

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/CS/HB 1391 Technology Innovation

SPONSOR(S): Government Operations & Technology Appropriations Subcommittee; Insurance & Banking Subcommittee; Grant, J. and Toledo

TIED BILLS: CS/HB 1393, CS/HB 1395 **IDEN./SIM. BILLS:** CS/SB 1870

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Insurance & Banking Subcommittee	14 Y, 0 N, As CS	Hinshelwood	Cooper
2) Government Operations & Technology Appropriations Subcommittee	9 Y, 2 N, As CS	Mullins	Topp
3) State Affairs Committee		Toliver	Williamson

SUMMARY ANALYSIS

The Division of State Technology (DST) within the Department of Management Services (DMS) oversees information technology governance and security for the executive branch of state government. The bill:

- Abolishes DST, establishes the Florida Digital Service (FDS) in its place, and creates the Division of Telecommunications within DMS.
- Places new duties and responsibilities under the newly created FDS and expands the duties and responsibilities currently assigned to DMS and DST, including the development and implementation of enterprise information technology systems.
- Tasks FDS with procuring a credential service provider for identity management and verification services.
- Requires that revenue generated from allowing qualified entities to utilize state identity data be deposited into the working capital trust fund.
- Removes the option for cabinet agencies to adopt alternative information technology architecture, project management, and reporting standards than those developed by DMS, and requires cabinet agencies to adhere to enterprise architecture standards developed by FDS.
- Creates the Enterprise Architecture Advisory Council as a 13-member advisory council within DMS.
- Removes DST as the head of the E911 system in Florida, and places the Division of Telecommunications as its new head.

The Office of Financial Regulation (OFR) regulates money services businesses, which include money transmitters and payment instrument sellers. The bill creates the Financial Technology Sandbox (sandbox) within OFR to allow a person to make an innovative financial product or service available to consumers as a money transmitter or payment instrument seller during a sandbox period that is initially not longer than 24 months but which can be extended one time for up to 12 months. The sandbox provides regulatory flexibility by permitting OFR to waive specified statutes and corresponding rule requirements. OFR may initially authorize a sandbox participant to provide the financial product or service to a maximum of 15,000 consumers but may authorize up to 25,000 consumers if the sandbox participant demonstrates adequate financial capitalization, risk management process, and management oversight. In addition to other statutes that OFR may waive, OFR may modify the net worth, corporate surety bond, and collateral deposit amounts required for money transmitters and payment instrument sellers. The modified amounts must be in such lower amounts that OFR determines to be commensurate with specified considerations regarding the sandbox application and commensurate with the maximum number of consumers authorized to receive the product or service under the sandbox.

The bill has no fiscal impact on local governments and an indeterminate fiscal impact on state government and the private sector.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Department of Management Services

Information Technology Management

The Department of Management Services (DMS)¹ oversees information technology (IT)² governance and security for the executive branch of state government. The Division of State Technology (DST) within DMS, established in 2019 through the merger of the former Agency for State Technology (AST) and the Division of Telecommunications,³ implements DMS' duties and policies in this area.⁴

The head of DST is appointed by the Secretary of Management Services⁵ and serves as the state chief information officer (CIO).⁶ The CIO must be a proven effective administrator with at least 10 years of executive level experience in the public or private sector.⁷ 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."⁸

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 agencies⁹ 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 data¹⁰ technical standards and terminologies for use by state agencies;

¹ See s. 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 Ch. 2019-118, L.O.F.

⁴ S. 20.22(2)(a), F.S.

⁵ 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.

⁶ S. 20.22(2)(b), F.S.

⁷ *Id.*

⁸ *State Technology, DMS*, https://www.dms.myflorida.com/business_operations/state_technology (last visited Jan. 27, 2020).

⁹ See s. 282.0041(27), F.S.

¹⁰ 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.¹¹

State Data Center and the Cloud-First Policy

In 2008, the Legislature created the State Data Center (SDC) system, established two primary data centers,¹² and required that agency data centers be consolidated into the two primary data centers.¹³ Data center consolidation was completed in fiscal year (FY) 2013-14. In 2014, the two primary data centers were merged to create the SDC.¹⁴ The SDC is established within DMS and DMS provides operational management and oversight of the SDC.¹⁵

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.¹⁶ The SDC must:

- Offer, develop, and support the services and applications defined in service-level agreements executed with its customer entities;¹⁷
- 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, that 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 SDC services to third-party cloud-computing services procured by a customer entity.

A state agency is prohibited, unless exempted¹⁸ 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.¹⁹

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

¹¹ S. 282.0051, F.S.

¹² The Northwood Shared Resource Center and the Southwood Shared Resource Center. Ss. 282.204-282.205, F.S. (2008).

¹³ Ch. 2008-116, L.O.F.

¹⁴ Ch. 2014-221, L.O.F.

¹⁵ See s. 282.201, F.S.

¹⁶ S. 282.201, F.S.

