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 448
INTRODUCER:	Senator Brandes
SUBJECT:	Agency for State Technology
DATE:	January 22, 2018
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Peacock	Caldwell	GO	**Pre-meeting**
2.			AGG	
3.			AP	

I. Summary:

SB 448 revises definitions of specified terms contained in the Enterprise Information Technology Services Management Act and revises certain powers, duties, and functions of the Agency for State Technology to provide for collaboration with the Department of Management Services.

The bill authorizes the Agency for State Technology's State Data Center to extend a service-level agreement with an existing customer for up to six months. The State Data Center must file a report with the Executive Office of the Governor within specified timeframes of the signing of an extension or the scheduled expiration of the service-level agreement with the customer. The report must outline issues preventing execution of new agreement and a schedule for resolving such issues.

The bill authorizes the Agency for State Technology to plan, design, and conduct testing with information technology resources to implement services that are within the scope of the services provided by the state data center, if cost-effective.

The bill has no known fiscal impact on state funds.

The bill takes effect July 1, 2018.

II. Present Situation:

Enterprise Information Technology Services Management Act

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

[1] Section 282.003, F.S.

The State Technology Office (STO) was established in the Department of Management Services (DMS) in 1997.[2] During the 2000 and 2001 legislative sessions,[3] the Legislature significantly amended statutes allowing for the consolidation and centralization of information technology (IT) assets and resources for executive branch agencies. While other sections of statute were amended to accomplish this policy direction, the primary chapter amended was Part I of Chapter 282, F.S., to either take existing powers and duties assigned to the DMS and transfer these powers and duties to the STO, or prescribe additional powers and duties to the STO to accomplish the policy direction of consolidating and centralizing IT. One of STO's new duties included developing and implementing service level agreements[4] with each agency that the STO provided IT services.

In 2007, the Legislature created the Agency for Enterprise Information Technology (AEIT) to oversee policies for the design, planning, project management, and implementation of enterprise IT services, to include IT security.[5] The State Data Center was created by the Legislature in 2008.[6]

In 2014, the Legislature abolished the AEIT and transferred its duties to the then newly created Agency for State Technology.[7]

Section 282.0041(2), F.S., defines the term "breach" as "a confirmed event that compromises the confidentiality, integrity, or availability of information or data."

Section 282.0041(10), F.S., defines the term "incident" as "a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology security policies, acceptable use policies, or standard security practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur."

The Florida Information Protection Act of 2014

The Florida Information Protection Act of 2014[8] requires businesses and governmental entities to provide notice to affected customers and the Department of Legal Affairs (DLA) when a breach of security of personal information occurs.[9] This act provides enforcement authority to the DLA under the Florida Deceptive and Unfair Trade Practices Act[10] to prosecute violations and to impose civil penalties for failure to report data breaches within specified timeframes.[11] Civil

[2] Chapter 97-286, L.O.F.
[3] Chapter 2000-164, L.O.F.; Chapter 2001-261, L.O.F.
[4] Section 282.0041(20), F.S., defines the term "service level agreement" to mean a written contract between the state data center and a customer entity which specifies the scope of services provided, service level, the duration of the agreement, the responsible parties, and service costs. A service-level agreement is not a rule pursuant to chapter 120.
[5] Chapter 2007-105, L.O.F.
[6] Chapter 2008-116, L.O.F.
[7] Chapter 2014-221, L.O.F.
[8] Chapter 2014-189, L.O.F.
[9] Section 501.171(3) and (4), F.S.
[10] Section 501.201, F.S.
[11] Section 501.171(9)(a), F.S.

penalties under the Florida Deceptive and Unfair Trade Practices Act include $1,000 per day for the first 30 days, $50,000 for each subsequent 30-day period up to 180 days, and $500,000 maximum penalty for violations continuing more than 180 days.[12] State governmental entities are not liable for civil penalties for failure to timely report security data breaches.[13] The Florida Information Protection Act requires the DLA to submit an annual report to the Legislature, by February 1 of each year, detailing any reported breaches of security by governmental entities or their third-party agents for the preceding year, along with any recommendations for security improvements.[14] The report must also identify any governmental entity that has violated the breach notification provisions.[15]

Section 501.171(1)(a), F.S., defines the term "breach of security" or "breach" as "unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use."

