By Senator Hutson

7-01682B-20 20201870__

A bill to be entitled

An act relating to technological development; amending s. 20.22, F.S.; renaming the Division of State Technology within the Department of Management Services; adding the Florida Digital Service to the department; amending s. 282.0051, F.S.; establishing the Florida Digital Service within the department; providing definitions; transferring specified powers, duties, and functions of the department to the Florida Digital Service and revising such powers, duties, and functions; providing appointments and requirements of the state chief information officer and chief data officer of the Florida Digital Service; requiring the Florida Digital Service to develop an enterprise architecture for all state departments and agencies; providing requirements for such enterprise architecture; providing duties of the Florida Digital Service under certain circumstances; authorizing the Florida Digital Service to enforce the enterprise architecture by specified means; 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 Program; providing definitions; providing certain waivers of requirements to specified persons under certain circumstances; requiring an application for the program for persons who want to make innovative financial products or services available to consumers;

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

providing application requirements; requiring the Office of Financial Regulation to pay an annual fee to the Department of Law Enforcement for a specified purpose; providing standards for application approval; requiring the Commissioner of Financial Regulation and any other persons exercising such powers to perform certain actions upon approval of an application; requiring posting of consumer protection bonds; providing disposition of such bonds under a specified circumstance; providing operation of the program; providing extensions and conclusion of sandbox periods; requiring persons who make innovative financial products or services available to consumers to submit a report; providing construction; providing that such persons are not immune from civil damages and are subject to criminal and consumer protection laws; providing penalties; providing service of process; requiring the office and the commissioner to adopt rules; authorizing the commissioner to issue certain orders and to enforce them in court; authorizing the commissioner to issue and enforce orders for payment of restitution and enforcement of certain bonds; requiring the commissioner to use certain proceeds for a specified purpose; providing an effective date.

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

Section 1. Subsection (2) of section 20.22, Florida

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

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 within~~ The Department of Management Services shall consist of the following ~~are established~~:

(a) The Facilities Program.

(b) The Division of Telecommunications ~~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) The Workforce Program.

(d)1. The Support Program.

2. The Federal Property Assistance Program.

(e) The Administration Program.

(f) The Division of Administrative Hearings.

(g) The Division of Retirement.

(h) The Division of State Group Insurance.

(i) The Florida Digital Service.

Section 2. Section 282.0051, Florida Statutes, is amended to read:

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

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

the Florida Digital Service within the department to create innovative solutions that securely modernize and optimize state government and achieve value through digital transformation and interoperability.

(1) As used in this section, the term:

(a) "Digital identity verifier" means a digital system capable of securely authenticating the identity of an external agent, including a person, an organization, an application, or a device, without physically storing the necessary data to validate a digital identity.

(b) "Enterprise" means the state or the entirety of state government and its subdivisions.

(c) "Enterprise architecture" means a comprehensive operational framework that contemplates the needs and assets of the enterprise to create a unified information technology environment.

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

(e) "Qualified entity" means a public or private entity or individual that enters into a binding agreement with the Florida Digital Service, meets usage criteria, agrees to terms and conditions, and is subsequently and prescriptively authorized by the Florida Digital Service to access digital assets as defined in the agreement.

(2) The Florida Digital Service ~~department~~ 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.

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

(b) ~~(2)~~ 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 Florida Digital Service ~~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 Florida Digital Service ~~department~~ 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 a technology component with a total project cost ~~costs~~ of $10 million or more and that are funded in the General Appropriations Act or any other law. The Florida Digital Service ~~department~~ shall report at least

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

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 Florida Digital Service ~~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 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 Florida Digital Service ~~department~~ shall biennially on 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 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 Florida Digital Service ~~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 or payment 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.

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

a. ~~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.

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.

~~7. Standardizing and consolidating procurement and~~

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

~~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.

~~(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.~~

(k)~~(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.

(l)~~(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.

(m)1.~~(13)(a)~~ Notwithstanding any other law, provide project oversight on any ~~information technology~~ project of the Department of Financial Services with a technology component, 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 Florida Digital Service ~~department~~.

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 Florida Digital Service ~~department~~ identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in the project plan. The report shall include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project and a recommendation for corrective actions required, including suspension or termination of the project.

(n)~~(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 cooperatively with these departments regarding the connections,

interfaces, timing, or accommodations required to implement such projects.

