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 Innovation, Industry, and Technology

BILL:	SB 1870
INTRODUCER:	Senators Hutson and Cruz
SUBJECT:	Technological Development
DATE:	February 7, 2020
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Wiehle/Baird	Imhof	IT	**Pre-meeting**
2.			BI	
3.			AP	

I. Summary:

SB 1870 abolishes the Division of State Technology within the Department of Management Services (DMS) and replaces it with the Florida Digital Service. The Florida Digital Service must develop an enforceable and comprehensive enterprise architecture, defined as "a comprehensive operational framework that contemplates the needs and assets of the enterprise to create a unified information technology environment." "Enterprise" is defined as the entirety of state government and its subdivisions; thus, the Florida Digital Service is to create a unified information technology environment for all governmental entities in the state.

The bill also creates the Financial Technology Sandbox Program within the Office of Financial Regulation to allow financial technology innovators to test new financial products and services in a supervised, flexible regulatory sandbox, using waivers of specified general law and rule requirements. The bill grants the Commissioner of Financial Regulation the power to waive, for a Sandbox participant, any requirement imposed by general law or rule in specified chapters. To participate, a person must file an application with and be approved by the Commissioner. A person whose Financial Technology Sandbox application is approved must be deemed to possess an appropriate license under any general law requiring state licensure or authorization. The approved person then may participate in the Financial Technology Sandbox and make an innovative financial product or service available to consumers. The Sandbox participant must provide consumers with specified disclosures before a consumer purchases or enters into an agreement to receive an innovative financial product or service through the Financial Technology Sandbox. A person who makes an innovative financial product or service available to consumers in the Financial Technology Sandbox is not immune from civil damages for acts and omissions relating to Sandbox activities and is subject to all criminal and consumer protection laws. The commissioner may, by order, revoke or suspend authorization granted to a person to make an innovative financial product or service available to consumers.

The bill takes effect July 1, 2020.

II. Present Situation:

Department of Management Services (DMS)

Information Technology (IT) Management

DMS[1] oversees IT[2] governance and security for the executive branch of state government. The Division of State Technology (DST), a subdivision of DMS subject to its control and supervision, implements DMS's duties and policies in this area.[3] The head of DST is appointed by the Secretary of Management Services[4] and serves as the state chief information officer (CIO).[5] The CIO must be a proven effective administrator with at least 10 years of executive level experience in the public or private sector.[6] DST "provides the State with guidance and strategic direction on a variety of transformational technologies, such as cybersecurity and data analytics, while also providing the following critical services: voice, data, software, and much more."[7] The duties and responsibilities of DMS and DST include:

- Developing IT policy for the management of the state's IT resources;
- Establishing IT architecture standards and assisting state agencies[8] in complying with those standards;
- Establishing project management and oversight standards with which state agencies must comply when implementing IT projects. The standards must include:
  - Performance measurements and metrics that reflect the status of an IT project based on a defined and documented project scope, cost, and schedule;
  - Methodologies for calculating acceptable variances in the projected versus actual scope, schedule, or cost of an IT project; and
  - Reporting requirements
- 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 which will promote interoperability and reduce the collection of duplicative data;
- Recommending open data[9] technical standards and terminologies for use by state agencies;

---

[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 and 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.*

[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. S. 282.0041(18), F.S.

- 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, 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 that agency data centers be consolidated into the primary data centers by 2019.[12] Data center consolidation was completed in FY 2013-14. In 2014, the two primary data centers were merged in law to create the SDC within then-existing Agency for State Technology.[13] The SDC is established within DMS and DMS 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 in the state's Capital Circle Office Center in Tallahassee for the provision of data center services. The SDC is led by the director of the SDC.[15] 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;[16]
- 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.

[10] S. 282.0051, F.S.
[11] The Northwood Shared Resource Center and the Southwood Shared Resource Center. Ss. 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] Section 282.201, F.S.
[16] A "customer entity" means an entity that obtains services from DMS. s. 282.0041(7), F.S.

