

The Florida Senate
BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Appropriations

BILL: CS/CS/CS/SB 1870

INTRODUCER: Appropriations Committee; Banking and Insurance Committee; Innovation, Industry, and Technology Committee; and Senators Hutson and Harrell

SUBJECT: Technology Innovation

DATE: March 5, 2020

REVISED: _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	<u>Wiehle/Baird</u>	<u>Imhof</u>	<u>IT</u>	<u>Fav/CS</u>
2.	<u>Johnson</u>	<u>Knudson</u>	<u>BI</u>	<u>Fav/CS</u>
3.	<u>Smith</u>	<u>Kynoch</u>	<u>AP</u>	<u>Fav/CS</u>

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/CS/SB 1870 abolishes the Division of State Technology within the Department of Management Services (DMS), reestablishes the Division of Telecommunications, and replaces the State Data Center with the Florida Digital Service, which is charged with proposing innovative solutions that securely modernizes state government, achieving value through digital transformation and interoperability, and supporting the cloud-first policy. The bill requires the Florida Digital Service (FDS) to develop a comprehensive enterprise architecture that addresses how information technology infrastructure may be modernized to achieve cloud-first objectives and to develop a data dictionary and data catalog for the enterprise. “Enterprise” means state agencies, including the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

The bill provides the following provisions for the Cabinet agencies:

- May adopt alternative standards in lieu of the enterprise architecture standards. If the Cabinet agency adopts an alternative standard, the agency must provide a written notification including an explanation of how they will support open data interoperability to the Governor, the President of the Senate, and the Speaker of the House of Representative.
- Clarifies that nothing within this section of law requires the Cabinet agency to integrate with information technology outside of its own department or with the FDS.
- The FDS may not retrieve or disclose any data without a shared-data agreement in place between the department and Cabinet agency.

The bill directs the FDS to document and submit use cases in collaboration with agencies and, contingent on an appropriation, assist with the deployment of new interoperability applications or solutions, including but not limited to:

- The Department of Health, 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; or
- Support military members, veterans, and their families.

Furthermore, the bill creates the Financial Technology Sandbox, within the Office of Financial Regulation (OFR), to license financial technology innovators to test new products and services within the areas of a regulatory sandbox using exceptions of specified general law and waivers of the corresponding rule requirements under defined conditions in the consumer finance, payment instruments sellers, and money transmitter programs.

The bill appropriates \$50,000 in nonrecurring funds for Fiscal Year 2020-2021 from the Administrative Trust Fund to the OFR to implement the provisions of section 559.592, Florida Statutes, relating to the Financial Technology Sandbox.

SB 2500, the Fiscal Year 2020-2021 General Appropriations Act, provides \$850,000 to the Department of Management Services for software to support the data catalog.

Except as otherwise provided (the sandbox provisions), the bill takes effect July 1, 2020.

II. Present Situation:

Department of Management Services (DMS)

Information Technology (IT) Management

The DMS¹ oversees IT² governance and security for the executive branch of state government. The Division of State Technology (DST), within the DMS, implements duties and policies of the DMS in this area.³ The head of DST is appointed by the Secretary of Management Services⁴ and serves as the state chief information officer (CIO).⁵ The CIO must have at least 10 years of executive level experience in the public or private sector.⁶ Since the creation of the Division of State Technology on July 1, 2019, a state CIO has not been appointed. The DST “provides the State with guidance and strategic direction on a variety of transformational technologies, such as

¹ Section 20.22, F.S.

² The term “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. s. 282.0041(14), F.S.

³ Section 20.22(2)(a), F.S.

⁴ The Secretary of Management Services serves as the head of DMS. The Secretary is appointed by the Governor, subject to confirmation by the Senate. s. 20.22(1), F.S.

⁵ Section 20.22(2)(b), F.S.

⁶ *Id.*

cybersecurity and data analytics, while also providing the following critical services: voice, data, software, and much more.”⁷ The duties of DMS and DST include:

- Developing IT policy for the management of the state’s IT resources including state’s data center and telecommunications network;
- Establishing IT architecture standards and assisting state agencies⁸ in complying with those standards;
- Establishing project management and oversight standards with which state agencies must comply when implementing IT projects;
- Performing project oversight of all state agency IT projects that have a total cost of \$10 million or more, as well as cabinet agency IT projects that have a total cost of \$25 million or more, and are funded in the General Appropriations Act or any other law;
- Recommending potential methods for standardizing data across state agencies;
- Recommending open data⁹ technical standards and terminologies for use by state agencies;
- Establishing best practices for the procurement of IT products and cloud-computing services in order to reduce costs, increase the quality of data center services and telecommunication services, or improve government services; and
- Establishing a policy for all IT-related state contracts, including state term contracts for IT commodities, consultant services, and staff augmentation services.¹⁰

State Data Center and the Cloud-First Policy

In 2008, the Legislature created the State Data Center (SDC) system, established two primary data centers,¹¹ and required consolidation of agency data centers into the primary data centers by 2019,¹² which was completed in FY 2013-14. In 2014, the two primary data centers were merged to create the SDC within the then-existing Agency for State Technology.¹³ In 2019, the Legislature abolished the Agency for State Technology and moved the SDC to the Division of State Technology within DMS. DST is required to provide operational management and oversight of the SDC.¹⁴

The SDC relies heavily on the use of state-owned equipment installed at the SDC facility located at the Capital Circle Office Center in Tallahassee for the provision of data center services. The SDC is required to do the following:

- Offer, develop, and support the services and applications defined in service-level agreements executed with its customer entities;¹⁵

⁷ *State Technology*, FLORIDA DEPARTMENT OF MANAGEMENT SERVICES, https://www.dms.myflorida.com/business_operations/state_technology (last visited Jan. 27, 2020).

⁸ See s. 282.0041(27), F.S.

⁹ The term “open data” means data collected or created by a state agency 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 distribution based on federal or state privacy, confidentiality, and security laws and regulations or data for which a state agency is statutorily authorized to assess a fee for its distribution. Section 282.0041(18), F.S.

¹⁰ Section 282.0051, F.S.

¹¹ The Northwood Shared Resource Center and the Southwood Shared Resource Center. Sections. 282.204-282.205, F.S. (2008).

¹² Ch. 2008-116, L.O.F.

¹³ Ch. 2014-221, L.O.F.

¹⁴ Section 282.201, F.S.

¹⁵ A “customer entity” means an entity that obtains services from DMS. s. 282.0041(7), F.S.

