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:	CS/SB 1870
INTRODUCER:	Innovation, Industry, and Technology Committee and Senators Hutson and Cruz
SUBJECT:	Technological Development
DATE:	February 11, 2020 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Wiehle/Baird	Imhof	IT	**Fav/CS**
2.			BI	
3.			AP	

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 1870 abolishes the Division of State Technology within the Department of Management Services (DMS), replacing it with the Florida Digital Service, which is to create innovative solutions that securely modernize state government, achieve value through digital transformation and interoperability, and fully support the cloud-first policy. The Florida Digital Service is to develop a comprehensive enterprise architecture that: recognizes the unique needs of those included within the enterprise, supports the cloud-first policy, and addresses how information technology infrastructure may be modernized to achieve cloud-first objectives. "Enterprise" means state agencies, including the Department of Legal Affairs, the Department of Agriculture and Consumer Services, the Department of Financial Services, and the judicial branch.

The bill creates the Enterprise Architecture Advisory Council within DMS to meet at least semiannually to discuss implementation, management, and coordination of the enterprise architecture; identify potential issues and threats with specific use cases; and recommend proactive solutions.

The bill creates, effective January 1, 2021, the Financial Technology Sandbox within the Office of Financial Regulation to allow financial technology innovators to test new products and services in a supervised, flexible regulatory sandbox using exceptions of specified general law and waivers of the corresponding rule requirements under defined conditions. It provides that the creation of a supervised, flexible regulatory sandbox provides a welcoming business

environment for technology innovators and may lead to significant business growth.

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

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;

---

[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.

- Recommending open data[9] 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, 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.

[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.
[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. 282.0041, F.S., to create definitions:

- "Credential service provider" means a provider competitively procured by the department to supply secure identity management and verification services based on open standards to qualified entities;

---

[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.*

- "Data-call" means an electronic transaction with the credential service provider that verifies the authenticity of a digital identity by querying enterprise data;
- "Electronic" means technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities;
- "Electronic credential" means a digital asset which verifies 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, the Department of Financial Services, and the judicial branch;
- "Enterprise architecture" means a comprehensive operational framework that contemplates the needs and assets of the enterprise to support interoperability across state government;
- "Interoperability" means the technical ability to share and use 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 department, meets usage criteria, agrees to terms and conditions, and is subsequently and prescriptively authorized by the department to access data under the terms of that agreement.

Section 3 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 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 revises provisions throughout the section which currently give DMS oversight and management authority over agency information technology projects to instead give the Florida Digital Service this oversight and management authority over agency projects that have an information technology component. In the provision for the Florida Digital Service to perform project oversight on all state agency information technology projects that have an information technology component with a total project cost costs of $10 million or more and that are funded in the General Appropriations Act or any other law, the bill requires the Florida Digital Service to establish a process for state agencies to apply for an exception to these requirements for a specific project with an information technology component. In the provision requiring that, notwithstanding any other law, the Florida Digital Service must provide project oversight on any project with an information technology component of the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services which has a total project cost of $25 million or more and which impacts one or more other agencies, the bill similarly requires the Florida Digital Service to establish a process for these departments to apply for an exception for a specific project with an information technology component.

The DMS Secretary is required to appoint a state chief information officer to head the Florida Digital Service, and the state chief information officer must appoint a chief data officer.

The Florida Digital Service must develop a comprehensive enterprise architecture for all state departments and agencies that:

- Recognizes the unique needs of those included within the enterprise that results in the publication of standards, terminologies, and procurement guidelines to facilitate digital interoperability;
- Supports the cloud-first policy; and
- Addresses how information technology infrastructure may be modernized to achieve cloud-first objectives.

