(2).

13. Section 560.208(2).

14. Section 560.209, only to the extent that the office may modify, but may not entirely eliminate, the net worth, corporate surety bond, and collateral deposit amounts required under that section. The modified amounts must be in such lower amounts that the office determines to be commensurate with the factors under paragraph (5)(c) and the maximum number of consumers authorized to receive the financial product or service under this section.

(b) The office may approve a Financial Technology Sandbox application if one or more of the general laws enumerated in paragraph (a) currently prevent the innovative financial product or service from being made available to consumers and if all other requirements of this section are met.

(c) A licensee may conduct business through electronic means, including through the Internet or a software application.

(5) FINANCIAL TECHNOLOGY SANDBOX APPLICATION; STANDARDS FOR APPROVAL.—

(a) Before filing an application for licensure under this

228190

section, a substantially affected person may seek a declaratory statement pursuant to s. 120.565 regarding the applicability of a statute, a rule, or an agency order to the petitioner's particular set of circumstances or a variance or waiver of a rule pursuant to s. 120.542.

(b) Before making an innovative financial product or service available to consumers in the Financial Technology Sandbox, a business entity must file with the office an application for licensure under the Financial Technology Sandbox. The commission shall, by rule, prescribe the form and manner of the application and how the office will evaluate and apply each of the factors specified in paragraph (c).

1. The application must specify each general law enumerated in paragraph (4)(a) which currently prevents the innovative financial product or service from being made available to consumers and the reasons why those provisions of general law prevent the innovative financial product or service from being made available to consumers.

2. The application must contain sufficient information for the office to evaluate the factors specified in paragraph (c).

3. An application submitted on behalf of a business entity must include evidence that the business entity has authorized the person to submit the application on behalf of the business entity intending to make an innovative financial product or service available to consumers.

4. The application must specify the maximum number of consumers, which may not exceed the number of consumers specified in paragraph (f), to whom the applicant proposes to provide the innovative financial product or service.


228190

5. The application must include a proposed draft of the statement or statements meeting the requirements of paragraph (6)(b) which the applicant proposes to provide to consumers.

(c) The office shall approve or deny in writing a Financial Technology Sandbox application within 60 days after receiving the completed application. The office and the applicant may jointly agree to extend the time beyond 60 days. Consistent with this section, the office may impose conditions on any approval. In deciding whether to approve or deny an application for licensure, the office must consider each of the following:

1. The nature of the innovative financial product or service proposed to be made available to consumers in the Financial Technology Sandbox, including all relevant technical details.

2. The potential risk to consumers and the methods that will be used to protect consumers and resolve complaints during the sandbox period.

3. The business plan proposed by the applicant, including company information, market analysis, and financial projections or pro forma financial statements, and evidence of the financial viability of the applicant.

4. Whether the applicant has the necessary personnel, adequate financial and technical expertise, and a sufficient plan to test, monitor, and assess the innovative financial product or service.

5. Whether any control person of the applicant, regardless of adjudication, has pled no contest to, has been convicted or found guilty of, or is currently under investigation for fraud, a state or federal securities violation, a property-based

228190

offense, or a crime involving moral turpitude or dishonest dealing, in which case the application to the Financial Technology Sandbox must be denied.

6. A copy of the disclosures that will be provided to consumers under paragraph (6)(b).

7. The financial responsibility of the applicant and any control person, including whether the applicant or any control person has a history of unpaid liens, unpaid judgments, or other general history of nonpayment of legal debts, including, but not limited to, having been the subject of a petition for bankruptcy under the United States Bankruptcy Code within the past 7 calendar years.

8. Any other factor that the office determines to be relevant.

(d) The office may not approve an application if:

1. The applicant had a prior Financial Technology Sandbox application that was approved and that related to a substantially similar financial product or service;

2. Any control person of the applicant was substantially involved in the development, operation, or management with another Financial Technology Sandbox applicant whose application was approved and whose application related to a substantially similar financial product or service; or

3. The applicant or any control person has failed to affirmatively demonstrate financial responsibility.

(e) Upon approval of an application, the office shall notify the licensee that the licensee is exempt from the provisions of general law enumerated in paragraph (4)(a) and the corresponding rule requirements during the sandbox period. The

228190

office shall post on its website notice of the approval of the application, a summary of the innovative financial product or service, and the contact information of the licensee.

(f) The office, on a case-by-case basis, shall specify the maximum number of consumers authorized to receive an innovative financial product or service, after consultation with the Financial Technology Sandbox applicant. The office may not authorize more than 15,000 consumers to receive the financial product or service until the licensee has filed the first report required under subsection (8). After the filing of that report, if the licensee demonstrates adequate financial capitalization, risk management processes, and management oversight, the office may authorize up to 25,000 consumers to receive the financial product or service.