- Maintain performance of the state data center by ensuring proper data backup, data backup recovery, disaster recovery, and appropriate security, power, cooling, fire suppression, and capacity;
- Develop and implement business continuity and disaster recovery plans, and annually conduct a live exercise of each plan;
- Enter into a service-level agreement with each customer entity to provide the required type and level of service or services;
- Assume administrative access rights to resources and equipment, including servers, network components, and other devices, consolidated into the SDC;
- Show preference, in its procurement process, for cloud-computing solutions that minimize or do not require the purchasing, financing, or leasing of SDC infrastructure, and that meet the needs of customer agencies, reduce costs, and that meet or exceed the applicable state and federal laws, regulations, and standards for IT security; and
- Assist customer entities in transitioning from state data center services to third-party cloud-computing services procured by a customer entity.

A state agency is prohibited, unless exempted¹⁶ elsewhere in law, from:

- Creating a new agency computing facility or data center;
- Expanding the capability to support additional computer equipment in an existing agency computing facility or data center; or
- Terminating services with the SDC without giving written notice of intent to terminate 180 days before termination.¹⁷

Cloud computing is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”¹⁸ In 2019, the Legislature mandated that each agency adopt a cloud-first policy that first considers cloud computing solutions in its technology sourcing strategy for technology initiatives or upgrades whenever possible or feasible.¹⁹ Each agency must, just like the SDC, show a preference for cloud-computing solutions in its procurement process and adopt formal procedures for the evaluation of cloud-computing options for existing applications, technology initiatives, or upgrades.²⁰

¹⁶ The following entities are exempt from the use of the SDC: the Department of Law Enforcement, the Department of the Lottery’s Gaming System, Systems Design and Development in the Office of Policy and Budget, regional traffic management centers, the Office of Toll Operations of the Department of Transportation, the State Board of Administration, state attorneys, public defenders, criminal conflict and civil regional counsel, capital collateral regional counsel, and the Florida Housing Finance Corporation. S. 282.201(2), F.S.

¹⁷ Section 282.201(3), F.S.

¹⁸ *Special Publication 800-145*, National Institute of Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (last visited Jan. 27, 2020). The term “cloud computing” has the same meaning as provided in Special Publication 800-145 issued by the National Institute of Standards and Technology (NIST). s. 282.0041(5), F.S.

¹⁹ Section 282.206(1), F.S.

²⁰ Section 282.206(2) and (3), F.S.

IT Security

The IT Security Act²¹ establishes requirements for the security of state data and IT resources. The DMS must designate a state chief information security officer (CISO) to oversee state IT security.²² The CISO must have expertise in security and risk management for communications and IT resources.²³ The DST is charged with the following duties regarding IT security:

- Establishing standards and processes consistent with generally accepted best practices for IT security, including cybersecurity;
- Adopting rules that safeguard an agency’s data, information, and IT resources to ensure availability, confidentiality, and integrity and to mitigate risks;
- Developing, and annually updating, a statewide IT security strategic plan that includes security goals and objectives for the strategic issues of IT security policy, risk management, training, incident management, and disaster recovery planning.²⁴

The IT Security Act requires the heads of state agencies to designate an information security manager to administer the IT security program of the state agency.²⁵ In part, the heads of state agencies are also required to annually submit to DMS the state agency’s strategic and operational IT security plans; conduct, and update every three years, a comprehensive risk assessment; and ensure that periodic internal audits and evaluations of the agency’s IT security program for the data, information, and IT resources of the state agency are conducted.²⁶

Telecommunication Services

The DST is also responsible for providing the state enterprise telecommunications system known as the SUNCOM Network. SUNCOM includes voice, data, radio, wiring and cabling, and conferencing service to state agencies, local governments, educational institutions, libraries, and non-profit organizations.²⁷ The DST also leads Emergency Support Functions (ESF 2)²⁸ and E-rate²⁹ and houses the Bureau of Public Safety, which provides Enhanced 911³⁰ and radio communications services to the state’s public safety entities.³¹

Financial Technology

Financial technology, often referred to as “FinTech,” encompasses a wide array of innovation in the financial services industry. FinTech is technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated

²¹ Section 282.318, F.S., is cited as the “Information Technology Security Act.”

²² Section 282.318(3), F.S.

²³ *Id.*

²⁴ Section 282.318(3), F.S.

²⁵ Section 282.318(4)(a), F.S.

²⁶ Section 282.318(4), F.S.

²⁷ Section 282.702, F.S.

²⁸ The DMS, as lead agency for ESF 2 under the direction of the Division of emergency Management, is the first point of contact for telecommunications service providers for equipment and services coordination to provide communications support statewide before, during, and after emergencies.

²⁹ E-Rate is a federal program created to ensure that schools and libraries have affordable access to advance telecommunications services.

³⁰ Section 365.171, F.S.

³¹ Sections 282.709 and 282.7101, F.S.

material effect on the provision of financial services.³² Technological innovation holds great promise for the provision of financial services, with the potential to increase market access, the range of product offerings, and convenience while also lowering costs to clients.³³ Greater competition and diversity in lending, payments, insurance, trading, and other areas of financial services can create a more efficient and resilient financial system.³⁴ Catalysts of FinTech innovations include technology, regulation, and evolving consumer preferences, including customization.³⁵

FinTech innovation is often thought to be synonymous with disruption of the traditional financial services market structure and its providers, such as financial institutions. However, to date, the relationship between incumbent financial institutions and FinTech firms appears to be largely complementary and cooperative in nature.³⁶ FinTech firms have generally not had sufficient access to the low-cost funding or the customer base necessary to pose a serious competitive threat to established financial institutions in mature financial market segments.³⁷ Partnering allows FinTech firms to operate while still being relatively small and, depending on the jurisdiction and the business model, unburdened by some financial regulation while still benefitting from access to incumbents' client base.³⁸ At the same time, incumbents benefit from access to innovative technologies that provide a competitive edge.³⁹ Yet there are exceptions to this trend, as some FinTech firms have established inroads in credit provision and payments.⁴⁰

Regulatory Sandboxes

Rapid Fintech development has brought with it regulatory uncertainty. Some suggest that regulatory relief and testing can be important when it comes to bringing innovative products to market.⁴¹ A well-designed and executed sandbox can facilitate innovation, protect consumers, and safeguard the financial systems.⁴² When approving pilots or issuing regulatory relief, some have suggested agencies adopt a data-driven approach, which incorporates information sharing and the ability to monitor experiments, to ensure the regulators can draw lessons from the sandbox.⁴³ Further, regulatory sandboxes can provide a Fintech business with valuable market insights while maintaining compliance, as well as greater knowledge of the laws surrounding its product or service, and the opportunity to begin building a relationship with a regulator.⁴⁴

³² Financial Stability Board, *FinTech and market structure in financial services: Market developments and potential financial stability implications* (Feb. 14, 2019), <https://www.fsb.org/2019/02/fintech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability-implications/> (last visited Feb. 14, 2020).