The Florida Digital Service, pursuant to legislative appropriation:

- Create 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;
- Develop and publish, in collaboration with the enterprise, a data dictionary for each agency that reflects the nomenclature in the comprehensive indexed data catalog;
- Review and document use cases across the enterprise architecture;
- Develop and publish standards that support the creation and deployment of application programming interfaces to facilitate integration throughout the enterprise;
- Facilitate collaborative analysis of enterprise architecture data to improve service delivery;
- Develop plans to 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;
- Publish standards necessary to facilitate a secure ecosystem of data interoperability that is compliant with the enterprise architecture and allows for a qualified entity to access enterprise's data under the terms of the agreements with the department; and
- Publishing standards that facilitate the deployment of applications or solutions to existing enterprise obligations in a controlled and phased approach.

Pursuant to legislative authorization and subject to appropriation, the department may procure a credential service provider through a competitive process to supply secure identity management and verification services to qualified entities based on open standards. The department also may enter into agreements with qualified entities. The terms of the agreements between the department, the credential service provider and the qualified entities must be based on the per-data-call or subscription charges to validate and authenticate and allow the department to recover any state costs for implementing and administering a solution. 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.

All revenues generated from the agreements with the credential service provider and qualified entities must be remitted to the department, and the department must deposit these revenues into the Department of Management Services Operating Trust Fund for distribution pursuant to a legislative appropriation and department agreements with the credential service provider and qualified entities.

The Florida Digital Service may develop a process to:

- Receive written notice from the state agencies within the enterprise of any planned or existing procurement of an information technology project that is subject to governance by the enterprise architecture;
- Intervene in any planned procurement by a state agency so that the procurement complies with the enterprise architecture; and
- Report to the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project within the judicial branch that does not comply with the enterprise architecture.

Section 4 amends s. 282.00515, F.S. It deletes the current provisions requiring the Cabinet agencies, the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services, to either adopt statutory information technology standards or adopt alternative standards based on best practices and industry standards, and authorizes the agencies to contract with DMS to provide information technology services. It replaces this with provisions creating the Enterprise Architecture Advisory Council, a 13-member group that is to meet at least semiannually to discuss implementation, management, and coordination of the enterprise architecture; identify potential issues and threats with specific use cases; and recommend proactive solutions.

Section 5 amends s. 282.318, F.S., to require the state chief information officer to appoint the state chief information security officer for the Florida Digital Service.

Sections 6, 7, 8, 9, and 10 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" effective January 1, 2021.

Creation of the Sandbox

The bill creates the Financial Technology Sandbox within the Office of Financial Regulation to allow financial technology innovators to test new products and services in a supervised, flexible regulatory sandbox, using exceptions of specified general law and waivers of the corresponding rule requirements under defined conditions. The creation of a supervised, flexible regulatory sandbox provides a welcoming business environment for technology innovators and may lead to significant business growth.

Definitions

The bill creates definitions:

- "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;

- "Financial product or service" means a product or service related to finance, including securities, consumer credit, or money transmission, which is traditionally subject to general law or rule requirements in chapters 560, 516, 517, 520, or 537, F.S., and which is under the jurisdiction of the office;
- "Financial Technology Sandbox" means the program which allows a person to make an innovative financial product or service available to consumers during a sandbox period through an exception to general laws or and a waiver of rule requirements;
- "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;
- "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 office 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 an exception to general law or a waiver of the corresponding rule requirements, as determined by the office, so that authorization is possible.

Sandbox Application

Before filing an application to enter the Financial Technology 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.

Before making an innovative financial product or service available to consumers in the Financial Technology Sandbox, a person must file an application with the office. The commission must prescribe by rule the form and manner of the application. In the application, the person 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 Financial Technology Sandbox, including all relevant technical details;
- 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 regarding the applicant's current and proposed capitalization;
- 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 person substantially 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, their 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 person substantially involved in the development, operation, or management of the applicant's innovative financial product or service; and
- Any other factor that the office determines to be relevant.

A business entity filing an application 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 a person applies on behalf of a business entity intending to make an innovative financial product or service available to consumers, the person must obtain the consent of the business entity.

