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 Governmental Oversight and Accountability

BILL:	SB 1570
INTRODUCER:	Senator Hooper
SUBJECT:	Information Technology Reorganization
DATE:	March 25, 2019
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Hackett	McVaney	GO	**Favorable**
2.			AEG	
3.			AP	

I. Summary:

SB 1570 makes changes in law relating to state agency information technology. Specifically, the bill:

- Transfers the Agency for State Technology, with all of its existing powers, duties, functions, personnel, records, property, and funds, including the state data center, to the Department of Management Services as the newly created Division of State Technology. The bill repeals the statute authorizing the Agency for State Technology.
- Clarifies that the Department of Environmental Protection will review practices related to geospatial data.
- Codifies the Statewide Travel Management System to standardize and maintain records of travel for all state executive and judicial branch agencies.
- Enacts a "cloud-first" policy to require all state agencies to show a preference for cloud-computing systems in their procurements process for new information technology.
- Creates a task force to study cybersecurity procedures, rules, and vulnerabilities and make recommendations thereupon.

The fiscal impact on state expenditures is indeterminate.

The bill takes effect July 1, 2019.

II. Present Situation:

Agency for State Technology

Chapter 282, F.S., is known as the Enterprise Information Technology Services Management Act.[1]

[1] Section 282.003, F.S.

General duties

The Agency for State Technology (AST) was created on July 1, 2014.[2] The executive director of AST is appointed by the Governor, subject to confirmation by the Senate. The duties and responsibilities of the AST include:[3]

- Developing and publishing information technology (IT) policy for management of the state's IT resources.
- Establishing and publishing IT architecture standards.
- Establishing project management and oversight standards with which state agencies must comply when implementing IT projects.
- Performing project oversight on all state IT projects with total costs of $10 million or more.
- Identifying opportunities for standardization and consolidation of IT services that support common business functions and operations.
- Establishing best practices for procurement of IT products in collaboration with the DMS.
- Participating with the DMS in evaluating, conducting and negotiating competitive solicitations for state term contracts for IT commodities, consultant services, or staff augmentation contractual services.
- Collaborating with the DMS in IT resource acquisition planning.
- Developing standards for IT reports and updates.
- Upon request, assisting state agencies in development of IT related legislative budget requests.
- Conducting annual assessments of state agencies to determine compliance with IT standards and guidelines developed by the AST.
- Providing operational management and oversight of the state data center.
- Recommending other IT services that should be designed, delivered, and managed as enterprise IT services.
- Recommending additional consolidations of agency data centers or computing facilities into the state data center.
- In consultation with state agencies, proposing methodology for identifying and collecting current and planned IT expenditure data at the state agency level.
- Performing project oversight on any cabinet agency IT project that has a total project cost of $25 million or more and impacts one or more other agencies.
- Consulting with departments regarding risks and other effects for IT projects implemented by an agency that must be connected to or accommodated by an IT system administered by a cabinet agency.
- Establishing policy for all IT-related state contracts, including state term contracts for IT commodities, consultant services, and staff augmentation services in collaboration with the DMS.[4] The IT policy must include:
    - Identification of the IT product and service categories to be included in state term contracts.
    - Requirements to be included in solicitations for state term contracts.
    - Evaluation criteria for the award of IT-related state term contracts.

[2] Chapter 2014-221, L.O.F.
[3] Section 282.0051, F.S.
[4] Chapter 2016-138, L.O.F.

- The term of each IT-related state term contract.
- The maximum number of vendors authorized on each state term contract.

Chief Information Officer

The AST is headed by an executive director, established in Section 20.61(1) F.S., who serves as the state's chief information officer and is appointed by the Governor and confirmed by the Senate. Current law requires that the state CIO preferably have executive-level experience in both the public and private sectors in development and implementation of information technology strategic planning; management of enterprise information technology projects, particularly management of large-scale consolidation projects; and development and implementation of fiscal and substantive information technology policy.

State Data Center

The state data center is housed within the AST and provides data center services that comply with applicable state and federal laws, regulations, and policies, including all applicable security, privacy, and auditing requirements.[5] The state data center must enter into a service-level agreement with each customer entity to provide required type and level of service or services. If a customer fails to execute an agreement within 60 days after commencement of service, the state data center may cease service.

State agencies, unless authorized by the Legislature or granted exemption by AST, may not:[6]

- Transfer existing computer services to any data center other than the State Data Center.
- Initiate a new computer service except with the State Data Center.