(o) ~~(15)~~ If adherence to standards or policies adopted by or established pursuant to this section causes conflict with federal regulations or requirements imposed on a state agency and results in adverse action against the state agency or federal funding, work with the state agency to provide alternative standards, policies, or requirements that do not conflict with the federal regulation or requirement. The Florida Digital Service ~~department~~ shall annually report such alternative standards to the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(p) Follow best purchasing practices of state procurement to the extent practicable for the purpose of creating innovative solutions that securely modernize and optimize state government to achieve value through digital transformation and to use best business practices employed by the private sector, notwithstanding chapter 287 and the authority of the department.

~~(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:~~

~~1. Identification of the information technology product and service categories to be included in state term contracts.~~

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

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

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

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

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

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

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

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

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

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

(3)(a) The Secretary of Management Services shall appoint a state chief information officer to head the Florida Digital Service. 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.

(b) The state chief information officer shall appoint a chief data officer, who shall report to the state chief

information officer. The chief data officer must be a proven, effective administrator who must have at least 10 years of experience in data management, data governance, interoperability, and security. The chief data officer is included in the Senior Management Service. As used in this paragraph, the term "data governance" means the practice of organizing, classifying, securing, and implementing policies, procedures, and standards for the effective use of an organization's structured and unstructured information assets.

(4) The Florida Digital Service shall develop an enforceable and comprehensive enterprise architecture for all state departments and agencies which:

(a) Recognizes the unique needs of all stakeholders and results in the publication of standards and terminologies, procurement guidelines, and the facilitation of digital interoperability.

(b) Establishes a comprehensive framework that accounts for all of the needs and responsibilities of a department and agency while defining how technology benefits and serves the overall mission of both entities.

(c) Addresses how hardware, operating systems, legacy systems, and programming and networking solutions may be used or improved to achieve current and future objectives.

(d) Allows the enterprise architecture to be enforced, as appropriate, to ensure stewardship of tax dollars.

(5) Upon the required production of information from the stakeholders of the enterprise architecture, the Florida Digital Service shall:

(a) Create and maintain a comprehensive indexed data

catalog that lists what data elements are housed within which department or agency and in which legacy system or application.

(b) Develop and publish for each state department and agency a data dictionary that reflects the nomenclature as existing in the comprehensive indexed data catalog.

(c) Create and maintain an indexed integration catalog that includes all integration tools currently used by each state department and agency.

(d) Review, confirm, and document operational use cases with all stakeholders across the enterprise architecture, including the Legislature and all state departments and agencies.

(e) Identify core functionality use cases reliant on digital and data infrastructure.

(f) Develop, collaboratively with stakeholders, solutions for authorized, mandated, or encouraged use cases within the enterprise.

(g) Develop, publish, and manage an application programming interface to facilitate integration throughout the enterprise.

(h) Facilitate collaborative analysis of enterprise architecture data to improve service delivery.

(i) Provide a testing environment in which any newly developed solution can be tested for compliance within the enterprise architecture and for functionality assurance before deployment.

(j) Create the functionality necessary for a secure ecosystem of data interoperability that is compliant with the enterprise architecture and allows for governmental and nongovernmental stakeholders to access the data store by:

1. Competitively procuring a credential service provider. As used in this subparagraph, the term "credential service provider" means an electronic credential provider that supplies secure credential services based on open standards for identity management and verification to qualified entities.

2. Upon the signing of the enterprise architecture terms of service and privacy policies, providing to qualified entities and digital identity verifiers appropriate access to the data store to facilitate authorized integrations to collaboratively, less expensively, or at no taxpayer cost, solve enterprise use cases.

(k) Architect and deploy applications or solutions to existing department and agency obligations in a controlled and phased approach, including, but not limited to:

1. Digital licenses, including full identification management.

2. Interoperability that contains the data functionality to enable supervisors of elections to authenticate voter eligibility in real time at the point of service.

3. The criminal justice database.

4. Motor vehicle insurance cancellation integration between insurers and the Department of Highway Safety and Motor Vehicles.

5. Interoperability solutions between agencies, including, but not limited to, 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.