(g) A licensee has a continuing obligation to promptly inform the office of any material change to the information provided under paragraph (b).

(6) OPERATION OF THE FINANCIAL TECHNOLOGY SANDBOX.—

(a) A licensee may make an innovative financial product or service available to consumers during the sandbox period.

(b)1. Before a consumer purchases, uses, receives, or enters into an agreement to purchase, use, or receive an innovative financial product or service through the Financial Technology Sandbox, the licensee must provide a written statement of all of the following to the consumer:

a. The name and contact information of the licensee.

b. That the financial product or service has been authorized to be made available to consumers for a temporary period by the office, under the laws of this state.


228190

c. That the state does not endorse the financial product or service.

d. That the financial product or service is undergoing testing, may not function as intended, and may entail financial risk.

e. That the licensee is not immune from civil liability for any losses or damages caused by the financial product or service.

f. The expected end date of the sandbox period.

g. The contact information for the office and notification that suspected legal violations, complaints, or other comments related to the financial product or service may be submitted to the office.

h. Any other statements or disclosures required by rule of the commission which are necessary to further the purposes of this section.

2. The written statement under subparagraph 1. must contain an acknowledgment from the consumer, which must be retained for the duration of the sandbox period by the licensee.

(c) The office may enter into an agreement with a state, federal, or foreign regulatory agency to allow licensees under the Financial Technology Sandbox to make their products or services available in other jurisdictions. The commission shall adopt rules to implement this paragraph.

(d) The office may examine the records of a licensee at any time, with or without prior notice.

(7) EXTENSIONS AND CONCLUSION OF SANDBOX PERIOD.—

(a) A licensee may apply for one extension of the initial 24-month sandbox period for 12 additional months for a purpose

228190

specified in subparagraph (b)1. or subparagraph (b)2. A complete application for an extension must be filed with the office at least 90 days before the conclusion of the initial sandbox period. The office shall approve or deny the application for extension in writing at least 35 days before the conclusion of the initial sandbox period. In determining whether to approve or deny an application for extension of the sandbox period, the office must, at a minimum, consider the current status of the factors previously considered under paragraph (5)(c).

(b) An application for an extension under paragraph (a) must cite one of the following reasons as the basis for the application and must provide all relevant supporting information:

1. Amendments to general law or rules are necessary to offer the innovative financial product or service in this state permanently.

2. An application for a license that is required in order to offer the innovative financial product or service in this state permanently has been filed with the office and approval is pending.

(c) At least 30 days before the conclusion of the initial 24-month sandbox period or the extension, whichever is later, a licensee shall provide written notification to consumers regarding the conclusion of the initial sandbox period or the extension and may not make the financial product or service available to any new consumers after the conclusion of the initial sandbox period or the extension, whichever is later, until legal authority outside of the Financial Technology Sandbox exists for the licensee to make the financial product or

service available to consumers. After the conclusion of the sandbox period or the extension, whichever is later, the business entity formerly licensed under the Financial Technology Sandbox may:

1. Collect and receive money owed to the business entity or pay money owed by the business entity, based on agreements with consumers made before the conclusion of the sandbox period or the extension.

2. Take necessary legal action.

3. Take other actions authorized by commission rule which are not inconsistent with this section.

(8) REPORT.—A licensee shall submit a report to the office twice a year as prescribed by commission rule. The report must, at a minimum, include financial reports and the number of consumers who have received the financial product or service.

(9) CONSTRUCTION.—A business entity whose Financial Technology Sandbox application is approved under this section:

(a) Is licensed under chapter 516, chapter 560, or both chapters 516 and 560, as applicable to the business entity's activities.

(b) Is subject to any provision of chapter 516 or chapter 560 not specifically excepted under paragraph (4)(a), as applicable to the business entity's activities, and must comply with such provisions.

(c) May not engage in activities authorized under part III of chapter 560, notwithstanding s. 560.204(2).

(10) VIOLATIONS AND PENALTIES.—

(a) A licensee who makes an innovative financial product or service available to consumers in the Financial Technology


228190

Sandbox remains subject to:

1. Civil damages for acts and omissions arising from or related to any innovative financial product or services provided or made available by the licensee or relating to this section.

2. All criminal and consumer protection laws and any other statute not specifically excepted under paragraph (4)(a).

(b)1. The office may, by order, revoke or suspend a licensee's approval to participate in the Financial Technology Sandbox if:

a. The licensee has violated or refused to comply with this section, any statute not specifically excepted under paragraph (4)(a), a rule of the commission that has not been waived, an order of the office, or a condition placed by the office on the approval of the licensee's Financial Technology Sandbox application;

b. A fact or condition exists that, if it had existed or become known at the time that the Financial Technology Sandbox application was pending, would have warranted denial of the application or the imposition of material conditions;

c. A material error, false statement, misrepresentation, or material omission was made in the Financial Technology Sandbox application; or

d. After consultation with the licensee, the office determines that continued testing of the innovative financial product or service would:

(I) Be likely to harm consumers; or

(II) No longer serve the purposes of this section because of the financial or operational failure of the financial product or service.