The state data center relies heavily on the use of state-owned equipment installed at the state data center facility located in the state's Capital Circle Office Center in Tallahassee for the provision of data center services, often financed through the Department of Financial Services' Consolidated Equipment Financing Program and through lease-purchase arrangements with hardware vendors. This equipment must be replaced periodically, usually around five years.

Information Technology Security

Section 282.318, F.S., establishes the requirements for the security of data and IT. The AST's duties in regards to IT security include:

- Establishing standards and processes for IT security consistent with generally accepted best practices.
- Adopting rules for IT security.
- Developing a statewide IT security strategic plan, updated annually.
- Developing a framework for use by state agencies for IT security responsibilities such as conducting IT security risk assessments and reporting IT security incidents.
- Providing IT security training for state agency information security managers.
- Annually reviewing state agency IT security plans.

[5] Section 282.201, F.S.
[6] Section 282.201(5), F.S.

Section 282.318(4)(h), F.S., requires that each state agency head include appropriate IT security requirements in written specifications for the solicitation of IT and IT resources and services that are consistent with the rules and guidelines established by the AST and DMS.

Cloud-First Policy

Cloud computing is the delivery of on-demand computing resources, including data center services, software applications, and data storage, over the Internet on a pay-for-use basis. The definition of cloud computing issued by the National Institute of Standards and Technology (NIST) in Special Publication 800-145 is the most broadly adopted definition of cloud computing.[7] The NIST definition describes the essential characteristics of cloud computing, the types of cloud computing service models, and the types of cloud computing deployment models.

Section 282.0051(6), F.S., provides the duty for the AST to collaborate with the Department of Management Services (DMS) to establish best practices for the procurement of information technology (IT) products in order to reduce costs, increase productivity, or improve services.

Section 282.318 (4) (h). F.S., requires that each state agency head include appropriate IT security requirements in written specifications for the solicitation of IT and IT resources and services that are consistent with the rules and guidelines established by the AST and DMS.

Several states including California, Colorado, Illinois, Michigan, and Texas have adopted a cloud-first policy. Some states have cloud strategies and plans with cloud computing components or are in the process of working to formalize policies and standards for cloud services.[8] The federal government has also implemented a cloud-first policy, first adopted by President Obama in 2011[9] and continued by President Trump in 2017.[10]

Technology Program in the Department of Management Services

The Technology Program is organized as the Division of Telecommunications and provides the state enterprise telecommunications system known as the SUNCOM Network. SUMCOM includes voice, data, radio, wiring and cabling, and conferencing service to state agencies, local governments, educational institutions, libraries, and non-profit organizations.[11] The Division also leads Emergency Support Functions (ESF 2)[12] and E-rate[13] and houses the Bureau of Public Safety, which provides Enhanced 911[14] and radio communications services to the state's public safety entities.[15]

[7] SP 800-145, The NIST Definition of Cloud Computing, (9/2011), National Institute of Standards and Technology.
[8] "State Government Practices for Cloud Implementation", (2015), National Association of State Procurement Officials.
[9] "Federal Cloud Computing Strategy", (2011), Vivek Kundra, Office of the U.S. Chief Information Officer.
[10] Executive Order No. 82 FR 22391, 3 C.F.R. 22391-22397 (2017).
[11] Section 282.703, F.S.
[12] DMS, as the lead agency for ESF 2 under the direction of the Division of Emergency Management, is the first point of contract for telecommunications service providers for equipment and services coordination to provide communications support statewide before, during, and after emergencies.
[13] E-Rate is a federal program created to ensure that schools and libraries have affordable access to advance telecommunications services.
[14] Section 365.171, F.S.
[15] Sections 282.709 and 282.7101, F.S.

Type Two Transfer

Section 20.06(2), F.S., provides for type two transfers. A type two transfer is the merging into another agency or department of an existing agency or department or a program, activity, or function thereof. A type two transfer preserves the merged entity's statutory powers, duties, rules, and functions, and the merged entity's records, personnel, property, and funds unless specifically severed or abolished. Pursuant to Rule 60L-33.003, Florida Administrative Code, if a transfer of an employee is legislatively mandated, the employee retains the status held in the position prior to the time of transfer unless the legislature directs otherwise. This rule means that the employee is transferred to the new entity and retains the employee's status in the originating agency, either probationary status, trainee status or permanent status.

Career Service System

An employee of the state of Florida will generally fall into one of four categories provided by Chapter 110, Florida Statutes:

- Career Service System;
- Senior Management System;
- Volunteers; or
- Selected Exempt Service System.