(6) The Florida Digital Service may enforce the enterprise

architecture by:

(a) Receiving written notice of any planned or existing procurement of digital solutions which is subject to governance by the enterprise architecture, which includes:

1. An attestation of compliance with the enterprise architecture.

2. A list of integrations tools needed.

3. Enterprise stakeholders actually or potentially involved or affected by the procurement.

4. Resources that would reduce the cost or increase the speed to deployment.

(b) Intervening in any procurement that does not comply with the enterprise architecture after the Florida Digital Service provided notice of noncompliance to relevant stakeholders through the following acts:

1. Delaying the procurement until it complies with the enterprise architecture.

2. Providing recommendations to cure the portions of the procurement which do not comply with the enterprise architecture.

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

Section 3. Paragraph (a) of subsection (3), paragraphs (d), (e), (g), and (j) of subsection (4), and paragraph (b) of 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 a state chief information security officer for the Florida Digital Service, who must be a proven, effective administrator and 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 ~~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 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

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

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 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 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:

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

(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.

Section 4. 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 5. 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 6. 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 7. 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 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 8. 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 9. Section 559.952, Florida Statutes, is created to read:

559.952 Financial Technology Sandbox Act.—

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

(2) CREATION OF THE FINANCIAL TECHNOLOGY SANDBOX PROGRAM.—There is created the Financial Technology Sandbox Program within the Office of Financial Regulation to allow financial technology innovators to test new products and services in a supervised, flexible regulatory sandbox, using waivers of specified general law and 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:

(a) "Blockchain" means a digital record of online transactions that are stored chronologically and obtained through consensus and that are decentralized and mathematically verified in nature.

(b) "Commissioner" means the Director of the Office of Financial Regulation, also known as the Commissioner of Financial Regulation, and any other person lawfully exercising such powers.

(c) "Consumer" means a person in this state, whether a natural person or a business entity, who purchases, uses, or enters into an agreement to receive an innovative financial

product or service made available through the Financial Technology Sandbox.

(d) "Financial product or service" means a product or service related to finance, including banking, securities, consumer credit, or money transmission, which is traditionally subject to general law or rule requirements in the chapters enumerated in paragraph (4)(a) and which is under the jurisdiction of the commissioner.

(e) "Financial Technology Sandbox" means, unless the context clearly indicates otherwise, the program created in this section, which allows a person to make an innovative financial product or service available to consumers during a sandbox period through a waiver of existing general laws and rule requirements, or portions thereof, as determined by the commissioner.

(f) "Innovative" means new or emerging technology, or new uses of existing technology, including blockchain technology, which provides a product, service, business model, or delivery mechanism to the public and has no substantially comparable, widely available analog in this state.

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

(h) "Sandbox period" means the period, initially not longer than 24 months, in which the commissioner has:

1. Authorized an innovative financial product or service to be made available to consumers.

2. Granted the person who makes the innovative financial product or service available a waiver of general law or rule requirements, as determined by the commissioner, so that the

authorization under subparagraph 1. is possible.

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

(a) Notwithstanding any other provision of law, upon approval of a Financial Technological Sandbox application, the commissioner may grant an applicant a waiver of a requirement, or a portion thereof, which is imposed by a general law or rule in any following chapter or part thereof, if all of the conditions in paragraph (b) are met:

1. Chapter 516, consumer finance.

2. Chapter 517, securities transactions.

3. Chapter 520, retail installment sales.

4. Chapter 537, title loans.

5. Part I or part II of chapter 560, general provisions of money services businesses or payment instruments and funds transmission.

6. Chapter 655, financial institutions generally.

7. Chapter 657, credit unions.

8. Chapter 658, banks and trust companies.

9. Chapter 660, trust business.

10. Chapter 662, family trust companies.

11. Chapter 663, international banking.

(b) The commissioner may grant, during a sandbox period, a waiver of a requirement, or a portion thereof, imposed by a general law or rule in any chapter enumerated in paragraph (a), if all of the following conditions are met:

1. The general law or rule does not currently authorize the innovative financial product or service to be made available to consumers.

2. The waiver is not broader than necessary to accomplish

the purposes and standards specified in this section, as determined by the commissioner.

3. No provision relating to the liability of an incorporator, director, or officer of the applicant is eligible for a waiver.

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

(a) Before making an innovative financial product or service available to consumers in the Financial Technology Sandbox, a person must file an application with the commissioner. The commissioner shall, by rule, prescribe the form and manner of the application.