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ Quan, Dan, *A Few Thoughts on Regulatory Sandboxes*, Center for Monetary and Financial Alternatives, Cato Institute, at <https://pacscenter.stanford.edu/a-few-thoughts-on-regulatory-sandboxes/> (last viewed Feb. 14, 2020).

⁴² *Id.*

⁴³ *Id.*

⁴⁴ Virtual Currency Report, *Fintech Regulatory Sandboxes: Update on Arizona's Sandbox and Other Developments*, (Feb. 11, 2019), JDSUPRA, at <https://www.jdsupra.com/legalnews/fintech-regulatory-sandboxes-update-on-85915/> (last viewed Feb. 14, 2020).

Arizona Regulatory Sandbox

Arizona was the first state to enact⁴⁵ and launch a regulatory sandbox (sandbox) program.⁴⁶ The program is established under the Attorney General's Office to foster innovation by enabling a business to obtain limited access to the Arizona market to test innovative financial products or services.⁴⁷ Some of the products or services approved for Arizona's sandbox include:

- A financial services "club" using money transmission services in connection with the sale of digital assets aimed at providing a cash management solution for licensed medical marijuana providers.
- A business model for income-sharing agreements that provide qualified consumers with a fixed amount of money in exchange for a percentage of the consumer's future income over a scheduled period of time, subject to contingencies involving periods of unemployment or lowered income.
- A consumer-lending platform that enables small business partners to provide lending options at the point of sale for consumers seeking to finance household related projects.⁴⁸

Office of Financial Regulation

The Office of Financial Regulation (OFR) regulates financial institutions, finance companies, money services businesses, and the securities industry.⁴⁹ The Financial Services Commission (commission), composed of the Governor, Chief Financial Officer, Attorney General, and the Commissioner of Agriculture and Consumer Services, serves as the agency head of the OFR for purposes of rulemaking under ss. 120.536 through 120.565, F.S.⁵⁰

Money Services Businesses

Money services businesses include payment instrument sellers, money transmitters, check cashers, foreign currency exchangers, and deferred presentment providers, pursuant to ch. 560, F.S., the Money Services Business Act. Money services businesses (MSBs) are regulated under two license categories.⁵¹ Money transmitters and payment instrument issuers⁵² are regulated under part II of ch. 560, F.S., while check cashers⁵³ and foreign currency

⁴⁵ House Bill 2434, 2018 Second Regular Session, approved by the Governor March 22, 2018.

⁴⁶ Press, Daniel, *Arizona Becomes First State to Establish FinTech Sandbox* (Mar. 24, 2018) at <https://cei.org/blog/arizona-becomes-first-state-establish-fintech-sandbox> (last viewed Feb. 15, 2020).

⁴⁷ Arizona Attorney General, Mark Brnovich, *Arizona's Fintech Sandbox, Frequently Asked Questions* at <https://www.azag.gov/fintech/faq> (last viewed Feb. 10, 2020).

⁴⁸ Arizona Attorney General, Mark Brnovich, *Sandbox participants* at <https://www.azag.gov/fintech/participants> (last viewed Feb. 15, 2020).

⁴⁹ Section 20.121(3)(a)2., F.S.

⁵⁰ *Id.*

⁵¹ Section 560.104, F.S., provides that banks, credit unions, trust companies, offices of an international banking corporation, or other financial depository institutions organized under the laws of any state of the United States are exempt from the provisions of ch. 560, F.S.

⁵² A person licensed as a money transmitter or payment instrument seller may also engage in the activities authorized for check cashers and foreign currency exchangers without paying additional licensing fees. See s. 560.204(2), F.S.

⁵³ "Check casher" means a person who sells currency in exchange for payment instruments received, except for travelers checks. Section 560.103(6), F.S.

exchangers⁵⁴ are regulated under part III. An applicant for licensure as a money services business must:

- Demonstrate the character and general fitness to command the confidence of the public and warrant the belief that the money services business shall operate lawfully and fairly;
- Be legally authorized to do business in this state;
- Be registered as a money services business with the federal Financial Crimes Enforcement Network;⁵⁵ and
- Have an anti-money laundering program, which meets the requirements of 31 C.F.R. 1022.210.⁵⁶

Pursuant to the Florida Control of Money Laundering in Money Services Business Act, a MSB must maintain certain records of each transaction involving currency or payment instruments in order to deter the use of a money services business to conceal proceeds from criminal activity and to ensure the availability of such records for criminal, tax, or regulatory investigations or proceedings.⁵⁷ A MSB must keep records of each transaction occurring in this state which it knows to involve currency or other payment instruments having a value greater than \$10,000; to involve the proceeds of specified unlawful activity; or to be designed to evade the reporting requirements of ch. 896, F.S., or the Florida Control of Money Laundering in Money Services Business Act.⁵⁸ The OFR may take administrative action against a MSB for failure to maintain or produce documents required by ch. 560, F.S., or federal anti-money laundering laws.⁵⁹ The OFR may also take administrative action against an MSB for other violations of federal anti-money laundering laws such as failure to file suspicious activity reports.⁶⁰

A money transmitter “receives currency,⁶¹ monetary value,⁶² or payment instruments⁶³ for the purpose of transmitting the same by any means, including transmission by wire, facsimile, electronic transfer, courier, the internet, or through bill payment services or other businesses that facilitate such transfer within this country, or to or from this country.”⁶⁴ A payment instrument seller sells, issues, provides, or delivers a payment instrument.⁶⁵ A money transmitter or payment instrument seller must:

⁵⁴ “Foreign currency exchanger” means a person who exchanges, for compensation, currency of the United States or a foreign government to currency of another government. s. 560.103(17), F.S.

⁵⁵ See 31 C.F.R. 1010.100 and 31 C.F.R. 1022.380. These provisions define money service businesses subject to registration with the Financial Crimes Enforcement Network (FinCEN).

⁵⁶ Section 560.1401, F.S.

⁵⁷ Section 560.123, F.S.

⁵⁸ *Id.*

⁵⁹ Section 560.114, F.S.

⁶⁰ *Id.*

⁶¹ “Currency” means the coin and paper money of the United States or of any other country which is designated as legal tender and which circulates and is customarily used and accepted as a medium of exchange in the country of issuance. Currency includes United States silver certificates, United States notes, and Federal Reserve notes. Currency also includes official foreign bank notes. Section 560.103(11), F.S.

⁶² “Monetary value” means a medium of exchange, whether or not redeemable in currency. s. 560.103(21), F.S.