¹⁷ The term “customer entity” means an entity that obtains services from DMS. S. 282.0041(7), F.S.

¹⁸ 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.

¹⁹ S. 282.201(3), F.S.

provider interaction.”²⁰ 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.²¹ 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.²²

IT Security

The IT Security Act²³ establishes requirements for the security of state data and IT resources.²⁴ DMS must designate a state chief information security officer (CISO) to oversee state IT security.²⁵ The CISO must have expertise in security and risk management for communications and IT resources.²⁶ 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;
 - 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.
- Reviewing the strategic and operational IT security plans of executive branch agencies annually.²⁷

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.²⁸ In part, the heads of state agencies must 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.²⁹

²⁰ *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.

²¹ S. 282.206(1), F.S.

²² S. 282.206(2) and (3), F.S.

²³ S. 282.318, F.S., is cited as the “Information Technology Security Act.”

²⁴ S. 282.318, F.S.

²⁵ S. 282.318(3), F.S.

²⁶ *Id.*

²⁷ S. 282.318(3), F.S.

²⁸ S. 282.318(4)(a), F.S.

²⁹ S. 282.318(4), F.S.

United States Digital Service

In 2014, President Obama created the United States Digital Service (USDS) to help federal agencies improve the digital services they provide to the public.³⁰ The USDS has two primary responsibilities, distributing guidance related to IT development and procurement to other federal agencies, and actively helping federal agencies develop digital services by embedding teams within the agencies' in-house technology divisions. USDS has created two guidebooks to help federal agencies improve and develop better digital services: the digital services playbook and the TechFAR handbook. The digital services playbook is designed to help government agencies build effective digital services that work well for users by utilizing private and public sector best practices.³¹ The TechFAR handbook explains to federal agencies how they can execute the digital services playbook in ways consistent with federal procurement policy.³²

Enhanced 911 (E911) System

DST oversees the E911 system in Florida.³³ DST must develop, maintain, and implement the statewide emergency communications E911 system plan.³⁴ The plan must provide for:

- The public agency emergency communications requirements for each entity of local government³⁵ 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.³⁶

DST is responsible for implementing and coordinating the plan, and must adopt any necessary rules and schedules related to public agencies³⁷ implementing and coordinating the plan.³⁸

The Secretary of Management Services, or his or her designee, is the director of the E911 system and serves as chair of the E911 Board.³⁹ The director of the E911 system is authorized to coordinate the activities of the system with state, county, local, and private agencies.⁴⁰ The director must consult, cooperate, and coordinate with local law enforcement agencies.⁴¹ An "E911 Board," composed of 11 members, administers funds derived from fees imposed on each user of voice communications service with a Florida billing address (place of primary use).⁴² The Governor appoints five members who are county 911 coordinators and five members from the telecommunications industry.⁴³ The E911 Board

³⁰ White House, *Delivering a Customer-Focused Government Through Smarter IT*, <https://obamawhitehouse.archives.gov/blog/2014/08/11/delivering-customer-focused-government-through-smarter-it> (last visited Feb. 24, 2020).

³¹ USDS, *Digital Services Playbook*, <https://playbook.cio.gov/> (last visited Feb. 24, 2020).

³² White House, *Delivering a Customer-Focused Government Through Smarter IT*, <https://obamawhitehouse.archives.gov/blog/2014/08/11/delivering-customer-focused-government-through-smarter-it> (last visited Feb. 24, 2020); see also USDS, *TechFAR Hub*, <https://techfarhub.cio.gov/> (last visited Feb. 24, 2020).

³³ S. 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.

³⁴ S. 365.171(4), F.S.

³⁵ The term "local government" means any city, county, or political subdivision of the state and its agencies. S. 365.171(3)(b), F.S.

³⁶ S. 365.171(4), F.S.

³⁷ The term "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.

³⁸ S. 365.171(4), F.S.

³⁹ S. 365.172(5)(a), F.S.

⁴⁰ S. 365.171(5), F.S.

⁴¹ *Id.*

⁴² S. 365.172(5), F.S.

⁴³ S. 365.172(5)(b), F.S.

makes disbursements from the Emergency Communications Number E911 System Trust Fund to county governments and wireless providers.⁴⁴

Agency Procurements

Agency⁴⁵ 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,⁴⁶ unless otherwise authorized by law:⁴⁷

- 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.⁴⁸
- 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.⁴⁹
- 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.⁵⁰

DMS is responsible for procuring state term contracts for commodities and contractual services from which state agencies must make purchases.⁵¹

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) must begin to review and prepare for the development of a secure and uniform system for issuing an optional digital proof of driver license.⁵²

The digital proof of driver license must be in such a format as to allow law enforcement to verify the authenticity of the digital proof of driver license.⁵³ DHSMV may adopt rules to ensure valid authentication of digital driver licenses by law enforcement.⁵⁴ 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.⁵⁵

⁴⁴ S. 365.172(5) and (6), F.S.