1. In the application, the person must specify the general law or rule requirements for which a waiver is sought, and the reasons why these requirements prohibit the innovative financial product or service from being made available to consumers.

2. The application must also contain the information specified in subparagraphs (e)1.-7.

(b) A business entity filing an application under this section must be 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.

(c) Before an employee applies on behalf of a business entity intending to make an innovative financial product or service available to consumers, the employee must obtain the consent of the business entity.

(d) The applicant must submit fingerprints for each individual filing an application under this section and each individual who is substantially involved in the development,

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

operation, or management of the innovative financial product or service for live-scan processing in accordance with rules adopted by the office.

1. The fingerprints may be submitted through a third-party vendor authorized by the Department of Law Enforcement to provide live-scan fingerprinting.

2. The Department of Law Enforcement must conduct the state criminal history background check, and a federal criminal history background check must be conducted through the Federal Bureau of Investigation.

3. All fingerprints submitted to the Department of Law Enforcement must be submitted electronically and entered into the statewide automated fingerprint identification system established in s. 943.05(2)(b) and available for use in accordance with s. 943.05(2)(g) and (h). The office shall pay an annual fee to the Department of Law Enforcement to participate in the system and shall inform the Department of Law Enforcement of any person whose fingerprints no longer must be retained.

4. The office shall review the results of the state and federal criminal history background checks and determine whether the applicant meets the office’s requirements.

5. For purposes of this paragraph, fingerprints are not required to be submitted if the applicant is a publicly traded corporation or is exempted under s. 560.104(1). The term “publicly traded” means a stock is currently traded on a national securities exchange registered with the Securities and Exchange Commission or traded on an exchange in a country other than the United States which is regulated by a regulator equivalent to the Securities and Exchange Commission and the

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

disclosure and reporting requirements of such regulator are substantially similar to those of the Securities and Exchange Commission.

(e) The commissioner shall approve or deny in writing a Financial Technology Sandbox application within 60 days after receiving the completed application. The commissioner and the applicant may jointly agree to extend the time beyond 60 days. The commissioner may impose conditions on any approval, consistent with this section. In deciding to approve or deny an application, the commissioner 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, which may include whether the product or service uses blockchain technology.

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 a statement of arranged capital.

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 person substantially involved in the development, operation, or management of the innovative financial product or service has been convicted of, or is currently under investigation for, fraud, a state or federal

securities violation, or any property-based offense.

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

7. Any other factor that the commissioner determines to be relevant.

(f) If an application is approved pursuant to paragraph (e), the commissioner shall specify the general law or rule requirements, or portions thereof, for which a waiver is granted and the length of the initial sandbox period, not to exceed 24 months. The commissioner shall post on the office's website notice of the approval of the application, a summary of the innovative financial product or service, and the contact information of the person making the financial product or service available.

(g) A person whose Financial Technology Sandbox application is approved shall post a consumer protection bond with the commissioner as security for potential losses suffered by consumers. The commissioner shall determine the bond amount, which must be at least $10,000 and commensurate with the risk profile of the innovative financial product or service. The commissioner may require that a bond under this paragraph be increased or decreased at any time based on the risk profile. Unless a bond is enforced under subparagraph (11)(b)2., the commissioner shall cancel the bond or allow it to expire 2 years after the date of the conclusion of the sandbox period.

(6) OPERATION OF THE FINANCIAL TECHNOLOGY SANDBOX.—

(a) A person whose Financial Technology Sandbox application is approved may make an innovative financial product or service available to consumers during the sandbox period.

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

(b) The commissioner may, on a case-by-case basis, specify the maximum number of consumers authorized to receive an innovative financial product or service, after consultation with the person who makes the financial product or service available to consumers.

(c)1. Before a consumer purchases or enters into an agreement to receive an innovative financial product or service through the Financial Technology Sandbox, the person making the financial product or service available must provide a written statement of all of the following to the consumer:

a. The name and contact information of the person making the financial product or service available to consumers.

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

c. That the state does not endorse the financial product or service and is not subject to liability for losses or damages caused by 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 person making the product or service available to consumers 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 name and contact information of the commissioner, and notification that suspected legal violations, complaints, or other comments related to the financial product or service may be submitted to the commissioner.

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

2. The written statement must contain an acknowledgement from the consumer, which must be retained for the duration of the sandbox period by the person making the financial product or service available.