The office shall approve or deny in writing a Financial Technology Sandbox application within 60 days after receiving the completed application. The office and the applicant may jointly agree to extend the time beyond 60 days. Consistent with this section, the office may impose conditions on any approval. In deciding to approve or deny an application, the office must consider the above-listed information in the application.

The office may not approve an application if the applicant had a prior Financial Technology Sandbox application that was approved and that related to a substantially similar financial product or service or if any person substantially involved in the development, operation, or management of the applicant's innovative financial product or service was substantially involved with another Financial Technology Sandbox applicant whose application was approved and whose application related to a substantially similar financial product or service.

Upon approval of an application, the office must specify the general law or rule requirements, or portions thereof, for which an exception or rule waiver is granted during the sandbox period and the length of the initial sandbox period, not to exceed 24 months. The office 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 person making the financial product or service available.

Sandbox Operation

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 office may, on a case-by-case basis and after consultation with the person who makes the financial product or service available to consumers, specify the maximum number of consumers authorized to receive an innovative financial product or service. The office may not authorize more than 15,000 consumers to receive the financial product or service until the person who makes the financial product or service available to consumers has filed the first required biennial report. After the filing of the first report, if the person demonstrates adequate financial capitalization, risk management process, and management oversight, the office 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 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 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 person making the financial product or service available.

The office 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.

A person whose Financial Technology Sandbox application is approved by the office must maintain comprehensive records relating to the innovative financial product or service. The person must keep these records for at least 5 years after the conclusion of the sandbox period. The commission may specify by rule additional records requirements. The office may examine the records at any time, with or without notice.

Sandbox Period Extension and Conclusion

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. A complete application for an extension must be filed with the office at least 90 days before the conclusion of the initial sandbox period. The office 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 a minimum, consider the current status of the factors previously considered in deciding to approve or deny an application to enter the Financial Technology 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 office, and approval is pending.

At least 30 days before the conclusion of the initial sandbox period or the extension, whichever is later, 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 extension and may not make the financial product or service available to any new consumers after the conclusion of the initial sandbox period or the extension, whichever is later, until legal authority outside of the Financial Technology Sandbox exists 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.

Exceptions of General Law and Waivers of Rules

The bill provides that if an application to enter the sandbox is approved for a person who otherwise would be subject to the provisions of chapters 560, 516, 517, 520, or 537, F.S., the following provisions are not be applicable to the approved sandbox participant:

- Section 560.1105, F.S., which provides records retention requirements for money services businesses;
- Section 560.118, F.S., which requires money services businesses to file annual financial audit reports;
- Section 560.125, F.S., except for s. 560.125(2), F.S., which provides for unlicensed activities by money services businesses and penalties for these activities, with subsection (2) providing that only a money services business licensed under Part II may appoint an authorized vendor;
- Section 560.128, F.S., which provides that a money services business and an authorized vendor must provide each customer with a toll-free telephone number, or the address and telephone number of the office, and which authorizes the Financial Services Commission to require, by rule, that a licensee display its license at each business location;
- Section 560.1401, F.S., except for s. 560.1401(2)-(4) , F.S., with subsections (1) and (5), which are excepted, requiring that an applicant for licensure as a money services business demonstrate to the office the character and general fitness necessary to command the confidence of the public and warrant the belief that the money services business or deferred presentment provider shall be operated lawfully and fairly and provide the office with all

information required under the chapter and related rules, and with subsections (2)-(4), which are not excepted, requiring that an applicant be legally authorized to do business in this state, be registered as a money services business with the Financial Crimes Enforcement Network, and have an anti-money laundering program in place which meets federal requirements;