⁴⁵ The term “agency” means 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. S. 287.012(1), F.S.

⁴⁶ The term “competitive solicitation” means 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. S. 287.012(6), F.S.

⁴⁷ See s. 287.057, F.S.

⁴⁸ S. 287.057(1)(a), F.S.

⁴⁹ S. 287.057(1)(b), F.S.

⁵⁰ S. 287.057(1)(c), F.S.

⁵¹ Ss. 287.042(2)(a) and 287.056(1), F.S.

⁵² S. 322.032(1), F.S.

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ S. 322.032(3), F.S.

Current law also establishes certain penalties for a person who manufactures or possesses a false digital proof of driver license.⁵⁶ 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 prison⁵⁷ and a fine not to exceed \$5,000,⁵⁸ or punishable under the habitual felony offender statute.⁵⁹
- Possesses a false digital proof of driver license commits a misdemeanor of the second degree, punishable by up to 60 days in prison⁶⁰ and a fine not to exceed \$500.⁶¹

The 2019 General Appropriations Act in Specific Appropriation 2743 provides funding for DHSMV to procure a credential service provider.⁶² On December 17, 2019, DHSMV issued a Request for Quotes (RFQ) for a credential service provider solution to support digital driver license qualified entities and electronic credential service providers. DHSMV intends to contract for this service by March 2020.⁶³

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.⁶⁴ The Division of Consumer Finance within OFR 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.

A money transmitter receives currency,⁶⁵ monetary value,⁶⁶ or payment instruments⁶⁷ 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.⁶⁸ A payment instrument seller sells, issues, provides, or delivers a payment instrument.⁶⁹ State and federally chartered financial depository institutions, such as banks and credit unions, are exempt from licensure as an MSB.⁷⁰

An applicant for a MSB license under ch. 560, F.S., must file an application with OFR and pay an application fee of \$375.⁷¹ The license must be renewed every two years by paying a renewal fee of \$750.⁷² Money transmitters and payment instrument sellers may operate through authorized vendors by providing OFR with specified information about the authorized vendor and by paying a fee of \$38

⁵⁶ S. 322.032(4), F.S.

⁵⁷ S. 775.082, F.S.

⁵⁸ S. 775.083(1)(c), F.S.

⁵⁹ S. 775.084, F.S.

⁶⁰ S. 775.082, F.S.

⁶¹ S. 775.083(1)(e), F.S.

⁶² Operational Work Plan for proviso in ch. 2019-115, s. 2743, Laws of Florida, submitted on Dec. 16, 2019, by DHSMV (on file with the Government Operations & Technology Appropriations Subcommittee).

⁶³ DHSMV RFQ, FLHSMV-RFQ-078-19 (on file with the Government Operations & Technology Appropriations Subcommittee).

⁶⁴ S. 20.121(3)(a)2., F.S.

⁶⁵ The term “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.

⁶⁶ The term “monetary value” means a medium of exchange, whether or not redeemable in currency. S. 560.103(21), F.S.

⁶⁷ The term “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.

⁶⁸ S. 560.103(23), F.S.

⁶⁹ S. 560.103(30) and (34), F.S.; *supra* note 62.

⁷⁰ S. 560.104, F.S.

⁷¹ Ss. 560.141 and 560.143, F.S.

⁷² *Id.*; s. 560.142, F.S.

per authorized vendor location at the time of application and renewal.⁷³ A money transmitter or payment instrument seller may also engage in the activities authorized for check cashers⁷⁴ and foreign currency exchangers⁷⁵ without paying additional licensing fees.⁷⁶

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.⁷⁷
- 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.⁷⁸ 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.⁷⁹
- Possess permissible investments, such as cash and certificates of deposit, with an aggregate market value of at least the aggregate face amount of all outstanding money transmissions and payment instruments issued or sold by the licensee or an authorized vendor in the United States.⁸⁰ 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.⁸¹

While MSBs are generally subject to federal anti-money laundering laws,⁸² 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 that meets the requirements of federal law.⁸³

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 payment instruments in order to deter the use of a money services business to conceal proceeds from criminal activity and to ensure the availability of such records for criminal, tax, or regulatory investigations or proceedings.⁸⁴ 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.⁸⁵ 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.⁸⁶ 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.⁸⁷

A money transmitter or payment instrument seller must maintain specified records for at least five years, including the following:⁸⁸

- 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.

⁷³ *Id.*; ss. 560.203, 560.205, and 560.208, F.S.

⁷⁴ The term "check casher" means a person who sells currency in exchange for payment instruments received, except travelers checks. S. 560.103(6), F.S.

⁷⁵ The term "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.

⁷⁶ S. 560.204(2), F.S.

⁷⁷ S. 560.209, F.S.

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ S. 560.210, F.S.

⁸¹ *Id.*

⁸² 31 C.F.R. pt. 1022.