228190

2. Written notice of a revocation or suspension order made under subparagraph 1. must be served using any means authorized by law. If the notice relates to a suspension, the notice must include any condition or remedial action that the licensee must complete before the office lifts the suspension.

(c) The office may refer any suspected violation of law to an appropriate state or federal agency for investigation, prosecution, civil penalties, and other appropriate enforcement action.

(d) If service of process on a licensee is not feasible, service on the office is deemed service on the licensee.

(11) RULES AND ORDERS.—

(a) The commission shall adopt rules to administer this section before approving any application under this section.

(b) The office may issue all necessary orders to enforce this section and may enforce these orders in accordance with chapter 120 or in any court of competent jurisdiction. These orders include, but are not limited to, orders for payment of restitution for harm suffered by consumers as a result of an innovative financial product or service.

Section 13. For the 2020-2021 fiscal year, the sum of $50,000 in nonrecurring funds is appropriated from the Administrative Trust Fund to the Office of Financial Regulation to implement s. 559.952, Florida Statutes, as created by this act.

Section 14. The creation of s. 559.952, Florida Statutes, and the appropriation to implement s. 559.952, Florida Statutes, by this act shall take effect only if SB 1872 or similar legislation takes effect and if such legislation is adopted in


228190

the same legislative session or an extension thereof and becomes a law.

Section 15. Except as otherwise expressly provided in this act, this act shall take effect July 1, 2020.

========== T I T L E A M E N D M E N T ==========

And the title is amended as follows:

Delete everything before the enacting clause and insert:

A bill to be entitled

An act relating to technology innovation; amending s. 20.22, F.S.; establishing the Florida Digital Service and the Division of Telecommunications within the Department of Management Services; abolishing the Division of State Technology within the department; amending s. 110.205, F.S.; exempting the state chief data officer and the state chief information security officer within the Florida Digital Service from the Career Service System; providing for the salary and benefits of such positions to be set by the department; amending s. 282.0041, F.S.; defining terms; revising the definition of the term "open data"; amending s. 282.0051, F.S.; revising information technology-related powers, duties, and functions of the department acting through the Florida Digital Service; specifying the designation of the state chief information officer and the state chief data officer; specifying qualifications for such positions; specifying requirements, contingent upon

228190

legislative appropriation, for the department; authorizing the department to develop a certain process; prohibiting the department from retrieving or disclosing any data without a certain shared-data agreement in place; specifying rulemaking authority for the department; amending s. 282.00515, F.S.; requiring the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services to notify the Governor and the Legislature and provide a certain justification and explanation if such agency adopts alternative standards to certain enterprise architecture standards; providing construction; prohibiting the department from retrieving or disclosing any data without a certain shared-data agreement in place; conforming a cross-reference; amending ss. 282.318, 287.0591, 365.171, 365.172, 365.173, and 943.0415, F.S.; conforming provisions to changes made by the act; creating s. 559.952, F.S.; providing a short title; creating the Financial Technology Sandbox within the Office of Financial Regulation; defining terms; requiring the office, if certain conditions are met, to grant a license to a Financial Technology Sandbox applicant, grant exceptions to specified provisions of general law relating to consumer finance loans and money services businesses, and grant waivers of certain rules; authorizing a substantially affected person to seek a declaratory statement before applying to the Financial

Technology Sandbox; specifying application requirements and procedures; specifying requirements and procedures for the office in reviewing and approving or denying applications; providing requirements for the office in specifying the number of the consumers authorized to receive an innovative financial product or service; specifying authorized actions of, limitations on, and requirements for licensees operating in the Financial Technology Sandbox; requiring licensees to make a specified disclosure to consumers; authorizing the office to enter into certain agreements with other regulatory agencies; authorizing the office to examine licensee records; authorizing a licensee to apply for one extension of an initial sandbox period for a certain timeframe; specifying requirements and procedures for applying for an extension; specifying requirements and procedures for, and authorized actions of, licensees when concluding a sandbox period or extension; requiring licensees to submit certain reports to the office at specified intervals; providing construction; specifying the liability of a licensee; authorizing the office to take certain disciplinary actions against a licensee under certain circumstances; providing construction relating to service of process; specifying the rulemaking authority of the Financial Services Commission; providing the office authority to issue orders and enforce the orders; providing an appropriation; providing that specified provisions of

228190

the act are contingent upon passage of other provisions addressing public records; providing effective dates.