A state agency is prohibited, unless exempted[17] 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.[18]

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."[19] 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.[20] 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.[21]

IT Security

The IT Security Act[22] establishes requirements for the security of state data and IT resources.[23] DMS must designate a state chief information security officer (CISO) to oversee state IT security.[24] The CISO must have expertise in security and risk management for communications and IT resources.[25] DMS is tasked 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 including:
    - Identifying protection procedures to manage the protection of an agency's information, data, and IT resources;

[17] The following entities are exempt from the use of the SDC: the Department of Law Enforcement, the Department of the Lottery's Gaming 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.
[18] Section 282.201(3), F.S.
[19] *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.
[20] Section 282.206(1), F.S.
[21] Section 282.206(2) & (3), F.S.
[22] Section 282.318, F.S., is cited as the "Information Technology Security Act."
[23] Section 282.318, F.S.
[24] Section 282.318(3), F.S.
[25] *Id.*

- Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes; and
- Recovering information and data in response to an IT security incident;
- Developing and publishing for use by state agencies an IT security framework; and
- Reviewing the strategic and operational IT security plans of executive branch agencies annually.[26]

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.[27] 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 to determine the security threats to the data, information, and IT resources of the state agency; develop, and periodically update, written internal policies and procedures; 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.[28]

Enhanced 911 (E911) System

DST oversees the E911 system in Florida.[29] DST is required by law to develop, maintain, and implement the statewide emergency communications E911 system plan.[30] The plan must provide for:

- The public agency emergency communications requirements for each entity of local government[31] in the state.
- A system to meet specific local government requirements, which must include law enforcement, firefighting, and emergency medical services, and may include other emergency services such as poison control, suicide prevention, and emergency management services.
- Identification of the mutual aid agreements necessary to obtain an effective E911 system.
- A funding provision that identifies the cost to implement the E911 system.[32]

DST is responsible for implementing and coordinating the plan, and must adopt any necessary rules and schedules related to public agencies[33] implementing and coordinating the plan.[34]

The Secretary of Management Services, or his or her designee, is the director of the E911 system and also serves as chair of the E911 Board.[35] The director of the E911 system is authorized to

[26] Section 282.318(3), F.S.
[27] Section 282.318(4)(a), F.S.
[28] Section 282.318(4), F.S.
[29] Section 365.171, F.S. Prior to 2019, the Division of Telecommunications, established in statute as the Technology Program within DMS, was the entity with oversight over E911. *See* ch. 2019-118, L.O.F.
[30] Section 365.171(4), F.S.
[31] "Local government" means any city, county, or political subdivision of the state and its agencies. s. 365.171(3)(b), F.S.
[32] *Id.*
[33] "Public agency" means the state and any city, county, city and county, municipal corporation, chartered organization, public district, or public authority located in whole or in part within this state which provides, or has authority to provide, firefighting, law enforcement, ambulance, medical, or other emergency services. s. 365.171(3)(c), F.S.
[34] Section 365.171(4), F.S.
[35] Section 365.172(5)(a), F.S.

coordinate the activities of the system with state, county, local, and private agencies.[36] The director must consult, cooperate, and coordinate with local law enforcement agencies.[37] An "E911 Board," composed of eleven members, is established in law to administer funds derived from fees imposed on each user of voice communications service with a Florida billing address (place of primary use).[38] The Governor appoints five members who are county 911 coordinators and five members from the telecommunications industry.[39] The E911 Board makes disbursements from the Emergency Communications Number E911 System Trust Fund to county governments and wireless providers.[40]

Agency Procurements

Agency[41] procurements of commodities or contractual services exceeding $35,000 are governed by statute and rule and require use of one of the following three types of competitive solicitations,[42] unless otherwise authorized by law:[43]

- Invitation to bid (ITB): An agency must use an ITB when the agency is capable of specifically defining the scope of work for which a contractual service is required or when the agency is capable of establishing precise specifications defining the actual commodity or group of commodities required.[44]
- Request for proposals (RFP): An agency must use an RFP when the purposes and uses for which the commodity, group of commodities, or contractual service being sought can be specifically defined and the agency is capable of identifying necessary deliverables.[45]
- Invitation to negotiate (ITN): An ITN is a solicitation used by an agency that is intended to determine the best method for achieving a specific goal or solving a particular problem and identifies one or more responsive vendors with which the agency may negotiate in order to receive the best value.[46]

DMS is responsible for procuring state term contracts for commodities and contractual services from which state agencies must make purchases.[47]

Digital Driver License

Current law provides for the establishment of a digital proof of driver license. Specifically, the Department of Highway Safety and Motor Vehicles (DHSMV) is required to begin to review and