- Section 560.141, F.S., except for s. 560.141(1)(b)-(d), F.S., which establishes the requirements for application for a license as a money services business, with paragraph (b) requiring a nonrefundable application fee, paragraph (c) requiring submission of fingerprints, and paragraph (d) requiring a copy of the applicant's written anti-money laundering program;
- Section 560.142, F.S., except that the office may prorate the license renewal fees provided in ss. 560.142 and 560.143, F.S., for an extension, which provides for license renewal;
- Section 560.143(2), F.S., to the extent necessary for proration of the renewal fee;
- Section 560.205, F.S., except for s. 560.205(1) and (3), F.S., which provides additional license application requirement, with subsection (2) requiring a sample form of payment instrument and subsection (4) requiring a copy of the applicant's most recent financial audit report, and with subsection (1) requiring a sample vendor contract and subsection (3) requiring documents demonstrating that net worth and bonding requirements have been met;
- Section 560.208, F.S., except for s. 560.208(3)-(6), F.S., which provides requirements for conduct of business, with subsections (1)-(2) authorizing a licensee to conduct business at one or more branches or by means of authorized vendors and to charge a different price for a money transmitter based on the mode of transmission and subsections (3)-(6) making the licensee responsible for acts of its authorized vendors and requiring the licensee to place a customer's property in a segregated account in a federally insured financial institution, to ensure that money transmitted is available to the designated recipient within 10 business days after receipt, and to immediately upon receipt of currency or payment instrument provide a confirmation or sequence number to the customer verbally, by paper, or electronically;
- Section 560.209, F.S., except that the office may modify the net worth, corporate surety bond, and collateral deposit amounts required, with the modified amounts be in such lower amounts that the office determines to be commensurate with the considerations under paragraph (4)(e) and the maximum number of consumers authorized to receive the financial product or service under this section; s. 560.209, F.S., provides minimum net worth, surety bond, and collateral deposit requirements;
- Section 516.03, F.S., except for the license and investigation fee. The office may prorate the license renewal fees for an extension granted under subsection (8). The office may not waive the evidence of liquid assets of at least $25,000; s. 516.03, F.S., provides for an application to make loans under the consumer finance chapter;
- Section 516.05, F.S., except that the office may make an investigation of the facts concerning the applicant's background, with this section providing for the license to make loans under the consumer finance chapter;
- Section 516.12, F.S., which provides licensee recordkeeping requirements;
- Section 516.19, F.S., which provides penalties for violations of specified sections of chapter 516, F.S.;
- Section 517.07, F.S., which provides for registration of securities to be sold in this state;
- Section 517.12, F.S., which requires registration of all securities dealers, associated persons, and issuers of securities;

- Section 517.121, F.S., which requires each dealer, investment adviser, branch office, associated person, or intermediary to maintain such books and records as the commission may prescribe by rule, and requires the Office of Financial Regulation to, at intermittent periods, examine their affairs and books and records;
- Section 520.03, F.S., except for the application fee, with this section providing for licenses to engage in the business of a motor vehicle retail installment seller;
- Section 520.12, F.S., which provides penalties for violation of provisions relating to retail installment sales;
- Section 520.25, F.S., which provides penalties for a violation of the provisions on retail installment sales of distributed energy generation systems;
- Section 520.32, F.S., except for the application fee, which provides for licenses to engage in retail installment transactions: The office may prorate fees for an extension;
- Section 520.39, F.S., which provides penalties for violations involving retail installment transactions;
- Section 520.52, F.S., except for the application fee, which provides for licensees for a sales finance company: The office may prorate fees for an extension;
- Section 520.57, F.S., which provides penalties for violations relating to engages in the business of a sales finance company;
- Section 520.63, F.S., except for the application fee, which provides for licensees engaging in or transacting business as a home improvement finance seller: The office may prorate fees for an extension;
- Section 520.98, F.S., which provides penalties for violations of provisions relating to home improvement finance sales;
- Section 520.997, F.S., which requires every licensee to maintain, at the principal place of business, such books, accounts, and records as will enable the office to determine whether the business is being operated in accordance with the provisions of chapter 520, F.S.;
- Section 537.004, F.S., except for s. 537.004(2) and (5), F.S., which provides for licenses for title loan lenders: The office may prorate fees for an extension;
- Section 537.005, F.S., except that the office may modify the required corporate surety bond amount, which provides for applications for licenses for title loan lenders;
- Section 537.007, F.S., which provides remedies for title loans made without a license;
- Section 537.009, F.S., which provides requirements for recordkeeping by a title loan lender; and
- Section 537.015, F.S., which provides criminal penalties for acting as a title loan lender without first obtaining the required license.