⁶³ “Payment instrument” means a check, draft, warrant, money order, travelers check, electronic instrument, or other instrument, payment of money, or monetary value whether or not negotiable. The term does not include an instrument that is redeemable by the issuer in merchandise or service, a credit card voucher, or a letter of credit. s. 560.103(29), F.S.

⁶⁴ Section 560.103(23), F.S.

⁶⁵ Section 560.103(30) and (34).

- Have a net worth of at least \$100,000 and an additional net worth of \$10,000 per location in this state, up to a maximum of \$2 million.⁶⁶
- Have a corporate surety bond in an amount between \$50,000 and \$2 million depending on the financial condition, number of locations, and anticipated volume of the licensee.⁶⁷ In lieu of a corporate surety bond, the licensee may deposit collateral such as cash or interest-bearing stocks and bonds with a federally insured financial institution.⁶⁸
- Possess permissible investments, such as cash and certificates of deposit, with an aggregate market value of at least the aggregate face amount of all outstanding money transmissions and payment instruments issued or sold by the licensee or an authorized vendor in the United States with exceptions.⁶⁹
- Maintain specified records for at least five years.⁷⁰

An applicant for licensure under part II, of ch. 560, F.S., must submit a nonrefundable fee of \$375 with the application form.⁷¹ Applicants are subject to a background check and other specified requirements.⁷²

Federal Regulation

The Financial Crimes Enforcement Network of the U.S. Department of Treasury (FinCEN) is charged with safeguarding the U.S. financial system from the abuses of money laundering, terrorist financing, and other financial crimes.⁷³ To that end, the FinCEN administers the Bank Secrecy Act (BSA).⁷⁴ The BSA regulations requires financial institutions, which includes money services businesses, to establish an anti-money laundering program, verify customer identity, maintain certain records, and file suspicious activity reports and currency transaction reports that have been determined to have a high degree of usefulness in criminal, tax, and regulatory investigations, as well as in certain intelligence and counter-terrorism matters.⁷⁵ Generally, an MSB is required to register with FinCEN, regardless of whether the MSB is licensed with the state, if it conducts more than \$1,000 in business with one person in one or more transactions on the same day, in one or more of the following services: money orders, traveler's checks, check cashing, currency dealing or exchange.⁷⁶ However, if a business provides money transfer services in any amount, the business is required to be registered.⁷⁷

⁶⁶ Section 560.209, F.S.

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ Section 560.210, F.S.

⁷⁰ Sections 560.1105 and 560.211, F.S.

⁷¹ Section 560.143, F.S.

⁷² Sections 560.114, 560.141, and part II, ch. 560, F.S.

⁷³ FinCEN, *What We Do*, <https://www.fincen.gov/what-we-do> (last visited Jan. 31, 2020).

⁷⁴ The Currency and Foreign Transactions Reporting Act of 1970 (which legislative framework is commonly referred to as the "Bank Secrecy Act" or "BSA.") These statutes are codified at 12 U.S.C. 1829b, 12 U.S.C. 1951-1959, 18 U.S.C. 1956, 18 U.S.C. 1957, 18 U.S.C. 1960, and 31 U.S.C. 5311-5314 and 5316-5332 and notes thereto.

⁷⁵ .31 C.F.R. ss. 1010.100 and 1022.380.

⁷⁶ *Id.*

⁷⁷ *Id.*

Consumer Finance Loans

The Florida Consumer Finance Act (act)⁷⁸ authorizes licensed lenders to make secured or unsecured consumer loans of money, credit, goods, or choses in action⁷⁹ in an amount or to a value of \$25,000 with a tiered interest rate structure such that the maximum annual interest rate allowed on each tier decreases as principle amounts increase:

- 30 percent on the first \$3,000,
- 24 percent on principal above \$3,000 and up to \$4,000, and
- 18 percent on principal above \$4,000 and up to \$25,000.⁸⁰

An applicant for licensure must pay a nonrefundable biennial license fee of \$625, meet liquid asset standards, and other eligibility requirements.⁸¹ Licenses granted under the act are for a single place of business and must be renewed every two years. The act provides grounds for disciplinary action by the OFR against an applicant or a licensee.⁸²

III. Effect of Proposed Changes:

Florida Digital Service

Section 1 amends s. 20.22, F.S., to abolish the Division of State Technology, reestablishes the Division of Telecommunications and creates the Florida Digital Service “FDS”.

Section 2 amends s.110.205, F.S., to add the state chief data officer and the state chief information security officer as positions exempt from career service and allows the Department of Management Services (DMS) to set the salary and benefits in accordance with the rules of the Senior Management Services.

Section 3 amends s. 282.0041, F.S., to create or revise the following definitions:

- “Data governance” means the practice of organizing, classifying, securing, and implementing policies, procedures, and standards for the effective use of an organization’s data;
- “Electronic” means technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities;
- “Electronic credential” means an electronic representation of the identity of a person, organization, application, or device;
- “Enterprise” means the collection of state agencies. The term includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services;
- “Enterprise architecture” means a comprehensive operational framework that contemplates the needs and assets of the enterprise to support interoperability across state government;

⁷⁸ Ch. 516, F.S.

⁷⁹ Chose in action” is defined as “1. A property right in personam, such as a debt owed by another person . . . 2. The right to bring an action to recover a debt, money, or thing. 3. Personal property that one person owns but another person possesses, the owner being able to regain possession through a lawsuit.” Black’s Law Dictionary 101 (3d ed. 1996).

⁸⁰ Section 516.031 (1), F.S. In addition, consumer finance lenders are permitted to charge other fees, as provided in s. 516.031(3), F.S.

⁸¹ Section 516.03(1), F.S.

⁸² Section 516.07, F.S.

- “Interoperability” means the technical ability to share and use data across and throughout the enterprise; and
- “Open data” amends the definition to include data collected by the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services and adds reference to specific exemptions for privacy, confidentiality, security, personal health, business or trade secret information

Section 4 amends s. 282.0051, F.S., to provide the powers and duties of the FDS. The FDS is created within the DMS to propose solutions that securely modernize state government, achieve value through digital transformation and interoperability, and fully support the cloud-first policy as specified in s. 282.206, F.S.

The bill specifies the following duties and responsibilities to the FDS:

- To develop an enterprise architecture that acknowledges the unique need of each entity within the enterprise, facilitates digital interoperability, and supports cloud-first policy⁸³, and addresses how information technology (IT) infrastructure may be modernized to achieve cloud-first objectives.
- To recommend other payment mechanisms to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.
- To conduct, every three years starting in 2021, a market analysis to determine whether the IT resources within the enterprise are utilized in the most cost-effective and cost-efficient manner and incorporate the results into a strategic plan for continued and future information technology and information services including approaches to implement new services or technologies. The analysis and report 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.
- To ensure the enterprise IT solutions are capable of utilizing an electronic credential and comply with the enterprise architecture standards.