[36] Section 365.171(5), F.S.
[37] *Id.*
[38] Section 365.172(5), F.S.
[39] Section 365.172(5)(b), F.S.
[40] Section 365.172(5) & (6), F.S.
[41] Section 287.012(1), F.S., defines "agency" as any of the various state officers, departments, boards, commissions, divisions, bureaus, and councils and any other unit of organization, however designated, of the executive branch of state government. "Agency" does not include the university and college boards of trustees or the state universities and colleges.
[42] Section 287.012(6), F.S., defines "competitive solicitation" as the process of requesting and receiving two or more sealed bids, proposals, or replies submitted by responsive vendors in accordance with the terms of a competitive process, regardless of the method of procurement.
[43] *See* s. 287.057, F.S.
[44] Section 287.057(1)(a), F.S.
[45] Section 287.057(1)(b), F.S.
[46] Section 287.057(1)(c), F.S.
[47] Sections 287.042(2)(a) and 287.056(1), F.S.

prepare for the development of a secure and uniform system for issuing an optional digital proof of driver license.[48] The statute authorizes DHSMV to contract with one or more private entities to develop a digital proof of driver license system.[49]

The digital proof of driver license developed by DHSMV or by an entity contracted by DHSMV must be in such a format as to allow law enforcement to verify the authenticity of the digital proof of driver license.[50] DHSMV may adopt rules to ensure valid authentication of digital driver licenses by law enforcement.[51] A person may not be issued a digital proof of driver license until he or she has satisfied all of the statutory requirements relating to the issuance of a physical driver license.[52]

Current law also establishes certain penalties for a person who manufacturers or possesses a false digital proof of driver license.[53] Specifically, a person who:

- Manufactures a false digital proof of driver license commits a felony of the third degree, punishable by up to five years in prison[54] and a fine not to exceed $5,000,[55] or punishable under the habitual felony offender statute.[56]
- Possesses a false digital proof of driver license commits a misdemeanor of the second degree, punishable by up to 60 days in prison[57] and a fine not to exceed $500.[58]

Regulation of Money Transmitters and Payment Instrument Sellers

State Regulation

The Office of Financial Regulation (OFR) regulates banks, credit unions, other financial institutions, finance companies, and the securities industry.[59] The OFR's Division of Consumer Finance licenses and regulates various aspects of the non-depository financial services industries, including money services businesses (MSBs) regulated under ch. 560, F.S. Money transmitters and payment instrument sellers are two types of MSBs, and both are regulated under part II of ch. 560, F.S.

[48] Section 322.032(1), F.S.
[49] Section 322.032(2), F.S.
[50] *Id.*
[51] *Id.*
[52] Section 322.032(3), F.S.
[53] Section 322.032(4), F.S.
[54] Section 775.082, F.S.
[55] Section 775.083(1)(c), F.S.
[56] Section 775.084, F.S.
[57] Section 775.082, F.S.
[58] Section 775.083(1)(e), F.S.
[59] Section 20.121(3)(a)2., F.S.

A money transmitter "receives currency,[60] monetary value,[61] or payment instruments[62] 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."[63] A payment instrument seller sells, issues, provides, or delivers a payment instrument.[64] State and federally chartered financial depository institutions, such as banks and credit unions, are exempt from licensure as an MSB.[65]

An applicant for licensure under ch. 560, F.S., must file an application together with an application fee of $375.[66] The license must be renewed every two years by paying a renewal fee of $750.[67] Money transmitters and payment instrument sellers may operate through authorized vendors by providing the OFR specified information about the authorized vendor any by paying a fee of $38 per authorized vendor location at the time of application and renewal.[68] A money transmitter or payment instrument seller may also engage in the activities authorized for check cashers[69] and foreign currency exchangers70 without paying additional licensing fees.[71]

A money transmitter or payment instrument seller must at all times:

- 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.[72]
- 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.[73] 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.[74]
- 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

[60] "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 that are customarily used and accepted as a medium of exchange in a foreign country. s. 560.103(11), F.S.
[61] "Monetary value" means a medium of exchange, whether or not redeemable in currency. s. 560.103(21), F.S.
[62] "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.
[63] Section 560.103(23), F.S.
[64] Section 560.103(30) & (34); *supra* note 62.
[65] Section 560.104, F.S.
[66] Sections 560.141 & 560.143, F.S.
[67] *Id.*; s. 560.142, F.S.
[68] *Id.*; ss. 560.203, 560.205, & 560.208, F.S.
[69] "Check casher" means a person who sells currency in exchange for payment instruments received, except travelers checks. s. 560.103(6), F.S.
[70] "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.
[71] Section 560.204(2), F.S.
[72] Section 560.209, F.S.
[73] *Id.*
[74] *Id.*