⁸³ S. 560.1401, F.S.

⁸⁴ S. 560.123, F.S.

⁸⁵ *Id.*

⁸⁶ S. 560.114, F.S.

⁸⁷ *Id.*

⁸⁸ Ss. 560.1105 and 560.211, F.S.

- 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.

Federal Regulation

The Financial Crimes Enforcement Network of the United States Department of Treasury (FinCEN) serves as the nation's financial intelligence unit and is charged with safeguarding the United States financial system from the abuses of money laundering, terrorist financing, and other financial crimes.⁸⁹ 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.⁹⁰ To that end, FinCEN administers the Bank Secrecy Act (BSA).⁹¹ BSA regulations require banks and other financial institutions, including MSBs, to take a number of precautions against financial crime.⁹² 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.⁹³

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.⁹⁴ However, an MSB must register with FinCEN if it provides money transfer services in any amount.⁹⁵

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."⁹⁶ Depending on the facts and circumstances surrounding a transaction, a person transmitting virtual currency may fall under FinCEN's BSA regulations.⁹⁷

Federal law criminalizes money transmission if the money transmitting business:⁹⁸

- 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.

⁸⁹ FinCEN, *What We Do*, <https://www.fincen.gov/what-we-do> (last visited Feb. 20, 2020).

⁹⁰ *Id.*

⁹¹ Many of the federal provisions of the BSA have been codified in ch. 560, F.S., which has provided OFR with additional compliance and enforcement tools.

⁹² *Supra* note 87.

⁹³ *Id.*

⁹⁴ 31 C.F.R. § 1010.100 and 1022.380.

⁹⁵ *Id.*

⁹⁶ 31 C.F.R. § 1010.100.

⁹⁷ 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).

⁹⁸ 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.⁹⁹ 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.¹⁰⁰ Greater competition and diversity in lending, payments, insurance, trading, and other areas of financial services can create a more efficient and resilient financial system.¹⁰¹ Drivers of FinTech innovations include technology, regulation, and evolving consumer preferences, including customization.¹⁰²

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.¹⁰³ 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.¹⁰⁴ 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.¹⁰⁵ At the same time, incumbents benefit from access to innovative technologies that provide a competitive edge.¹⁰⁶ Yet there are exceptions to this trend, as some FinTech firms have established inroads in credit provision and payments.¹⁰⁷

Effect of the Bill

State Information Technology

The bill abolishes DST and establishes the Florida Digital Service (FDS) in its place. FDS is a subdivision of DMS. The bill provides that the mission of FDS is to “create innovative solutions that securely modernize state government and achieve value through digital transformation and interoperability.” The bill expands the duties and responsibilities currently assigned to DMS and DST and assigns new duties and responsibilities to FDS. The bill provides that FDS is tasked with the following *new* duties and responsibilities:

- Creating and maintaining a comprehensive indexed data catalog.
- Developing and publishing a data dictionary for each agency.
- Developing solutions for authorized, mandated, or encouraged use cases in collaboration with the enterprise.¹⁰⁸
- Reviewing and documenting use cases across the enterprise architecture (EA).¹⁰⁹

⁹⁹ 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).

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ The bill defines “enterprise” to mean the collection of state agencies as defined in s. 282.0041, F.S., except that the term includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, the Department of Financial Services, and the judicial branch of government.

¹⁰⁹ The bill defines “enterprise architecture” to mean a comprehensive operational framework that contemplates the needs and assets of the enterprise to support interoperability across state government.

- Developing, publishing, and managing an application programming interface to facilitate integration throughout the enterprise.
- Facilitating collaborative analysis of EA data to improve service delivery.
- Providing a testing environment in which any newly developed solution can be tested for compliance with the EA and for functionality assurance before deployment.
- Creating the functionality necessary for a secure ecosystem of data interoperability that is compliant with the EA and allowing a qualified entity to access the stored data.
- Developing a process to receive written notice from state agencies within the enterprise of any planned or existing procurement of an IT project that is subject to governance by the EA.
- Developing a process to intervene in any planned procurement so that it complies with the EA.
- Requiring FDS to report to the Governor, the President of the Senate, and the Speaker of the House of Representatives on any IT project within the judicial branch that does not comply with the EA.
- Requiring the state CIO appoint a chief data officer (CDO). The CDO reports to the CIO and is included in the Senior Management Service class of the Florida Retirement System.
- Requiring FDS to develop a comprehensive EA for the enterprise that:
 - Recognizes the unique needs of those within the enterprise and results in the publication of standards and terminologies, procurement guidelines, and the facilitation of digital interoperability;
 - Supports the state's cloud-first policy; and
 - Addresses how IT infrastructure may be modernized to achieve current and future cloud-first objectives.
- Requiring FDS to develop and deploy applications or solutions to existing enterprise obligations in a controlled and phased approach including:
 - Digital licenses, including full identification management;
 - Interoperability that enables 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 DHSMV;
 - 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; and
 - Interoperability solutions to support military members and their families.