The bill amends the date to January 1 of each even-numbered year for the DMS to provide recommendations for standardization and consolidation of IT services that support interoperability and the cloud-first policy to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

The bill also adds a requirement for the state chief information officer to have, prior to appointment, at least five 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.

The bill adds a chief data officer with significant and substantive experience in data management, data governance, interoperability, and security.

The FDS shall do the following within funds appropriated to the FDS:

⁸³ Section 282.206, F.S.

- Create, not later than October 1, 2021, and maintain a comprehensive indexed data catalog that lists what data elements are housed within the enterprise and in which legacy system or application these data elements are located and what data is restricted from public disclosure;
- 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;
- Adopt, by rule, standards that support the creation and deployment of application programming interfaces to facilitate integration throughout the enterprise;
- Adopt, by rule, standards necessary to facilitate a secure ecosystem of data interoperability that is compliant with the enterprise architecture;;
- Adopt, by rule, standards that facilitate the deployment of applications or solutions to existing enterprise obligations in a controlled and phased approach; and
- After submission of documented use cases developed in conjunction with the affected agencies, assist the affected agencies with the deployment, contingent upon a specific appropriation , of new interoperable applications and solutions for:
 - The Department of Health, the Agency for Healthcare Administration, the Agency for Persons with Disabilities, the Department of Education, the Department of Elderly Affairs, and the Department of Children and Families; and
 - Support of military members, veterans, and their families.

Upon adoption of the enterprise architecture, the FDS may develop a process to:

- Receive written notice from the enterprise of procurement of an information technology project that is subject to governance by the enterprise architecture; and
- Participate in the development of specifications and recommend modifications of any procurement by state agencies that the procurement complies with the enterprise architecture.

The bill adds a requirement that the FDS may not retrieve or disclose any data without a shared data agreement in place between the department and the enterprise entity that has primary custodial responsibility of, or data-sharing responsibility for, that data.

Section 5 amends s. 282.00515, F.S., to revise the current process which requires the Cabinet agencies to either adopt the IT architecture standards established in s. 282.0051, F.S., or adopt alternative standards based on best practices and industry standards. The bill provides that, if a Cabinet agency adopts alternative standards in lieu of the enterprise architecture standards, such agency must provide a written justification, including an explanation on how the agency will achieve open data interoperability, to; the Governor, the President of the Senate, and the Speaker of the House of Representatives.t

The bill clarifies that nothing in this section of law 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 department or with the FDS and the FDS may not retrieve or disclose any data without a data sharing agreement in place.

Sections 6, 7, 8, 9, 10, and 11 amend ss. 282.318, 287.0591, 365.171, 365.172, 365.173, and 943.0415, F.S., respectively, to make technical, conforming changes.

Financial Technology Sandbox

Section 12 creates s. 559.952, F.S., the “Financial Technology Sandbox” (“sandbox”) effective January 1, 2021, within the Office of Financial Regulation (OFR). Subsection (2) provides that the intent of the sandbox is to allow financial technology innovators to test new products and services in a supervised, flexible regulatory sandbox, using exceptions from specified general law and waivers of the corresponding rule requirements under defined conditions. Subsection (3) creates definitions of terms, including the following:

- “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.
- “Commission” means the Financial Services Commission.
- “Consumer” means a person in this state, whether a natural person or a business entity, 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.
- “Control person,” is defined to have the same meaning as provided in s. 516.01, F.S.
- “Corresponding rule requirements” means the commission rules, or portions thereof, which implement the general laws enumerated in the bill.
- “Financial product or service” means a product or service related to a consumer finance loan, as defined in s. 516.01, F.S., or as a money transmitter or payment instrument seller, as defined in s. 560.103, F.S., including mediums of exchange that are in electronic or digital form, which is subject to general law or corresponding rule requirements in the sections enumerated in paragraph (4)(a) and to general law or corresponding rule requirements in the sections enumerated in paragraph (4)(a) and which is under the jurisdiction of the office.
- “Financial Technology Sandbox” means the program which allows a licensee to make an innovative financial product or service available to consumers as a person who makes and collects consumer finance loans, as defined in s. 516.01, F.S., or as a money transmitter or payment instrument seller, as defined in s. 560.103, F.S., during a sandbox period through an exception to general laws or a waiver of rule requirements, or portions thereof.
- “Innovative” means new or emerging technology, or new uses of existing technology, which provides a product, service, business model, or delivery mechanism to the public and which is not known to have a comparable offering in this state outside of the Financial Technology Sandbox.
- “Licensee” means a business entity that has been approved by the office to participate in the Financial Technology Sandbox.
- “Office” means, unless the context clearly indicates otherwise, the Office of Financial Regulation.
- “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 law.

Sandbox Application; Standards for Approval (Subsection 5)

Before filing an application to enter the sandbox, a substantially affected person may seek a declaratory statement regarding the applicability of a statute, rule, or agency order to the

petitioner's particular set of circumstances.

The Commission shall, by rule, prescribe the form and manner of the application and how the office will evaluate each application.

Before making an innovative financial product or service available to consumers in the sandbox, a business entity must file an application for licensure with the OFR. In the application, the business entity must specify the general law or rule requirements for which an exception or waiver is sought and the reasons why these requirements prevent the innovative financial product or service from being made available to consumers. The application must also contain:

- The nature of the innovative financial product or service proposed to be made available to consumers in the sandbox;
- The maximum number of consumers to whom the applicant proposes to provide the innovative financial product or service;
- The potential risk to consumers, and the methods that will be used to protect consumers and resolve complaints during the sandbox period;
- The business plan proposed by the applicant;
- 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;
- If any control person involved in the development, operation, or management of the applicant's innovative financial product or service 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, any property-based offense, or any crime involving moral turpitude or dishonest dealing, the application to the sandbox will be denied. A plea of no contest, a conviction, or a finding of guilt must be reported regardless of adjudication;
- A copy of the disclosures that will be provided to consumers;
- The financial responsibility of any control person; and
- Any other factor that the office determines to be relevant.

The OFR may not approve an application if the applicant had a prior sandbox application that was approved and that related to a substantially similar financial product or service, or if any control person substantially involved in the development, operation, or management of the applicant's innovative financial product or service was substantially involved with another sandbox applicant whose application was approved and whose application related to a substantially similar financial product or service, or if the applicant or any control person has failed to affirmatively demonstrate financial responsibility.

The OFR must approve or deny in writing a sandbox application within 60 days after receipt of the completed application. The OFR and the applicant may jointly agree to extend the time beyond 60 days. Consistent with this section, the OFR may impose conditions on any approval.