States.[75] The OFR may waive the permissible investments requirement if the dollar value of a licensee's outstanding payment instruments and money transmitted do not exceed the bond or collateral deposit.[76]

While MSBs are generally subject to federal anti-money laundering laws,[77] Florida law contains many of the same anti-money laundering reporting requirements and recordkeeping requirements with the added benefit of state enforcement. An MSB applicant must have an anti-money laundering program which meets the requirements of federal law.[78] Pursuant to the Florida Control of Money Laundering in Money Services Business Act, an MSB must maintain certain records of each transaction involving currency or payments 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.[79] An MSB must keep records of each transaction occurring in this state which it knows to involve currency or other payment instruments having a greater value 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.[80] The OFR may take administrative action against an MSB for failure to maintain or produce documents required by ch. 560, F.S., or federal anti-money laundering laws.[81] 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.[82]

A money transmitter or payment instrument seller must maintain specified records for at least five years, including the following:[83]

- A daily record of payment instruments sold and money transmitted.
- A general ledger containing all asset, liability, capital, income, and expense accounts, which must be posted at least monthly.
- Daily settlement records received from authorized vendors.
- Monthly financial institution statements and reconciliation records.
- Records of outstanding payment instruments and money transmitted.
- Records of each payment instrument paid and money transmission delivered.
- A list of the names and addresses of all of the licensee's authorized vendors.
- Records that document the establishment, monitoring, and termination of relationships with authorized vendors and foreign affiliates.
- Any additional records, as prescribed by rule, designed to detect and prevent money laundering.

[75] Section 560.210, F.S.
[76] *Id.*
[77] 31 C.F.R. pt. 1022
[78] Section 560.1401, F.S.
[79] Section 560.123, F.S.
[80] *Id.*
[81] Section 560.114, F.S.
[82] *Id.*
[83] Sections 560.1105 & 560.211, F.S.

Federal Regulation

The Financial Crimes Enforcement Network of the U.S. Department of Treasury (FinCEN) serves as the nation's financial intelligence unit and is charged with safeguarding the U.S. financial system from the abuses of money laundering, terrorist financing, and other financial crimes.[84] The basic concept underlying FinCEN's core activities is "follow the money" because criminals leave financial trails as they try to launder the proceeds of crimes or attempt to spend their ill-gotten profits.[85] To that end, the FinCEN administers the Bank Secrecy Act (BSA).[86] The BSA regulations require banks and other financial institutions, including MSBs, to take a number of precautions against financial crime.[87] The BSA regulations require financial institutions to establish an anti-money laundering program (such as verifying customer identity), maintain certain records (such as transaction related data), and file reports (such as 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.[88]

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.[89] However, if a business provides money transfer services in any amount, it is required to be registered.[90]

FinCEN's BSA regulations define "money transmission services" as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[91] Depending on the facts and circumstances surrounding a transaction, a person transmitting virtual currency may fall under FinCEN's BSA regulations.[92]

Federal law also criminalizes money transmission if the money transmitting business:[93]

- Is operated without a license in a state where such unlicensed activity is subject to criminal sanctions;
- Fails to register with FinCEN; or
- Otherwise involves the transportation or transmission of funds that are known to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity.

---

[84] FinCEN, *What We Do*, https://www.fincen.gov/what-we-do (last visited Jan. 31, 2020).
[85] *Id.*
[86] Many of the federal provisions of the BSA have been codified in ch. 560, F.S., which has provided the OFR with additional compliance and enforcement tools.
[87] *Id.*
[88] *Id.*
[89] 31 C.F.R. § 1010.100 & 1022.380.
[90] *Id.*
[91] 31 C.F.R. § 1010.100.
[92] FinCEN Guidance, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001* (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (last visited Jan. 31, 2020).
[93] 31 U.S.C. § 1960.