Section 501.171(1)(g)1., F.S., provides that "personal information" means either of the following:

- An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:
  - A social security number;
  - A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
  - A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
  - Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
  - An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
- A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Section 501.171(1)(g)2., F.S., provides that the term (personal information) "does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable."

[12] Section 501.171(9)(b), F.S.
[13] Section 501.171(1)(b), F.S.
[14] Section 501.171(7), F.S.
[15] *Id*.

Agency for State Technology

The AST was created on July 1, 2014.[16] The executive director of AST is appointed by the Governor and confirmed by the Senate. The duties and responsibilities of the AST include:[17]

- 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[18] IT project that has a total project cost of $25 million or more and impacts one or more other agencies.
- Consulting with state agencies 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.
- Reporting annually to the Governor, the President of the Senate and the Speaker of the House of Representatives regarding state IT standards or policies that conflict with federal regulations or requirements.
- 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. The IT policy must include:

[16] Chapter 2014-221, L.O.F.
[17] Section 282.0051, F.S.
[18] Section 20.03(1), F.S. The term "cabinet" means collectively the Attorney General, the Chief Financial Officer, and the Commissioner of Agriculture, as specified in s. 4, Art. IV of the State Constitution.

  - 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.
  - The term of each IT-related state term contract.
  - The maximum number of vendors authorized on each state term contract.
- In collaboration with the DMS, evaluating vendor responses for state term contract solicitations and invitations to negotiate, answering vendor questions on state term contract solicitations, and ensuring that IT policy is included in all solicitations and contracts that are administratively executed by the DMS.

State Data Center Service-Level Agreements

The State Data Center is established 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.[19] 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.

Below is a table listing the customers of the AST's State Data Center. The customers include state agencies, a water management district, a county, local agencies, and non-profit organizations.

AST Agency Customers	
Agency for Health Care Administration	Department of State
Agency for Persons with Disabilities	Department of Veterans' Affairs
Department of Citrus	Executive Office of the Governor
Department of Business & Professional Regulation	Division of Emergency Management
Department of Corrections	Fish & Wildlife Conservation Commission
Department of Children & Families	Florida Commission on Human Relations
Department of Economic Opportunity	Department of Highway Safety & Motor Vehicles
Department of Environmental Protection	Justice Administrative Commission
Department of Juvenile Justice	Public Employees Relations Commission
Department of Military Affairs	Public Service Commission
Department of Management Services	Northwest Florida Water Management District
Department of Education	Santa Rosa County
Department of Elder Affairs	Miami-Dade Expressway Authority
Department of Health	Greater Orlando Aviation Authority
Department of Lottery	Children Home Society
Department of Revenue	Department of Transportation

[19] Section 282.201, F.S.

From 2008 to 2014, s. 282.203, F.S., allowed an existing customer's service-level agreement with the AST to continue under the terms of the previous fiscal year's agreement, if a customer did not execute a new service-level agreement within 60 days of the agreement's expiration.

Funding Methodology

The Department of Financial Services (DFS) has responsibility for the preparation of the annual Statewide Cost Allocation Plan (SWCAP) required under the provisions of the U.S. Management and Budget (OMB) Circular A-87.[20] The circular establishes principles and standards for determining costs for federal awards carried out through grants, cost reimbursement contracts, and other agreements with state, local, and federally recognized Indian tribal governments. The SWCAP is the mechanism by which the state identifies, summarizes, and allocates statewide indirect costs. The SWCAP also includes financial and billing information for central services directly charged to agencies or programs. The DFS must ensure that the SWCAP represents the most favorable allocation of central services cost allowable to the state by the Federal government.[21]

Appendix C of OMB Circular A-87, defines "billed central services" as central services billed to benefited agencies and/or programs on an individual fee-for-service or similar basis. Typical expenditures of billed central services include computer services, transportation services, insurance, and fringe benefits.[22]

The services provided by the State Data Center to state agencies are an example of "billed central services." The State Data Center must adhere to the SWCAP in accounting for agency resources utilized.

Pilot Projects

From 2008 to 2014, s. 282.203, F.S., allowed the primary data centers to plan, design, and establish pilot projects and conduct experiments with IT resources.