The systems provide the pay schedules, benefits, and certain policies for each class of employee. Section 110.205, F.S., provides that all non-exempt employees belong to the career service system. Section 110.205(2)(e), F.S., exempts the executive director of the Agency for State Technology from the Career Service System. Section 110.205(n) allows each department head to designate a maximum of 20 policymaking or managerial positions as being exempt from the Career Service System. A department head may additionally designate one position which directly reports to the department head in the Senior Management Service.

Task Force Requirements under 20.03, Florida Statutes

Section 20.03(8), F.S., defines "task force" to mean an "advisory body created without specific statutory enactment for a time not to exceed 1 year or created by specific statutory enactment for a time not to exceed 3 years and appointed to study a specific problem and recommend a solution or policy alternative related to that problem." This provision specifies that the existence of a task force terminates upon the completion of its assignment.

III. Effect of Proposed Changes:

Section 1 authorizes a type two transfer of AST to DMS pursuant to s. 20.06(2), F.S. This includes transferring all of AST's powers, duties, functions, records, offices, personnel, property, issues, contracts, authority, rules, funds, etc. Organizationally, the AST structure is merged with the Technology Program within DMS (see section 3 below). Pursuant to s. 20.06(2)(c), F.S., all administrative rules of the AST remain in effect after the type two transfer.

Section 2 provides that all contracts and interagency agreements involving AST are continued following the transfer.

Section 3 creates the Division of State Technology within DMS, directed by the state chief information officer. This division is a result of a merger of the existing Technology Program and the AST structure. It sets minimum qualifications for the state chief information officer similar to the current qualifications found in s. 20.61, F.S., but adds a 10-year experience requirement.

Section 4 continues the transfer of certain duties to the Department of Environmental Protection, relating to geospatial data, beyond the current expiration date of July 1, 2019. The DEP must review policies, practices, and standards related to all geospatial data managed by state agencies and water management districts. The section allows the Department of Environmental Protection to adopt rules to that end.

Section 5 repeals s. 20.61, F.S., which created the Agency for State Technology.

Section 6 grants rulemaking authority to the DMS relating to the Statewide Travel Management System. The Statewide Travel Management System is defined as the system developed by DMS to collect data on, standardize and automate travel management for public officers and employees. The section requires all executive branch state agencies and the judicial branch to report travel using the Statewide Travel Management System. The section also states that the travel reports may not reveal confidential or exempt information.

Section 7 changes the short title for Chapter 282, F.S., to the "Information Technology Management Act."

Section 8 define the terms "agency assessment," "breach," "cloud computing," "data," and "open data."

Section 9 amends s. 282.0051, F.S., to shift the current statutory powers, duties, and functions of the AST to the DMS. In addition, the section:

- Removes the duty to review all information technology purchases by state agencies which cost $250,000 or more.
- Requires reports on projected costs for data center services to be sent to the Office of Policy and Budget rather than to each customer entity's agency head.
- Adds a duty to recommend methods of standardizing data as well as open data technical standards.

Section 10 amends s. 282.201, F.S., relating to the state data center. The section moves the state data center from the AST to DMS, and provides that the department will appoint a director for the state data center.

In addition, Section 10 requires the state data center to enter into service-level agreements with its customers and establish the costs of each service by agency application.

Section 10 also requires the state data center to show a preference for cloud-computing solutions in its procurement process, and it shall assist customer entities in transitioning from state data center use to third-party cloud-computing services.

Section 11 creates s. 282.206, F.S., to establish a cloud-first policy for state agencies. This policy provides that, in their procurement processes, each state agency shall show a preference for cloud-computing services that does not require, or minimizes, the use of state data center infrastructure. It provides that each agency will create procedures for the evaluation of cloud-computing options and a plan with regards to its use of the state data center. Each agency must notify the state data center by May 31 and November 30 of each year regarding changes in its use of the state data center.

Section 12 amends s. 282.318, F.S., to shift the current statutory duties of the AST to the DMS, relating to information technology security DMS is required to designate a state chief information security officer. Agencies must consult with the DMS regarding their information technology and cybersecurity needs.

Section 12 requires information technology resources and services to meet or exceed the applicable state and federal laws, regulations, and standards. Current law provides that standards are set by the AST.

Section 13 amends s. 17.0315, F.S., to replace the executive director of the AST with the state chief information officer on the financial and cash management system task force.