Financial Technology

Financial technology, often referred to as "FinTech", encompasses a wide array of innovation in the financial services space. FinTech is technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services.[94] 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.[95] Greater competition and diversity in lending, payments, insurance, trading, and other areas of financial services can create a more efficient and resilient financial system.[96] Drivers of FinTech innovations include technology, regulation, and evolving consumer preferences, including customization.[97]

FinTech innovation is often thought to be synonymous with disruption of the traditional financial services market structure and its providers, such as banks. However, to date, the relationship between incumbent financial institutions and FinTech firms appears to be largely complementary and cooperative in nature.[98] 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.[99] Partnering allows FinTech firms to viably 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.[100] At the same time, incumbents benefit from access to innovative technologies that provide a competitive edge.[101] Yet there are exceptions to this trend, as some FinTech firms have established inroads in credit provision and payments.[102]

III. Effect of Proposed Changes:

Florida Digital Service

Section 1 amends s. 20.22, F.S., to abolish the Division of State Technology and create the Division of Telecommunications and the Florida Digital Service.

Section 2 amends s. 282.0051, F.S, to provide the powers, duties, and functions of the Florida Digital Service. The bill establishes the Florida Digital Service within the Department of Management Services to create innovative solutions that securely modernize and optimize state government and achieve value through digital transformation and interoperability. It creates definitions:

---

[94] 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 Jan. 31, 2020).
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.*

- "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;
- "Enterprise" means the state or the entirety of state government and its subdivisions;
- "Enterprise architecture" means a comprehensive operational framework that contemplates the needs and assets of the enterprise to create a unified information technology environment;
- "Interoperability" means the technical and legal ability to share data across and throughout the enterprise; and
- "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.

The DMS Secretary is required to 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. The state chief information officer must appoint a chief data officer, who will 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.

The Florida Digital Service must develop an enforceable and comprehensive enterprise architecture for all state departments and agencies which:

- Recognizes the unique needs of all stakeholders and results in the publication of standards and terminologies, procurement guidelines, and the facilitation of digital interoperability;
- 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;
- Addresses how hardware, operating systems, legacy systems, and programming and networking solutions may be used or improved to achieve current and future objectives;
- Allows the enterprise architecture to be enforced, as appropriate, to ensure stewardship of tax dollars.

Upon the required production of information from the stakeholders of the enterprise architecture, the Florida Digital Service must:

- 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;
- Develop and publish for each state department and agency a data dictionary that reflects the nomenclature as existing in the comprehensive indexed data catalog;
- Create and maintain an indexed integration catalog that includes all integration tools currently used by each state department and agency;

- Review, confirm, and document operational use cases with all stakeholders across the enterprise architecture including the Legislature and all state departments and agencies;
- Identify core functionality use cases reliant on digital and data infrastructure;
- Develop, collaboratively with stakeholders, solutions for authorized, mandated, or encouraged use cases within the enterprise;
- Develop, publish, and manage an application programming interface to facilitate integration throughout the enterprise;
- Facilitate collaborative analysis of enterprise architecture data to improve service delivery;
- 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;
- 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:
    - 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.
    - 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;
- Architect and deploy applications or solutions to existing department and agency obligations in a controlled and phased approach, including, but not limited to:
    - Digital licenses, including full identification management;
    - Interoperability that contains the data functionality to enable supervisors of elections to authenticate voter eligibility in real time at the point of service;
    - The criminal justice database;
    - Motor vehicle insurance cancellation integration between insurers and the Department of Highway Safety and Motor Vehicles;
    - 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.

The Florida Digital Service may enforce the enterprise architecture by:

- Receiving written notice of any planned or existing procurement of digital solutions which is subject to governance by the enterprise architecture, which includes:
    - An attestation of compliance with the enterprise architecture;
    - A list of integrations tools needed;
    - Enterprise stakeholders actually or potentially involved or affected by the procurement; and
    - Resources that would reduce the cost or increase the speed to deployment.
- 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:

- Delaying the procurement until it complies with the enterprise architecture and
- Providing recommendations to cure the portions of the procurement which do not comply with the enterprise architecture.

Section 3 amends s. 282.318, F.S., to requires the state chief information security officer for the Florida Digital Service, to 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. It also makes technical, conforming changes.

Sections 4, 5, 6, 7, and 8 amend ss. 287.0591, 365.171, 365.172, 365.173, and 943.0415, F.S., respectively, to make technical, conforming changes.

Financial Technology Sandbox

Section 9 creates s. 559.952, F.S., the "Financial Technology Sandbox Act." It creates 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.