During a sandbox period, these exceptions are applicable if all of the following conditions are met:

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

Notwithstanding any other provision of law, upon approval of a Financial Technology Sandbox application, the office may grant an applicant a waiver of a requirement, or a portion thereof, which is imposed by rule as authorized by any of the following provisions of general law, if all of the above conditions.

Report

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, at a minimum, include financial reports and the number of consumers who have received the financial product or service.

Construction

A person whose Financial Technology Sandbox application is approved must be deemed licensed under the applicable exceptions to general law or waiver of the rule requirements unless the person's authorization to make the financial product or service available to consumers under this section has been revoked or suspended.

Violations and Penalties

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 statutes and any other statute not specifically excepted.

The office 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, a rule of the commission, an order of the office, or a condition placed by the office on the approval of the person's Financial Technology Sandbox application;
- A fact or condition exists that, if it had existed or become known at the time that the Financial Technology Sandbox application was pending, would have warranted denial of the application or the imposition of material conditions;
- 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 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 Financial Technology Sandbox is not feasible, service on the office shall be deemed service on such person.

Rules and Orders

The commission must adopt rules to administer this section.

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

Effective Date

Section 10 provides that, except as otherwise expressly provided, the bill takes effect July 1, 2020. This refers to the sandbox provisions, which take effect January 1, 2021.

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:

The bill *may* be interpreted authorize executive branch employees, not the Legislature, to determine the application of general law, without guidance or limitation. See VII Related Issues 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 its subdivisions, relating to state IT management, places new responsibilities on that department, and creates two new governmental entities: the Florida Digital Service and the Enterprise Architecture Advisory Council. 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]

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

VI. Technical Deficiencies:

None.

VII. Related Issues:

There is some uncertainty as to how some of the sandbox provisions on exceptions to general law will be interpreted and applied. The bill provides the following provisions.

- In the application [to enter the sandbox], the person 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." (Lines 806-810)
- "If the application [to enter the sandbox] is approved for a person who otherwise would be subject to the provisions of chapters 560, 516, 517, 520, or 537, the following provisions shall not be applicable to the approved sandbox participant" (Lines 996-1000); and
- "During a sandbox period, the exceptions granted in paragraph (a) are applicable if all of the following conditions are met:
  - The general law or corresponding rule currently prevents the innovative financial product or service to be made available to consumers.
  - The exceptions or rule waivers are not broader than necessary to accomplish the purposes and standards specified in this section, as determined by the office." (Lines 1063-1071)

The exceptions to general law provisions appear to except application of *all* listed to every sandbox participant, which would negate the provisions for specification of specific general law for which an exception is sought and for approval of an application and application of the exceptions only if *the* general law prevents making the product or service available and the exceptions are not broader than necessary to accomplish the purposes and standards. If, on the other hand, the latter provisions are given effect, in essence reading something like an "as appropriate, on a case by case basis" standard into the exception provision, this raises an unlawful delegation of legislative authority issue as the employee making the determinations of applicability and lack of overbreadth would be determining which statutes apply, not the Legislature. See IV E. Other Constitutional Issues.

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 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 910-913) It also provides that a person who makes an innovative product or service available in the sandbox is not immune from civil damages for acts and omissions relating to this section and is subject to all criminal statutes. (Lines 1089-1095) 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. Given the bill's provisions on exceptions of requirements imposed by general law or waiver of the corresponding rule requirements (989-1075), however, this may not be the case as some potential liability and criminal acts 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 Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

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 find 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.