(d) The commissioner may enter into an agreement with a state, federal, or foreign regulatory agency to allow persons:

1. Who make an innovative financial product or service available in this state through the Financial Technology Sandbox to make their products or services available in other jurisdictions.

2. Who operate in similar financial technology sandboxes in other jurisdictions to make innovative financial products and services available in this state under the standards of this section.

(e)1. A person whose Financial Technology Sandbox application is approved by the commissioner shall maintain comprehensive records relating to the innovative financial product or service. The person shall keep these records for at least 5 years after the conclusion of the sandbox period. The commissioner may specify by rule additional records requirements.

2. The commissioner may examine the records maintained under subparagraph 1. at any time, with or without notice. All direct and indirect costs of an examination conducted under this subparagraph shall be paid by the person making the innovative financial product or service available to consumers.

(7) EXTENSIONS AND CONCLUSION OF SANDBOX PERIOD.—

(a) A person who is authorized to make an innovative financial product or service available to consumers may apply for an extension of the initial sandbox period for up to 12 additional months, with the option of multiple extensions for the purpose of pursuing licensure from the office. An application for an extension must be made at least 60 days before the conclusion of the initial sandbox period or, if the extension is a second or subsequent extension, at least 60 days before the conclusion of the current extension. The commissioner shall approve or deny the application for extension in writing at least 35 days before the conclusion of the initial sandbox period or the conclusion of the current extension, if applicable.

(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 that:

1. Amendments to general law or rules are necessary to conduct financial technology business in this state permanently.

2. An application for a license or other authorization required to conduct business in this state has been filed with the appropriate office, and approval is pending.

(c) Unless granted an extension under this subsection at least 30 days before the conclusion of the initial sandbox period or the current extension, a person who makes an innovative financial product or service available shall provide written notification to consumers regarding the conclusion of the initial sandbox period or the current 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 current extension until legal authority outside of the Financial Technology Sandbox exists to make the financial product or service available to consumers. The person shall wind down operations with existing consumers within 60 days after the conclusion of the sandbox period or the current extension, except that, after the 60th day, the person may:

1. Collect and receive money owed to the person and service loans made by the person, based on agreements with consumers made before the conclusion of the sandbox period or the current extension.

2. Take necessary legal action.

3. Take other actions authorized by rule by the commissioner which are not inconsistent with this subsection.

(8) REPORT.—A person authorized to make an innovative financial product or service available to consumers under subsection (5) shall submit a report to the commissioner twice a year as prescribed by rule.

(9) CONSTRUCTION.—

(a) A person whose Financial Technology Sandbox application is approved shall be deemed to possess an appropriate license under any general law requiring state licensure or authorization.

(b) Authorization to make an innovative financial product or service available to consumers under subsection (5) does not create a property right.

(c) The state does not endorse the financial product or service and is not subject to liability for losses or damages

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

caused by the financial product or service.

(10) VIOLATIONS AND PENALTIES.—

(a) A person who makes an innovative financial product or service available to consumers in the Financial Technology Sandbox is:

1. Not immune from civil damages for acts and omissions relating to this section.

2. Subject to all criminal and consumer protection laws.

(b)1. The commissioner may, by order, revoke or suspend authorization granted to a person to make an innovative financial product or service available to consumers if:

a. The person has violated or refused to comply with this section or any rule, order, or decision adopted by the commissioner;

b. A fact or condition exists that, if it had existed or become known at the time of the Financial Technology Sandbox application, 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 person, 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.

2. Written notice of a revocation or suspension order made under subparagraph 1. shall 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 person must complete before the commissioner lifts the suspension.

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

(d) If service of process on a person making an innovative financial product or service available to consumers in the Financial Technology Sandbox is not feasible, service on the commissioner shall be deemed service on such person.

(11) RULES AND ORDERS.—

(a) The office and the commissioner shall adopt rules to administer this section.

(b) The commissioner may issue all necessary orders to enforce this section and may enforce these orders in any court of competent jurisdiction. These orders include, but are not limited to, orders for:

1. Payment of restitution.

2. Enforcement of a bond, or a portion of a bond, posted under paragraph (5)(g). The commissioner shall use proceeds from such bonds to offset losses suffered by consumers as a result of an innovative financial product or service.

Section 10. This act shall take effect July 1, 2020.

CODING: Words ~~stricken~~ are deletions; words underlined are additions.