The bill creates definitions:

- "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;
- "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;
- "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;
- "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;
- "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;
- "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;

- "Office" means, unless the context clearly indicates otherwise, the Office of Financial Regulation; and
- "Sandbox period" means the period, initially not longer than 24 months, in which the commissioner has:
    - Authorized an innovative financial product or service to be made available to consumers; and
    - 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.

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:

- Chapter 516, consumer finance;
- Chapter 517, securities transactions;
- Chapter 520, retail installment sales;
- Chapter 537, title loans;Part I or part II of chapter 560, general provisions of money services businesses or payment instruments and funds transmission;
- Chapter 655, financial institutions generally;
- Chapter 657, credit unions;
- Chapter 658, banks and trust companies;
- Chapter 660, trust business;
- Chapter 662, family trust companies; and
- Chapter 663, international banking.

During a sandbox period, the commissioner may waive a requirement, or a portion thereof, imposed by a general law or rule in any of the above-listed chapters if all of the following conditions are met:

- The general law or rule does not currently authorize the innovative financial product or service to be made available to consumers;
- The waiver is not broader than necessary to accomplish the purposes and standards specified in this section, as determined by the commissioner; and
- No provision relating to the liability of an incorporator, director, or officer of the applicant is eligible for a waiver.

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 must, by rule, prescribe the form and manner of the application, which must provide for the following:

- The applicant 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;
- 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;

- 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;
- The applicant must submit fingerprints for each individual filing an application under this section and each individual who is substantially involved in the development, operation, or management of the innovative financial product or service for live-scan processing in accordance with rules adopted by the office;
    - The fingerprints may be submitted through a third-party vendor authorized by the Department of Law Enforcement (DLE) to provide live-scan fingerprinting;
    - DLE must conduct the state criminal history background check, and a federal criminal history background check must be conducted through the Federal Bureau of Investigation;
    - All fingerprints submitted to DLE must be submitted electronically and entered into the statewide automated fingerprint identification system and the office must pay an annual fee to DLE to participate in the system and inform DLE of any person whose fingerprints no longer must be retained;
    - The office must review the results of the state and federal criminal history background checks and determine whether the applicant meets the office's requirements; and
    - 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), F.S.

The application must contain, and in determining whether to approve or deny the application the commissioner must consider:

- 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;
- 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, including a statement of arranged capital;
- 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;
- 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;
- A copy of the disclosures required to be provided to consumers; and
- Any other factor that the commissioner determines to be relevant.

The commissioner must 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.

If an application is approved, the commissioner must 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 must 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. A person whose Financial Technology Sandbox application is approved must post a consumer protection bond with the commissioner as security for potential losses suffered by consumers. The commissioner must 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 be increased or decreased at any time based on the risk profile. Unless a bond is enforced, the commissioner must cancel the bond or allow it to expire two years after the date of the conclusion of the sandbox period.

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

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:

- 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 commissioner, under the laws of this state;
- 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;
- That the financial product or service is undergoing testing, may not function as intended, and may entail financial risk;
- 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;
- The expected end date of the sandbox period;
- 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; and
- Any other statements or disclosures required by rule of the commissioner which are necessary to further the purposes of this section.

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.

The commissioner 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 Financial Technology Sandbox to make their products or services available in other jurisdictions; and

- 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.

A person whose Financial Technology Sandbox application is approved by the commissioner must maintain comprehensive records relating to the innovative financial product or service. The person must keep these records for at least five years after the conclusion of the sandbox period. The commissioner may specify by rule additional records requirements. The commissioner may examine the records at any time, with or without notice. All direct and indirect costs of an examination conducted under this subparagraph must be paid by the person making the innovative financial product or service available to consumers.

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 must 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. 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: amendments to general law or rules are necessary to conduct financial technology business in this state permanently or 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.

Unless granted an extension 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 must 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 must 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:

- 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;
- Take necessary legal action; and
- Take other actions authorized by rule by the commissioner which are not inconsistent with this subsection.

A person authorized to make an innovative financial product or service available to consumers must submit a report to the commissioner twice a year as prescribed by rule.

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

Authorization to make an innovative financial product or service available to consumers does not create a property right. 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.

A person who makes an innovative financial product or service available to consumers in the Financial Technology Sandbox is not immune from civil damages for acts and omissions relating to this section and is subject to all criminal and consumer protection laws.

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:

- The person has violated or refused to comply with this section or any rule, order, or decision adopted by the commissioner;
- 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;
- A material error, false statement, misrepresentation, or material omission was made in the Financial Technology Sandbox application; or
- After consultation with the person, 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 commissioner lifts the suspension.