Cybercrime Office within the Florida Department of Law Enforcement

In 2011, the Cybercrime Office (Office) was established within the Florida Department of Law Enforcement (FDLE)[23] when the Department of Legal Affairs' Cybercrime Office was transferred to the FDLE.[24] The Office is tasked with the following:

- Investigating violations of state law pertaining to the sexual exploitation of children, which are facilitated by or connected to the use of any device capable of storing electronic data;[25]

[20] Section 215.195(1), F.S. Also, see 2 CFR Part 225, Appendix C, Appendix D, and Appendix E.
[21] *Id*.
[22] 2 CFR Part 225, Appendix C.
[23] Section 943.0415, F.S.
[24] Chapter 2011-132, L.O.F.
[25] Section 943.0415(1), F.S.

- Monitoring state IT resources and providing analysis on IT security, incidents, threats, and breaches;[26]
- Investigating violations of state law pertaining to IT security incidents[27] and assisting in incident response and recovery;[28]
- Providing security awareness training and information to state agency employees concerning cybersecurity, online sexual exploitation of children, and security risks, and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the AST;[29] and
- Consulting with the AST in the adoption of rules relating to the IT security provisions in s. 282.318, F.S.[30]

The Office may collaborate with state agencies to provide IT security awareness training to state agency employees.[31] State agencies are required to report IT security incidents and breaches to the Office.[32]

III. Effect of Proposed Changes:

Section 1 amends s. 282.0041(2), F.S., to narrow the definition of the term "breach" to only include the unauthorized access to "personal information". This term will have the same meaning of the term "breach" defined in s. 501.171(1)(a), F.S.

The term "incident" contained in s. 282.0041(10), F.S., is amended. The amended definition of "incident" means "a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur."

Section 2 amends s. 282.0051(18)(b), F.S., to clarify that the AST will evaluate vendor responses only for state term contract solicitations and invitations to negotiate that are specifically related to IT. This amendment removes ambiguity of whether the AST had a duty to evaluate state-term contract solicitations and invitation to bids that were not IT-related.

Section 282.0051(18)(c), F.S., is amended to provide that the AST will answer vendor questions only on IT-related state term contract solicitations. This amendment removes the ambiguity of whether the AST had a duty to answer vendor questions on state-term contract solicitations that were not IT-related.

Section 282.0051(18)(d), F.S., is amended to provide that the AST shall ensure all IT-related solicitations by the DMS are procured and state contracts are managed in accordance with

[26] Section 943.0415(2), F.S.
[27] In accordance with s. 282.0041, F.S.
[28] Section 943.0415(3), F.S.
[29] Section 943.0415(4), F.S.
[30] Section 931.0415(5), F.S.
[31] Section 282.318(4)(i), F.S.
[32] Section 282.318(4)(j), F.S.

existing policy established under s. 282.0051(18)(a), F.S. This amendment clarifies the AST's duty does not apply to non-IT solicitations and state term contracts.

Section 3 amends s. 282.201(2)(d), F.S., to provide a State Data Center service-level agreement may be extended for up to six months. If the State Data Center and an existing customer execute a service-level agreement extension or fail to execute a new service-level agreement, the State Data Center must submit a report to the Executive Office of the Governor within five days after the date of the executed extension, or 15 days before the scheduled expiration date of the service-level agreement. Such report must explain the specific issues preventing execution of a new service-level agreement and describe the plan and schedule for resolving those issues.

In addition, this section:

- Deletes the requirement within a service-level agreement to provide certain termination notice to the AST;
- Authorizes the AST to plan, design, and conduct testing with IT resources to implement services that are within the scope of services provided by the State Data Center, if cost effective; and
- Deletes obsolete provisions related to the schedule for consolidations of agency data centers.

Section 4 reenacts s. 943.0415(2) and (3), F.S., related to the Cybercrime Office within the FDLE, to incorporate the amended definitions of "breach" and "incident" made in s. 282.0041, F.S.

Section 5 provides an effective date of July 1, 2018.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

The mandate restrictions do not apply because the bill does not require counties and municipalities to spend funds, reduce counties' or municipalities' ability to raise revenue, or reduce the percentage of state tax shared with counties and municipalities.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

According to the AST, SB 448 has no fiscal impact.[33]

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill amends sections 282.0041, 282.0051, and 282.201 of the Florida Statutes.

This bill reenacts section 943.0415 of the Florida Statutes.

IX. Additional Information:

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

None.

B. Amendments:

None.

[33] AST, *Senate Bill 448 Analysis* (Oct. 13, 2017) (copy on file with the Senate Governmental Oversight and Accountability Committee).