The bill makes the following changes to the duties and responsibilities of FDS currently in law:

- Expands the types of agency projects over which FDS has oversight from state agency IT projects that have a total cost of \$10 million or more and cabinet agency IT projects that have a total cost of \$25 million or more, to projects meeting those thresholds with *any* technology component;
- Requires FDS to identify opportunities for standardization and consolidation of IT services that support interoperability and the state's cloud-first policy;
- Requires FDS to develop and implement other payment mechanisms to recover the cost of SDC services through charges to the applicable customer entities; and
- Eliminates the requirement that FDS conduct an annual market analysis to determine whether the state's approach to SDC services is the most effective and cost-efficient manner by which customer entities can acquire such services.

In addition to the duties described above, FDS also must procure a credential service provider (CSP), pursuant to legislative authorization and subject to appropriation. The CSP is a provider that supplies secure identity management and verification services based on open standards to qualified entities. DMS is required to enter into agreements with electronic credential providers (ECP) that have the technological capabilities necessary to integrate with the CSP as well as:

- Ensure secure validation and authentication of data;
- Meet usage criteria;

- Agree to terms and conditions, privacy policies, and uniform remittance terms relating to the consumption of a digital driver license or identification; and
- Include clear, enforceable, and significant penalties for violating the agreements.

The bill provides that the agreements between DMS and the CSP, ESP, and qualified entities¹¹⁰ must be based on the per-data-call¹¹¹ or subscription charges to validate and authenticate a digital license or identification card. All revenue generated must be remitted to DMS and deposited in the DMS Operating Trust Fund for distribution pursuant to legislative appropriation. However, the revenue may not be derived from sources other than the per-data-call or subscription charges.

Once a qualified entity or an ECP signs the EA terms of service and privacy policy, the FDS must provide appropriate access to the stored data to facilitate authorized integrations to collaboratively solve enterprise use cases.

The bill creates the Enterprise Architecture Advisory Council (Council) as an advisory council¹¹² within DMS. The Council is composed of 13 members appointed to staggered terms of four years. The Council consists of:

- Four members appointed by the Governor;
- The director of the Office of Policy and Budget in the Executive Office of the Governor, or the person acting in the director's capacity should the position be vacant;
- The Secretary of Management Services or the person acting in the secretary's capacity should the position be vacant;
- The state CIO or the person acting in the CIO's capacity should the position be vacant;
- One member appointed by the Chief Justice of the Florida Supreme Court;
- One member appointed by the President of the Senate;
- One member appointed by the Speaker of the House of Representatives;
- The CIO of the Department of Financial Services or the person acting in the CIO's capacity should the position be vacant;
- The CIO of the Department of Legal Affairs or the person acting in the CIO's capacity should the position be vacant;
- The CIO of the Department of Agriculture and Consumer Services or the person acting in the CIO's capacity should the position be vacant.

The Council must meet semiannually beginning October 1, 2020, to discuss implementation, management, and coordination of the EA; identify potential issues and threats with specific use cases; and recommend proactive solutions.

The bill re-establishes the Division of Telecommunications within DMS and places the Division of Telecommunications as the new head of the E911 system in Florida.

Financial Technology Sandbox

The bill creates the Financial Technology Sandbox (sandbox) within OFR to allow financial technology innovators to test new products and services in a supervised, flexible regulatory sandbox, using waivers of specified general law and corresponding rule requirements under defined conditions.

The sandbox allows a person to make an innovative financial product or service available to consumers as a money transmitter or payment instrument seller during a period that is initially not longer than 24

¹¹⁰ The bill defines "qualified entity" to mean a public or private entity or individual that enters into a binding agreement with DMS, 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.

¹¹¹ The bill defines "data-call" to mean an electronic transaction with the CSP that verifies the authenticity of a digital identity by querying enterprise data.

¹¹² The term "council" or "advisory council" means an advisory body created by specific statutory enactment and appointed to function on a continuing basis for the study of the problems arising in a specified functional or program area of state government and to provide recommendations and policy alternatives. S. 20.03(7), F.S.

months but which can be extended one time for up to 12 months. A “financial product or service” is a product or service related to money transmitters and payment instrument sellers, including mediums of exchange that are in electronic or digital form, which is subject to general law or corresponding rule requirements in the enumerated statutes that may be waived by OFR. “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.