Section 14 amends s. 20.055, F.S., to remove the reference to AST in the definition of "state agency."

Section 15 amends s. 97.0525 to replace AST with DMS in a reference to their risk assessment methodology for identifying security risks.

Section 16 amends s. 110.205, F.S., to exempt the chief information officer from the state career service. Division heads are separately exempt under s. 110.205(j), F.S. In moving from an agency to a division head position, the AST structure will no longer enjoy the 20 designated exempt positions. Those positions will fall under DMS's umbrella and no longer be exempt unless designated by the head of DMS.

Section 17 amends s. 215.322, F.S., to state that the state chief information officer, rather than the AST, must review requests to use electronic collection methods and consult with the chief financial officer on uniform security safeguards for cardholder data.

Section 18 amends s. 215.96, F.S., to replace the executive director of the AST with the state chief information officer on the coordinating council under the Florida Financial Management Information System Act.

Section 19 amends s. 287.057, F.S., to replace the AST with the chief information officer as the consulting entity for the DMS maintaining a program for online procurement of commodities and contractual services.

Section 20 amends s. 282.00515, F.S., replaces the AST with the DMS as the body with whom several departments may contract for various technological services pursuant to s. 282.0051, F.S.

Section 21 amends s. 287.0591, F.S., to replace the executive director of the AST with the state chief information officer as the person who may certify that long term contracts are beneficial to the state. It also states that the Division of State Technology, rather than the AST, may participate in DMS's competitive solicitations for information technology commodities, consultant services, or staff augmentation services.

Section 22 amends s. 365.171, F.S., to replace the Technology Program with the Division of State Technology in the definition for "office" as used in s. 365.171, F.S., emergency communications number "E911."

Section 23 amends s. 365.172, F.S., to replace the Technology Program with the Division of State Technology in the definition for "office" as used in ss. 365.171, 365.172, 365.173, and 365.174, F.S., emergency communications number E911 state plan.

Section 24 amends s. 365.173, F.S., to replace the Technology Program with the Division of State Technology as the location of the fund created to hold revenue from fees and subscriptions in the E911 system.

Sections 25 and 26 amend ss. 445.011 and 445.045, F.S., respectively, to replace the executive director of the AST with the state chief information officer as the person with whom CareerSource Florida, Inc., shall coordinate.

Section 27 amends s. 668.50, F.S., to replace the AST with the DMS as the body who may specify various regulations and procedures regarding electronic records under the Uniform Electronic Transaction Act.

Section 28 amends s. 943.0415, F.S., to replace the AST with the DMS as the body with whom the Cybercrime Office of the Department of Law Enforcement is to consult.

Section 29 creates the Florida Cybersecurity Task Force. The task force is to:
- Recommend methods to secure the State's network systems and data,
- Identify and recommend remedy for high-risk cybersecurity issues,
- Recommend a process to regularly asses cybersecurity infrastructure,
- Identify gaps in the state's cybersecurity infrastructure,
- Recommend improvements to the cybersecurity of emergency management and disaster response systems,
- Recommend cybersecurity improvements for the state data center, and
- Recommend improvements relating to the state's operational plans for the response to a cybersecurity attack.

The task force is to be chaired by the Lieutenant Governor or her designee, and composed of at least 9 additional members, to include:
- A representative of the computer crime center of the Department of Law Enforcement;
- A representative of the fusion center of the Department of Law Enforcement;
- The state chief information officer;
- The state chief information security officer;

- A representative of the Division of Emergency Management;
- A representative of the Office of the Chief Inspector General;
- An individual appointed by the President of the Senate;
- An individual appointed by the Speaker of the House of Representatives;
- Members of the private sector appointed by the Governor.

The task force shall convene by October 1, 2019, and shall meet as necessary, but at least quarterly. The Division of State Technology within DMS will provide staffing and administrative support to the task force. The task force is to submit a final report of its findings and recommendations on or before November 1, 2020.

Section 30 provides that the bill shall take effect July 1, 2019.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Not applicable. The bill does not require counties and municipalities to spend funds, reduce counties' or municipalities' ability to raise revenue, or reduce the percentage of a state tax shares with counties and municipalities.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None identified.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Vendors offering a cloud solution may be more likely to be awarded IT procurements under the "cloud-first" policy established in this bill.

C. Government Sector Impact:

The "cloud-first" policy may result in increased costs to the state agencies. It appears that state agencies must show some preference to a private vendor providing a cloud-computing solution over a similar cloud-computing solution provided by the state data center, without regard to the costs of the procured solution. On the other hand, the state data center is most likely to be reduced in size over time, even if the state data center offers a cloud solution.

