HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/CS/CS/HB 1033 Information Technology Security
SPONSOR(S): State Affairs Committee; Government Operations Appropriations Subcommittee; Government Operations Subcommittee; Artiles and others
TIED BILLS: HB 1035, CS/HB 1037 **IDEN./SIM. BILLS:** CS/SB 7050

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Government Operations Subcommittee	13 Y, 0 N, As CS	Toliver	Williamson
2) Government Operations Appropriations Subcommittee	9 Y, 0 N, As CS	Keith	Topp
3) State Affairs Committee	18 Y, 0 N, As CS	Toliver	Camechis

SUMMARY ANALYSIS

The Agency for State Technology (AST) is administratively housed within the Department of Management Services. The executive director of the AST, who serves as the state's chief information officer, is appointed by the Governor and confirmed by the Senate. Current law establishes positions within the AST and establishes the agency's duties and responsibilities.

The bill requires the AST to establish standards and processes consistent with best practices for both information technology (IT) security and cybersecurity. It also requires the AST to develop and publish guidelines and processes for an IT security framework that includes establishing agency computer security incident response teams and establishing an IT security incident reporting process that includes a procedure and tiered reporting timeframe for notification of the AST and the Department of Law Enforcement.

The bill requires the AST to annually provide training for state agency information security managers and computer security incident response team members. It also requires each state agency head to establish an agency computer security incident response team and to comply with all applicable guidelines and reporting processes established by the AST and conduct IT security and cybersecurity awareness training for new employees within their first 30 days of employment.

The bill requires one of the Governor's appointments to the Technology Advisory Council established within the AST to be a cybersecurity expert.

The bill requires certain entities that experience an IT security breach to include in their notice to affected individuals information indicating whether the breached entity offers free financial credit monitoring and, if the individual's personal health information was compromised, information on how to obtain free health care record monitoring.

This bill does not appear to have a fiscal impact on state or local governments.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Agency for State Technology

In 2014, the Legislature created the Agency for State Technology (AST) within the Department of Management Services (DMS).[1] The executive director of the AST, who serves as the state's chief information officer, is appointed by the Governor and confirmed by the Senate.[2] The following positions are established within the AST, all of whom are appointed by the executive director:

- Deputy executive director, who serves as the deputy chief information officer;[3]
- Chief planning officer and six strategic planning coordinators;[4]
- Chief operations officer;[5]
- Chief information security officer;[6] and
- Chief technology officer.[7]

AST's duties and responsibilities include:

- 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 for use by state agencies when implementing IT projects;
- Performing project oversight on all state agency IT projects with a total project cost of $10 million or more that are funded in the General Appropriations Act or any other law;
- Performing project oversight on any cabinet agency IT project with a total project cost of $25 million or more and that impacts one or more agencies;
- Providing operational management and oversight of the state data center;
- Recommending additional consolidations of agency data centers or computing facilities into the state data center;
- Identifying opportunities for standardization and consolidation of IT services that support business functions and operations that are common across state agencies;
- Establishing, in collaboration with the DMS, best practices for the procurement of IT products in order to reduce costs, increase productivity, or improve services;
- 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;
- Developing standards for IT reports and updates for use by state agencies;
- Assisting state agencies, upon request, in developing IT related legislative budget requests; and
- Conducting annual assessments of state agencies to determine their compliance with all IT standards and guidelines developed and published by the AST.[8]

Technology Advisory Council

The Legislature established the Technology Advisory Council (Council) within the AST.[9] The Council is comprised of seven members: four members appointed by the Governor, two of whom must be from

[1] The AST is administratively housed within the DMS as a separate budget program and is not subject to its control, supervision, or direction.
[2] Section 20.61(1)(a), F.S.
[3] Section 20.61(2)(a), F.S.
[4] Section 20.61(2)(b), F.S., requires one coordinator to be assigned to each of the following major program areas: health and human services, education, government operations, criminal and civil justice, agriculture and natural resources, and transportation and economic development.
[5] Section 20.61(2)(c), F.S.
[6] Section 20.61(2)(d), F.S.
[7] Section 20.61(2)(e), F.S.
[8] Section 282.0051, F.S.

the private sector; one member, appointed by each of the President of the Senate and the Speaker of the House of Representatives; and one member appointed jointly by the Cabinet members.[10] The Council considers and makes recommendations to the executive director of the AST on matters pertaining to enterprise IT policies, standards, services and architecture.[11] The executive director must consult with the Council with regard to executing the AST's duties and responsibilities that relate to statewide IT strategic planning and policy.[12]

It is unclear whether a meeting of the Council has convened since its creation.