The bill authorizes OFR to waive the following statutes and corresponding rule requirements for purposes of the sandbox:

- Section 560.1105, F.S., relating to records retention.
- Section 560.118, F.S., relating to reports.
- Section 560.125, F.S., relating to unlicensed activity; penalties. However, OFR may not waive the portion of the statute that permits only a money services business licensed as a money transmitter or payment instrument seller to appoint an authorized vendor.
- Section 560.128, F.S., relating to customer contacts; license display.
- Section 560.1401, F.S., relating to licensing standards. However, OFR may not waive the portions of the statute that require an applicant to be legally authorized to do business in this state, to be licensed with FinCEN (if applicable), and to have an anti-money laundering program in place.
- Section 560.141, F.S., relating to license application. However, OFR may not waive the portions of the statute that impose a licensing fee, require fingerprints and background checks, and require the applicant to provide a copy of the applicant’s anti-money laundering program.
- Section 560.142, F.S., relating to license renewal. However, OFR may prorate, but may not entirely waive, the license renewal fees for an extension granted under the sandbox.
- Section 560.143(2), F.S., relating to license renewal fees, to the extent necessary for proration of the renewal fee.
- Section 560.205, F.S., relating to additional license application requirements. However, OFR may not waive portions of the statute requiring an applicant to provide a sample authorized vendor contract (if applicable) and documents demonstrating that the net worth and bond requirements have been fulfilled.
- Section 560.208, F.S., relating to conduct of business. However, OFR may not waive portions of the statute making a licensee responsible for the acts of its authorized vendors, requiring a licensee to place customer assets in a segregated account in a federally insured financial institution, and requiring a licensee to ensure that money transmitted is available to the designated recipient within 10 business days after receipt.
- Section 560.209, F.S., relating to net worth; corporate surety bond; collateral deposit in lieu of bond. However, OFR may modify, but may not entirely waive, the net worth, corporate surety bond, and collateral deposit amounts. The modified amounts must be in such lower amounts that OFR determines to be commensurate with specified considerations regarding the sandbox application and commensurate with the maximum number of consumers authorized to receive the financial product or service under the sandbox.

OFR may grant a waiver if the general law or corresponding rule currently prevents the innovative financial product or service to be made available to consumers. No provision relating to the liability of an incorporator, director, or officer of the applicant is eligible for a waiver. The waiver must not be broader than necessary to accomplish the purposes and standards of the sandbox, as determined by OFR.

Before filing a sandbox application, 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 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. 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.

In the sandbox application, the applicant must specify the general law or rule requirements for which a 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 following information, which OFR must consider in deciding whether to approve or deny an application:

- The nature of the innovative financial product or service proposed to be made available to consumers in the 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.
- Whether 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, a property-based offense, or a crime involving moral turpitude or dishonest dealing. A plea of no contest, a conviction, or a finding of guilt must be reported under this subparagraph regardless of adjudication.
- A copy of specified 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.
- Any other factor OFR determines to be relevant.

OFR may not approve an application if:

- The applicant had a prior sandbox application that was approved and that related to a substantially similar financial product or service; or
- Any person substantially involved in the development, operation, or management of the applicant's innovative financial product or service was substantially involved in such with another sandbox applicant whose application was approved and whose application related to a substantially similar financial product or service.

OFR must approve or deny in writing an application within 60 days after receiving the completed application, though OFR and the applicant may jointly agree to extend the time beyond 60 days. OFR may impose conditions on any approval, consistent with the sandbox. Upon approval of an application, OFR must specify the general law or rule requirements, or portions thereof, for which a waiver is granted during the sandbox period and the length of the initial sandbox period, not to exceed 24 months.

A person whose sandbox application is approved must be deemed licensed under part II of ch. 560, F.S., unless the person's authorization to make the financial product or service available to consumers under the sandbox has been revoked or suspended.

OFR must post on its website notice of the approval of the application, a summary of the innovative financial product or service, and the contact information of the person making the financial product or service available.

OFR 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. OFR may not authorize more than 15,000 consumers to receive the financial product or service until the sandbox participant has filed the first report required under the sandbox. After the filing of the report, if the person demonstrates adequate financial capitalization, risk management process, and management oversight, OFR may authorize up to 25,000 consumers to receive the financial product or service.

The person making the financial product or service available must provide a written statement to the consumer, which must contain an acknowledgement from the consumer, of all of the following information:

- 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 OFR under the laws of Florida.
- That the 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.
- Any other statements or disclosures required by rule of the Financial Services Commission (commission), which are necessary to further the purposes of this section.

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

A sandbox participant must maintain comprehensive records relating to the innovative financial product or service and must keep these records for at least five years after the conclusion of the sandbox period. The commission may specify by rule additional records requirements. OFR may examine these records at any time, with or without notice.

A sandbox participant may apply for an extension of the initial sandbox period for up to 12 additional months. 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.
- 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 OFR, and approval is pending.

A complete application for an extension must be filed at least 90 days before the conclusion of the initial sandbox period. OFR must approve or deny the application for extension in writing at least 35 days before the conclusion of the initial sandbox period. In deciding to approve or deny an application for extension of the sandbox period, OFR must, at a minimum, consider the current status of the factors previously considered at the time of application for the initial sandbox period.