Upon approval of an application, the OFR must notify the licensee of their exemption from general law enumerated in the bill and corresponding rule during the sandbox period and the length of the initial sandbox period, not to exceed 24 months. The OFR must 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 making the financial product or service available.

Exceptions of General Law and Waivers of Rules (Subsection 4)

Notwithstanding any other law, the following provisions of general law and corresponding rule requirements are not applicable to the licensee during the sandbox period:

- Section 516.03(1), F.S., relating to the application of a license, to waive the authority of the OFR to request information about the applicant or control person regarding their qualifications, educational and business history, and disciplinary and criminal history. Subsection (5) of section 12 of the bill requires an applicant to provide information concerning their financial and technical expertise, as well as information, including financial responsibility, concerning any control persons. Further the bill and section 516.07, F.S., provide grounds for the denial of a licensee. Section 516.05(1) and (2), F.S., relating to the licensure requirements, to allow for waivers of the 2-year license period and provisions relating to inactive licenses. However, the requirement for the OFR to conduct a background check, required in subsection (1) is not waived.
- Section 560.109, F.S., relating to the examinations and investigations is waived only to the extent that the section requires the OFR to examine a licensee at least once every five years beyond the authorized sandbox period.
- Section 560.118(1), F.S., relating to reports, to waive the quarterly reporting requirement. The bill requires sandbox licensees to submit reports twice a year.
- Section 560.125, F.S., relating to unlicensed activities and penalties, waives subsection (1), only to the extent that subsection would prohibit a licensee from engaging in the business of a money services business during the sandbox period; and subsection (2) is waived only to the extent that subsection would prohibit a licensee from appointing an authorized vendor during the sandbox period
- Section 560.128, F.S., relating to customer contact information and license, to waive the requirements that a licensee provide contact information for the licensee and the OFR and display a license at each location.
- Section 560.141, F.S., relating to the application for a license as a money services business, waives the submission of the following information:
 - Date and state of the applicant's formation.
 - A description of the applicant's business structure.
 - If the applicant or parent is a publicly traded company, copies of all filings made with the U.S. Securities and Exchange Commission or with a similar regulator in another country within the preceding year.
 - The name of the registered agent in this state.
 - Information concerning the company organization, financial viability, and financial responsibility are required as part of the sandbox application process.
- Section 560.142, F.S., relating to the issuance of a license renewal except that the OFR may prorate, but not entirely waive, the license renewal period. The initial sandbox license period is 24 months and the OFR may grant an extension for an additional 12 months, if certain conditions are met.
- Section 560.143(2), F.S., relating to license renewal fees, only to the extent necessary for proration of the renewal fee.

- Section 560.204(1), F.S., relating to unlicensed activity, only to the extent that subsection would prohibit an applicant from engaging in, or advertising it engages in, the selling or issuing of payment instruments or in the activity of a money transmitter during the sandbox period.
- Section 560.205(2), F.S., relating to additional license application requirements, the submission of a sample form of payment instrument is waived. Section 560.208(2), F.S., relating to conduct of businesses, to waive the authority of a licensee to charge a different price for a money transmitter service based on the mode of transmission if certain conditions are met. or
- Section 560.209, F.S., relating to net worth, corporate surety bonds, and collateral deposit in lieu of bond, only to the extent that the OFR may modify, but not entirely waive, the net worth, corporate surety bond, and collateral deposit amounts required under this section. The modified amounts must be in such lower amounts that the OFR determines to be commensurate with the considerations under paragraph (5)(c) and the maximum number of consumers authorized to receive the financial product or service under this section.

Sandbox Operation (Subsection 6)

A licensee may make an innovative financial product or service available to consumers during the initial sandbox period of 24 months. The OFR may, on a case-by-case basis and after consultation with the licensee, specify the maximum number of consumers authorized to receive an innovative financial product or service. The OFR may not authorize more than 15,000 consumers to receive the financial product or service until the licensee has filed the first required biannual report. After the filing of the first report, if the licensee demonstrates adequate financial capitalization, risk management process, and management oversight, the OFR may authorize up to 25,000 consumers to receive the financial product or service.

Before a consumer purchases, uses, receives, or enters into an agreement to purchase, use, or receive an innovative financial product or service through the sandbox, the licensee must provide a written statement to the consumer that includes the following disclosures:

- The name and contact information of the person making the financial product or service available to consumers;
- 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;
- That this state does not endorse the financial product or service;
- That the financial product or service is undergoing testing, may not function as intended, and may entail financial risk;
- That the person making the financial product or service available to consumers is not immune from civil liability for any losses or damages caused by the financial product or service;
- The expected end date of the sandbox period;
- 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; and
- Any other statements or disclosures required by rule of the commission.

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

The OFR may enter into an agreement with a state, federal, or foreign regulatory agency to allow persons who make an innovative financial product or service available in this state through the sandbox to make their products or services available in other jurisdictions. The commission must adopt rules to implement this provision.

The OFR may examine the records of a sandbox licensee at any time, with or without notice.

Sandbox Period Extension and Conclusion (Subsection 7)

A licensee may apply for an extension of the initial sandbox period for 12 additional months. A complete application for an extension must be filed with the OFR at least 90 days before the conclusion of the initial sandbox period. The OFR must approve or deny the application for extension in writing at least 35 days before the conclusion of the initial sandbox period. In deciding to approve or deny an application for extension of the sandbox period, the office must at least consider the status of the factors previously considered in deciding to approve or deny an application to enter the sandbox. An application for an extension must cite one of the following reasons as the basis for the application and must provide all relevant supporting information that:

- Amendments to general law or rules are necessary to offer the innovative financial product or service in this state permanently; or
- 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 OFR, and approval is pending.

At least 30 days before the conclusion of the initial sandbox period or the extension, whichever is later, a licensee must 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 sandbox exists to make the financial product or service available to consumers. After the conclusion of the sandbox period or the extension, whichever is later, the person who makes the innovative financial product or service available may:

- Collect and receive money owed to the person or pay money owed by the person, based on agreements with consumers made before the conclusion of the sandbox period or the extension;
- Take necessary legal action; and
- Take other actions authorized by commission rule, which are not inconsistent with this subsection.

Reporting (Subsection 8)

A person authorized to make an innovative financial product or service available to consumers must submit a report to the office twice a year, as prescribed by commission rule. The report must include financial reports and the number of consumers who have received the financial product or service.