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 must be deemed service on such person.

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.

The office and the commissioner must adopt rules to administer this section. 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 payment of restitution or for enforcement of a bond, or a portion of a bond. The commissioner must use proceeds from such bonds to offset losses suffered by consumers as a result of an innovative financial product or service.

Section 10 provides 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:

Lines 698-827 authorize the Commissioner of Financial Regulation to waive general law and rule requirements, without guidance or limitation. The cornerstone of American democracy known as separation of powers recognizes three separate branches of government—the executive, the legislative, and the judicial—each with its own powers and responsibilities. Florida courts have traditionally applied a strict separation of powers doctrine, stating that no branch may encroach on the powers of another and that no branch may delegate to another branch its constitutionally assigned power. *Chiles v. Children A, B, C, D, E, & F*, 589 So.2d 260, 264 (Fla.1991). This prohibition, known as the nondelegation doctrine, requires that "fundamental and primary policy decisions ... be made by members of the legislature who are elected to perform those tasks, and [that the] administration of legislative programs must be pursuant to some minimal standards and guidelines ascertainable by reference to the enactment establishing the program." *Askew v. Cross Key Waterways*, 372 So.2d 913, 925 (Fla.1978). In other words, statutes granting power to the executive branch "must clearly announce adequate standards to guide ... in the execution of the powers delegated. The statute must so clearly define the power delegated that the [executive] is precluded from acting through whim, showing favoritism, or exercising unbridled discretion." *Lewis v. Bank of Pasco County*, 346 So.2d 53, 55–56 (Fla.1976).

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The bill could result in a positive fiscal impact on state government revenues as it requires certain entities which use the newly-created digital license functionality to pay a per-use fee or purchase a subscription in order to verify the authenticity of a digital identity. The bill specifies that the revenue generated must be collected by DMS and deposited in the working capital trust fund for distribution pursuant to legislative appropriation.

The bill will have an indeterminate fiscal impact on state government expenditures as it expands the current duties of DMS, and it subdivisions, relating to state IT management, places new responsibilities on that department, and creates three new governmental entities: the Florida Digital Service, the Enterprise Architecture Advisory Council, and the Division of Telecommunications. It is unclear if the bill's requirements could be absorbed within DMS's current resources.

The bill will have a negative fiscal impact on the OFR. Under the Financial Technology Sandbox, the fees will be the same as under the existing license in part II of ch. 560, F.S., except that the renewal fee can be prorated because the Financial Technology Sandbox can only be extended for up to one year, whereas the renewed license under part II of ch. 560, F.S., is for a two-year period. Depending on the number of participants and the complexity of oversight, it is possible that the OFR may need more staff. Additionally, the OFR will need to make changes to their information technology infrastructure in order to administer the program. According to the OFR, such changes will cost an estimated $250,115.[103]

VI. Technical Deficiencies:

None.

VII. Related Issues:

At lines 98-103, the bill provides the following definitions:

- "Enterprise" means the state or the entirety of state government and its subdivisions; and
- "Enterprise architecture" means a comprehensive operational framework that contemplates the needs and assets of the enterprise to create a unified information technology environment.

At lines 435-455, the bill authorizes the Florida Digital Service to "enforce the enterprise architecture" by intervening in any planned or existing procurement of digital solutions which is subject to governance by the enterprise architecture that does not comply with the enterprise architecture and delaying the procurement until it complies with the enterprise architecture. This means that the Florida Digital Service may delay a procurement by: any executive branch agency, including Cabinet agencies; the judicial branch; and the Legislature and its agencies.

The bill requires a person making a financial product or service available through the Financial Technology Sandbox to provide consumers a written notice containing a statement that the person

[103] Email from Alex Anderson, Director of Governmental Relations for the OFR, RE: PCS for HB 1391 Fiscal Impact (Feb. 3, 2020).

making the product or service available "is not immune from civil liability for any losses or damages caused by the financial product or service." (Lines 683-635) This seems to suggest an intent that the person retain the same level of liability for losses or damages as if they were operating outside the Sandbox. (Lines 698-731) Given the bill's provisions on waiver of requirements imposed by general law or rule, however, this may not be the case as some potential liability may be based, at least in part, on these requirements.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 20.22, 282.0051, 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 Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.