At least 30 days before the conclusion of the initial sandbox period or the extension, whichever is later, the sandbox participant must provide written notification to consumers regarding the conclusion of the initial sandbox period or the extension and may not make the financial product or service available to any new consumers after the conclusion of the initial sandbox period or the extension, whichever is later, until legal authority outside of the sandbox exists to make the financial product or service available to consumers. After the conclusion of the sandbox period or the extension, whichever is later, the person 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.
- Take other actions authorized by commission rule, which are not inconsistent with the sandbox.

A sandbox participant must submit a report to OFR twice a year as prescribed by rule. The report must, at a minimum, include financial reports and the number of consumers who have received the financial product or service.

A sandbox participant is not immune from civil damages and is subject to all criminal and consumer protection laws.

OFR may, by order, revoke or suspend authorization granted to a sandbox participant if:

- The sandbox participant has violated or refused to comply with the sandbox statute, a rule of the commission, an order of OFR, or a condition placed by OFR on the approval of the person's sandbox application;
- A fact or condition exists that, if it had existed or become known at the time that the sandbox application was pending, would have warranted denial of the application or the imposition of material conditions;
- A material error, false statement, misrepresentation, or material omission was made in the sandbox application; or
- After consultation with the person, continued testing of the innovative financial product or service would be likely to harm consumers or would no longer serve the purposes of the sandbox 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 OFR lifts the suspension. OFR 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 sandbox participant is not feasible, service on OFR is deemed service on such person.

The commission must adopt rules to administer the sandbox. OFR may issue all necessary orders to enforce the sandbox statute and may enforce these orders in accordance with ch. 120, F.S., or in any court of competent jurisdiction. These orders include, but are not limited to, orders for payment of restitution for harm suffered by consumers as a result of an innovative financial product or service.

B. SECTION DIRECTORY:

Section 1. Amends s. 20.22, F.S., relating to DMS.

Section 2. Amends s. 282.0041, F.S., creating definitions for “credential service provider,” “data-call,” “electronic,” “electronic credential,” “electronic credential provider,” “enterprise,” “enterprise architecture,” “interoperability,” and “qualified entity.”

Section 3. Amends s. 282.0051, F.S., relating to FDS; powers, duties, and functions.

Section 4. Amends s. 282.00515, F.S., relating to the EA Advisory Council.

Section 5. Amends s. 282.318, F.S., relating to security of data and IT.

Section 6. Amends s. 287.0591, F.S., relating to IT.

Section 7. Amends s. 365.171, F.S., relating to emergency communications number E911 state plan.

Section 8. Amends s. 365.172, F.S., relating to emergency communications number "E911."

Section 9. Amends s. 365.173, F.S., relating to Communications Number E911 System Fund.

Section 10. Amends s. 943.0415, F.S., relating to Cybercrime Office.

Section 11. Creates s. 560.214, F.S., relating to the sandbox.

Section 12. For FY 2020-2021, provides an appropriation to OFR to implement the sandbox.

Section 13. Provides an effective date of January 1, 2021, except as otherwise provided.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

The bill may result in a positive fiscal impact on state government revenues as it requires certain entities that use the newly created electronic credential 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 all revenue generated must be remitted to DMS and deposited in the DMS Operating Trust Fund for distribution pursuant to legislative appropriation.

The bill may also result in a negative impact on state agencies that currently derive revenues from data transactions such as DHSMV (driver license related data), the Department of Health (vital statistics certificates), and the Florida Department of Law Enforcement (criminal history records). In FY 2018-19, DHSMV received \$82.8 million related to public records requests for driver license related data, as authorized in Florida Statutes. This includes the records and fees authorized in ss. 322.20 and 320.05(3)(b)8., F.S. This revenue supports DHSMV operations including the Florida Highway Patrol.¹¹³

2. Expenditures:

The bill will have a negative, significant fiscal impact on state government expenditures as it considerably expands the current duties of DMS, and its subdivisions, relating to state IT management, and places new responsibilities on DMS. It is unclear what if any of the bill's requirements could be absorbed within DMS's current resources. The current DST has no resources or staffing for application development nor for the implementation and maintenance of procured systems. The current Office of the State CIO within DST has four staff for project oversight – a task that is considerably expanded in the bill. The bill also adds review of all planned state agency information technology procurements subject to the EA, a significant workload that cannot be handled with the five current strategic planning coordinators within DST.

The bill may have a negative, significant fiscal impact on cabinet agencies, each of which are currently authorized in law to optionally develop its own standards for IT infrastructure, project management, and reporting, independent from those standards established by DST. It is unknown as to the scope and cost of remediation that may be necessary for these agencies to adhere to new enterprise standards developed by FDS.

The bill may have a negative, significant fiscal impact on state agencies and the judicial branch. It is unknown as to the scope and cost of remediation that may be necessary for these entities to adhere to new EA standards developed by FDS.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The impact of the sandbox on the private sector is indeterminate, as it is unknown how many businesses may participate, what types of products or services such businesses would offer, and how many consumers in total would be offered the products or services.