Construction (Subsection 9)

A business entity whose sandbox application is approved under this section is deemed licensed under chapter 516, chapter 560, or both chapter 516 and 560, F.S., as applicable to the business entity's activities. The business entity is subject to any provision of chapter 516 or chapter 560, F.S., not specifically excepted under paragraph (4)(a), as the applicable to the business entity's activities, and must comply with such provisions. Notwithstanding s. 560.204(2), F.S., the business entity may not engage in part III of chapter 560, F.S.

Violations and Penalties (Subsection 10)

A licensee who makes an innovative financial product or service available to consumers in the sandbox is not immune from civil damages for acts and omissions relating to this section and is subject to all criminal statutes and any other statute not specifically excepted. The OFR may, by order, revoke or suspend authorization granted to a person to make an innovative financial product or service available to consumers if:

- The licensee has violated or refused to comply with this section, a rule of the commission, an order of the OFR, or a condition placed by the office on the approval of the person's sandbox application;
- A fact or condition exists that, if it had existed or become known at the time that the sandbox application was pending, would have warranted denial of the application or the imposition of material conditions;
- A material error, false statement, misrepresentation, or material omission was made in the sandbox application; or
- After consultation with the licensee, continued testing of the innovative financial product or service would:
 - Be likely to harm consumers; or
 - No longer serve the purposes of this section because of the financial or operational failure of the financial product or service.

Written notice of a revocation or suspension order 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 person must complete before the office lifts the suspension. 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 actions. If service of process on a person making an innovative financial product or service available to consumers in the sandbox is not feasible, service on the OFR is deemed service on such person.

Rules and Orders (Subsection 11)

The commission must adopt rules to administer this section prior to approving any sandbox application. The OFR may issue all necessary orders to enforce this section and may enforce the orders in accordance with ch. 120, F.S., 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 because of an innovative financial product or service.

Appropriation for the Sandbox

Section 13 provides an appropriation of \$50,000 in nonrecurring funds from the Administrative Trust Fund to the Office of Financial Regulation to implement s. 559.952, F.S., as created by this act.

Effective Date

Section 14. The creation of s. 559.952, F.S., and the appropriation to implement s. 559.952, F.S., by this act shall take effect only if SB 1872 or similar legislation takes effect and if such legislation is adopted in the same legislative session or an extension thereof and becomes a law. SB 1872 creates public record exemptions for certain records containing proprietary business information related to the Financial Technology Sandbox.

Section 15 provides that, except as otherwise expressly provided, the bill takes effect July 1, 2020.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

Entering into Reciprocal Agreements with Other States, Federal Agencies, or Foreign Regulatory Agencies

Statutory authorization to enter reciprocal agreements with other states may potentially implicate the “nondelegation doctrine.” Article III, Section 1 of the Florida Constitution states that “[t]he legislative power of the state shall be vested in a legislature of the State of Florida.” The Florida Supreme Court has held that this constitutional provision requires that “primary policy decisions shall be made by members of the legislature who

are elected to perform those tasks, and administration of legislative programs must be pursuant to some minimal standards and guidelines....”⁸⁴

The Legislature may constitutionally transfer subordinate functions to "permit administration of legislative policy by an agency with the expertise and flexibility to deal with complex and fluid conditions."⁸⁵ However, the Legislature "may not delegate the power to enact a law or the right to exercise unrestricted discretion in applying the law."⁸⁶ Further, the nondelegation doctrine precludes the Legislature from delegating its powers "absent ascertainable minimal standards and guidelines."⁸⁷ When the Legislature delegates power to another body, it "must clearly announce adequate standards to guide in the execution of the powers delegated."⁸⁸

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

There could be a fiscal impact on businesses that have a reduced regulatory structure by inclusion into the Financial Technologies Sandbox. This could allow these businesses to be more successful or could result in the failure of the business.

C. Government Sector Impact:

Sections 1 through 11 of the Bill:

The bill will have a significant negative fiscal impact on state government expenditures. It is unclear how the Florida Digital Service (FDS), within the DMS, will be funded. The current structure of the Division of State Technology allows the Office of the State Chief Information Officer (OCIO) to be included within the state data center’s cost recovery model. The bill provides for much different duties and structure which is unlikely to be allowable under Florida’s Statewide Cost Allocation Plan. The actual structure of the FDS is not clear, but the current budget of the OCIO in SB 2500, the Senate’s General Appropriations Bill, funded through the cost recovery model is \$6,090,379. Also, the current duties of the OCIO have significantly expanded and the OCIO may not have the staffing levels to support this expanded workload. Of the \$6,090,379 provided in SB 2500, \$850,000 from the Working Capital Trust Fund is specifically appropriated for software to support the data catalog specified in this bill.

⁸⁴ *Askew v. Cross Key Waterways*, 372 So.2d 913, 925 (Fla. 1978).

⁸⁵ *Microtel v. Fla. Pub. Serv. Comm'n*, 464 So.2d 1189, 1191 (Fla.1985) (citing *State, Dep't of Citrus v. Griffin*, 239 So.2d 577 (Fla.1970)).

⁸⁶ *Sims v. State*, 754 So.2d 657, 668 (Fla. 2000).

⁸⁷ *Dep't of Bus. Reg., Div. of Alcoholic Beverages and Tobacco v. Jones*, 474 So.2d 359, 361 (Fla. 1st DCA 1985).

⁸⁸ *Martin*, 916 So.2d at 770.

Sections 12 through 14 of the Bill:***Office of Financial Regulation (OFR)***

The OFR estimates that they will need \$50,000 in nonrecurring funds to make changes to their information technology infrastructure in order to administer the Financial Technology Sandbox program.⁸⁹

VI. Technical Deficiencies:**VII. Related Issues:****VIII. Statutes Affected:**

This bill substantially amends the following sections of the Florida Statutes: 20.22, 110.205, 282.0041, 282.0051, 282.00515, 282.318, 287.0591, 365.171, 365.172, 365.173, and 943.0415.

This bill creates section 559.952 of the Florida Statutes.

IX. Additional Information:**A. Committee Substitute – Statement of Substantial Changes:**
(Summarizing differences between the Committee Substitute and the prior version of the bill.)**CS/CS/CS by Appropriations on March 3, 2020:**

The committee substitute:

- Adds a definition for data governance, removes definitions for credential service provider, data-call, and qualified entity, and modifies definition for open data to include references to disclosure exemptions for privacy, confidentiality, security, personal health, business or trade secret information and state public records laws.
- Removes the authority for the Florida Digital Service (FDS) to procure a credential service provider.
- Removes the authority for the FDS to enter into agreements with qualified entities to access state data for a fee, and for the revenue from the fees to be deposited into the Department of Management Services (DMS) operating trust fund.
- Amends the date for the FDS to provide recommendations for standardization or consolidation of information technology (IT) services to January 1 of each even-numbered year.
- Allows the FDS to submit recommendations for other payment mechanism to the Governor, President, and Speaker and such mechanisms can only be implemented if specifically authorized by the Legislature.