VI. Technical Deficiencies:

Section 6 amends s. 112.061, F.S., to codify the Statewide Travel Management System. Line 197-198 states the purpose of the system is to "collect and store information relating to public officer and employee travel information." Public officers and employees, for purposes of chapter 112, F.S., include local government officer and employees as well as state officers and employees. Lines 203-204 require state executive branch agencies and the judicial branch to report travel information on the system. Lines 209-213 require state executive branch agencies and the judicial branch to use the system for travel authorization and reimbursement. If the use of the Statewide Travel Management System is intended to be limited to state public officers and employees, the Legislature may want to consider modifying lines 197-198 to read "collect and store information relating to state executive branch and judicial branch travel information."

Section 16 amends s. 110.205(e), F.S., to exempt the chief information officer from the state career service. Because the chief information officer is the director of the Division of State Technology, that position is exempted pursuant to s. 110.205(j), F.S. Section 16 could simply be repealed so that no confusion occurs.

Section 29 creates the Florida Cybersecurity Task Force within the DMS. Lines 1460 - 1461 of the bill state that the task force will operate in a manner consistent with s. 20.052, F.S. Section 20.052, F.S, requires the private citizen members of an advisory body that is adjunct to an executive branch agency to be appointed by the Governor, the head of the department, the executive director of the department, or a Cabinet officer. If the task force must operate consistent with this requirement, the appointments by the President of the Senate and the Speaker of the House of Representatives may not be private citizens (most likely must be members of the Legislature).

The Florida Cybersecurity Task Force is composed of a representative of the FDLE computer crime center, a representative of the FDLE fusion center, the state chief information officer and the state chief information security officer, and others. These four state employees may have an on-going working relationship required to effectively accomplish their various job duties. However, as a member of the same advisory body, subject to public meetings requirements, these four state employees may not be able to communicate for their normal job duties if their discussions include topics addressed by the advisory committee.

VII. Related Issues:

Section 11 establishes a "cloud-first" policy for state agencies. The state agencies are directed to "show a preference for cloud-computing solutions that either minimize or do not require the use

of state data center infrastructure when cloud-computing solutions meet the needs of the agency, reduce costs, and meet or exceed the applicable state and federal laws, regulations, and standards for IT security." From the client agency's point of view, the state data center may be providing "cloud-computing." Stated another way, this cloud-first policy appears to direct state agencies to show a preference for private vendors providing cloud-computing over the state data center providing cloud-computing with new infrastructure. This may result in the client agency paying higher costs for IT solutions to the extent that the state data center solution is less expensive than the private vendor solution.

Section 29 creates the Florida Cybersecurity Task Force to review various IT security issues. Pursuant to s 20.052(5)(c), F.S., a meeting of an advisory body is a public meeting under s. 286.011, F.S., unless otherwise authorized. The public nature of the meetings may hinder open communication among the task force members. Section 286.0113, F.S., provides that a portion of a meeting that would reveal a security or firesafety system plan or portion thereof made confidential by s. 119.071(3)(a), F.S., is exempt from the public meetings requirements of s. 286.011 and s. 24(b), Art. I of the State Constitution. However, most of the IT security information is made confidential and exempt under the provisions of s. 282.318, F.S. Thus, the exemption from public meetings requirements does not appear to apply.

Likewise, there is a concern regarding the use of confidential and exempt information by the task force, particularly if persons not employed by the state are appointed to the task force. Information relating to IT security is typically confidential and exempt. Such information may be available to the Auditor General, the Cybercrime Office, the Chief Inspector General, and now, under the bill, the Division of State Technology of the DMS. It is unclear whether state agencies will be permitted to share confidential and exempt with the task force. Note that the task force is adjunct to the DMS and is not related to the Division of State Technology. The FDLE has recommended incorporating language into the task force providing that any confidential or exempt information the task force obtains remains confidential or exempt in the hands of the task force.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 20.22, 20.255, 112.061, 282.003, 282.0041, 282.0051, 282.201, 282.318, 17.0315, 20.055, 97.0525, 110.205, 215.322, 215.96, 287.057, 282.00515, 287.0591, 365.171, 365.172, 365.173, 445.011, 445.045, 668.50, and 943.0415.

This bill creates the following sections of the Florida Statutes: 282.206

This bill repeals the following sections of the Florida Statutes: 20.61

IX. Additional Information:

A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.