¹¹³ Email from Suzie Carey, Chief Financial Officer for DHSMV (Feb. 7, 2020).
STORAGE NAME: h1391c.SAC
DATE: 3/1/2020

D. FISCAL COMMENTS:

No funding has been requested by DMS or provided in the bill for the new and expanded responsibilities identified in the bill, except for the establishment of a data catalog as requested in DMS' FY 2020-21 legislative budget request, which has been funded in both the House of Representatives and Senate appropriations bills. Most of the new FDS duties are subject to legislative appropriation.

The bill will have a negative fiscal impact on OFR. Under the 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 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, OFR may need more staff. Additionally, OFR will need to make changes to its IT infrastructure in order to administer the program. According to OFR, such changes will cost an estimated \$250,115.¹¹⁴ The bill appropriates \$50,000 in nonrecurring funds for FY 2020-2021 from the Administrative Trust Fund for the amount that cannot be funded out of existing appropriations within OFR.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. This bill does not appear to affect county or municipal governments.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill requires the commission¹¹⁵ to adopt rules to administer the sandbox. Section 560.105(2), F.S., appears to grant the commission with sufficient authority to promulgate the rules required by the bill.

C. DRAFTING ISSUES OR OTHER COMMENTS:

- The bill expands DMS project oversight from “information technology projects” to projects with an “information technology component,” which is not defined in the bill or in current law.
- The bill requires FDS to create functionality that allows qualified entities to “access stored data,” but “stored data” is not defined, and the bill does not provide authority for FDS to access, share, or monetize other agencies’ data, which would be needed for FDS to procure a CSP and to enter into revenue sharing agreements.
- DHSMV has already been funded in the 2019 General Appropriations Act to procure a CSP and plans to execute a contract by March 2020. The bill does not address this duplication of effort.
- The bill does not identify what types or combinations of state data are authorized to be provided to qualified entities, nor does it identify usage criteria or for what authorized purposes qualified entities may be provided certain state data.
- There are no provisions in the bill to ensure the authorized use of state data. DHSMV and other states’ departments of motor vehicles have had to revoke records access with requesting parties for misuse or abuse of data.¹¹⁶
- While the bill does require that agreements with ECPs include clear, enforceable, and significant penalties for violations of the agreements, it is unknown what penalty mechanisms are available

¹¹⁴ Email from Alex Anderson, Director of Governmental Relations for the OFR, RE: PCS for HB 1391 Fiscal Impact (Feb. 3, 2020).

¹¹⁵ The commission is composed of the Governor, Attorney General, Chief Financial Officer, and Commissioner of Agriculture. S. 20.121(3), F.S. The commission members are OFR’s agency head for the purpose of rulemaking. S. 20.121(3)(c), F.S.

¹¹⁶ See Joseph Cox, *DMVs Are Selling Your Data to Private Investigators*, VICE NEWS (Sept. 5, 2019), https://www.vice.com/en_us/article/43kxqzq/dmvs-selling-data-private-investigators-making-millions-of-dollars (last visited Feb. 20, 2020).

to FDS for violations. Additionally, this penalty language in the bill only applies to ECPs and not to qualified entities.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On February 4, 2020, the Insurance & Banking Subcommittee considered a proposed committee substitute and reported the bill favorably as a committee substitute. The committee substitute:

- Creates the EA Advisory Council.
- Removes a provision that allowed FDS to use best practices instead of the procurement procedures in ch. 287, F.S.
- Requires DMS to enter into agreements with certain entities regarding digital licenses and requires that revenues resulting from the agreements be deposited into the working capital trust fund.
- Removes a provision requiring the CISO to have 10 years of experience.
- Provides additional definitions.
- Narrows the scope of the sandbox to focus on money transmitters and payment instrument sellers.
- Makes other technical and conforming changes.

On February 11, 2020, the Government Operations & Technology Appropriations Subcommittee adopted one amendment and reported the bill favorably as a committee substitute. The committee substitute:

- Removes provisions governing the experience required for the State Chief Information Officer.
- Removes provisions governing the experience required for the Chief Data Officer.
- Requires that certain duties of the FDS be pursuant to legislative appropriation.
- Requires that procurement of a credential service provider and agreements with qualified entities be pursuant to legislative authorization and subject to appropriation.
- Requires all revenues generated from agreements with the credential service provider and qualified entities be remitted to DMS.
- Changes the fund for the depositing of revenues from the working capital trust fund to the DMS Operating Trust Fund.
- Clarifies the contract with the credential service provider allow the enterprise to use the service at no cost.
- Requires FDS to report to the Governor, the President of the Senate, and the Speaker of the House of Representatives on any IT project within the judicial branch that does not comply with the enterprise architecture.
- Changes the membership of the Enterprise Architecture Advisory Council.
- Makes other technical and conforming changes.

The analysis is drafted to the committee substitute as approved by the Government Operations & Technology Appropriations Subcommittee.