⁸⁹ Email from Office of Financial Regulation, CS/SB 1870 Fiscal Impact (Feb. 14, 2020). On file with the Banking and Insurance Committee.

- Requires the FDS to conduct a market analysis every three years and incorporate the results into a strategic plan. The analysis and plan must be submitted to the Governor, President, and Speaker by December 31 of the year the analysis was conducted.
- Add requirement that enterprise IT solutions must be capable of utilizing an electronic credential and comply with the enterprise architecture standards.
- Adds experience requirements for the Chief Information Officer (CIO) and Chief Data Officer (CDO).
- Allows the DMS to set the salary and benefits for the CIO, CDO, and Chief Information Security Officer as Senior Management Service.
- Provide deadlines for the development of a statewide data dictionary and data catalog.
- Requires the DMS to use the rulemaking process for developing and publishing statewide IT standards as it relates to architecture, data interoperability, interfaces, and the deployment of new applications and solutions to existing systems.
- Removes authority to set standards over existing solutions for digital proof of driver's licenses, authentication of voter eligibility, and integration for motor vehicle insurance cancellation.
- Amends the notification requirements for the Cabinet agencies when adopting alternative IT standards.
- Clarifies that there is no requirements in s. 282.0051, F.S., for Cabinet agencies to integrate with systems outside of their department and that the FDS may not retrieve or disclose any data without a data sharing agreement in place.
- Makes technical clarifying changes for specific exemptions in general law for the financial technology sandbox
- Adds requirement for applicants to specify the number of consumers they propose to offer their product or service to and include a draft of the proposed consumer disclosures as part of the initial application
- Requires the Office of Financial Regulation (OFR) to consider the financial responsibility of an applicant and requires the OFR to deny a license if an applicant does not comply with these requirements.
- Revises license periods to provide that the initial sandbox license is for a period of 24 months, instead of up to 24 months, and the extension licensee is for a period of 12 months, instead of up to 12 months.
- Provides that a business entity whose sandbox application is approved by the OFR is licensed under chapter 516, chapter 560, or both chapters 516 and 560, as applicable to the activities of the business entity; and is subject to any provision of chapter 516 or chapter 560 not specifically excepted, as applicable to the activities of the business entity, and must comply with such provisions.

CS/CS by Banking and Insurance on February 19, 2020:

The CS:

- Eliminates the Enterprise Architecture Advisory Council.
- Revises powers and duties of the Florida Digital Services.
- Revises the definition of the term, "enterprise," to exclude the judicial branch.

- Provides that a credential service provider and qualifying entity revenues may not be derived from any other transactions that generate revenue for the enterprise outside of the per-data-call or subscription charges.
- Provides technical, conforming changes.
- Revises the Financial Regulatory Sandbox program to limit the scope to products or services relating to a consumer finance loan or a money transmitter and payment instrument seller.
- Creates additional definitions relating to the Financial Regulatory Sandbox program.
- Eliminates the authority of the Office of Financial Regulation to enter into reciprocity agreements with other states, federal agencies, or foreign regulatory agencies to allow persons operating in sandboxes in other jurisdictions to operate in this state.
- Revises requirements for the application for licensure under the Financial Regulatory Sandbox program.
- Removes additional recordkeeping requirements for sandbox licensees.
- Appropriates \$50,000 in nonrecurring funds from the Administrative Trust Fund to the Office of Financial Regulation to implement the provisions of s. 559.952, F.S.

CS by Innovation, Industry, and Technology on February 10, 2020:

The committee substitute:

- Creates the definitions relating to the Florida Digital Service in s. 282.0041, F.S., instead of s. 282.0051, F.S.;
- Provides new definitions for “credential service provider,” “data call,” “electronic,” “electronic credential,” and “electronic credential provider”;
- Changes the definition of “enterprise” for purposes of the provisions on the Florida Digital Service’s enterprise architecture to include all entities within the executive branch of state government, plus the Justice Administrative Commission and the Public Service Commission, and Department of Legal Affairs, the Department of Agriculture and Consumer Services, the Department of Financial Services, and the judicial branch;
- Expands the Florida Digital Service’s oversight of and involvement in projects that have an information technology component and provides for exceptions;
- Deletes all qualifications for the state chief information officer, the state chief data officer, and the state chief information security officer;
- Deletes the provisions on the Florida Digital Service enforcing the enterprise architecture by intervening in any procurement of information technology and delaying the procurement until it complies with the enterprise architecture;
- Deletes the requirement that the enterprise architecture’s comprehensive account for all of the needs and responsibilities of a department;
- Requires the terms of the contract with a credential service provider pay for that service on a per-data call or subscription basis, with the revenues from these charges deposited into DMS’s operating trust fund for distribution, with DMS to recover all costs for implementing and administering the electronic credential solution;
- Authorizes the Florida Digital Service to “report to the legislative branch on any project within the judicial branch which does not comply with the enterprise architecture, while understanding the separation of powers”;

- Creates the Enterprise Architecture Advisory Council to meet semiannually to discuss implementation, management, and coordination of the enterprise architecture; identify potential issues and threats with specific use cases; and develop proactive solutions;
- Creates the Financial Technology Sandbox Act effective January 1, 2021;
- Provides authority for exceptions rather than waivers of certain statutory requirements;
- Deletes banking products and services from the definition of financial product or service and deletes references to blockchain technology;
- Deletes from the definition of “innovative” the requirement that the technology “has no substantially comparable, widely available analog in this state”;
- Authorizes the Office of Financial Regulation, not the Commissioner of the Office of Financial Regulation to waive a requirement or a portion thereof which is imposed by a general law or rule, and lists individual statutes which may be waived instead of entire chapters;
- Provides for declaratory statement on applicability of statutes, rules, or orders;
- Provides that the Financial Services Commission is to prescribe by rule the form and manner of the application to enter the Financial Technology Sandbox, not the Commissioner of the Office of Financial Regulation;
- Deletes a requirement that the applicant submit fingerprints for each individual filing an application and each individual who is substantially involved in the development, operation, or management of the innovative financial product or service, together with all the provisions relating to this requirement;
- Deletes a requirement that a person whose Financial Technology Sandbox application is approved post a consumer protection bond with the commissioner as security for potential losses suffered by consumers;
- Adds a limitation of 15,000 consumers to receive the financial product or service prior to filing the first activity report, with the limit increased after such filing to 25,000; and
- Adds a requirement that these reports, at a minimum, include financial reports and the number of consumers who have received the financial product or service.

B. Amendments:

None.