Information Technology Security Act

The Information Technology Security Act[13] provides that the AST is responsible for establishing standards and processes consistent with generally accepted best practices for IT security and adopting rules that safeguard an agency's data, information, and IT resources to ensure availability, confidentiality, and integrity.[14] In addition, the AST must:

- Develop, and annually update, a statewide IT security strategic plan;
- Develop and publish an IT security framework for state agencies;[15]
- Collaborate with the Cybercrime Office of the Florida Department of Law Enforcement in providing training for state agency information security managers; and
- Annually review the strategic and operational IT security plans of executive branch agencies.[16]

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.[17] In part, the heads of state agencies are also required to annually submit to the AST the state agency's strategic and operational IT security plans; conduct, and update every three years, a comprehensive risk assessment[18] 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[19] of the agency's IT security program for the data, information, and IT resources of the state agency are conducted.[20]

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)[21] when the Department of Legal Affairs' Cybercrime Office was transferred to FDLE.[22] The Office is tasked with:

- 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;[23]
- Monitoring state IT resources and providing analysis on IT security, threats, and breaches;[24]

---

[9] Section 20.61(3), F.S.
[10] *Id*.
[11] Section 20.61(3)(a), F.S.
[12] Section 20.61(3)(b), F.S.
[13] Section 282.318, F.S.
[14] Section 282.318(3), F.S.
[15] The term "state agency" is defined to mean any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. Section 282.0041(23), F.S.
[16] Section 282.318(3), F.S.
[17] Section 282.318(4)(a), F.S.
[18] The risk assessment is confidential and exempt from s. 119.07(1), F.S., except that such information shall be available to the Auditor General, the Agency for State Technology, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General. Section 282.318(4)(c), F.S.
[19] The results of such audits and evaluations are confidential and exempt from s. 119.07(1), F.S., except that such information must be made available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Agency for State Technology, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. Section 282.318(4)(f), F.S.
[20] Section 282.318(4), F.S.
[21] Section 943.0415, F.S.
[22] FDLE document entitled Florida Department of Law Enforcement Cybercrime Office (on file with the Government Operations Subcommittee).
[23] Section 943.0415(1), F.S.

- Investigating violations of state law pertaining to IT security incidents[25] and assisting in incident response and recovery;[26]
- 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;[27] and
- Consulting with the AST in the adoption of rules relating to the IT security provisions in s. 282.318, F.S.[28]

The Office may collaborate with state agencies to provide IT security awareness training to state agency employees.[29] State agencies are required to report IT security incidents and breaches to the Office.[30]

Notice of Data Security Breach

In 2014, the Legislature passed the Florida Information Protection Act of 2014.[31] The act requires a covered entity to provide notice to the Department of Legal Affairs of any breach in security[32] affecting 500 or more individuals in the state.[33] The act also requires covered entities to give notice to each individual in the state whose personal information was accessed, or the entity reasonably believes to have been accessed, as a result of a breach of security.[34] The covered entity must provide written notice within 30 days after the determination of a breach or reason to believe a breach has occurred,[35] which must be sent by mail or e-mail. The notice must include:

- The date, estimated date, or estimated date range of the breach of security;
- A description of the personal information that was accessed or reasonably believed to have been accessed as part of the breach of security; and
- Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.[36]

The term "covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements, the term includes a governmental entity.[37]

Effect of the Bill

The bill requires the AST to establish standards and processes consistent with best practices for both IT security and cybersecurity. The bill also requires the AST to develop and publish guidelines and processes for an IT security framework for use by state agencies for:

- Establishing an agency computer security incident response team to respond to IT security incidents;

---

[24] Section 943.0415(2), F.S.
[25] The term "incident" is defined to mean a violation or imminent threat of violation, whether such violation is accidental or deliberate, of IT 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. Section 282.0041(10), F.S.
[26] Section 943.0415(3), F.S.
[27] Section 943.0415(4), F.S.
[28] Section 931.0415(5), F.S.
[29] Section 282.318(4)(h), F.S.
[30] Section 282.318(4)(d), F.S.
[31] Chapter 2014-189, L.O.F.
[32] The term "breach of security" or "breach" is defined to mean 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)(a), F.S.
[33] Section 501.171(3), F.S.
[34] Section 501.171(4), F.S.
[35] Section 501.171(4)(a), F.S.
[36] Section 501.171(4)(e), F.S.
[37] Section 501.171(1)(b), F.S.

- Establishing an IT security incident reporting process that must include a procedure for notification of the AST and the Office. The bill requires the notification procedure to provide for tiered reporting timeframes with the timeframes based upon the level of severity of the IT security incident; and
- Incorporating information obtained through detection and response activities into agency incident response plans.

Additionally, the bill requires each agency head to:

- Conduct IT security awareness training that specifically includes cybersecurity awareness training within 30 days of an employee commencing employment;
- Establish, in consultation with the AST and the Office, an agency computer security incident response team that must comply with the guidelines and processes for responding to an IT security incident established by the AST;
- Implement risk assessment remediation plans recommended by the AST; and
- Report an IT security incident or breach to the Office in addition to the AST.

The bill requires an agency's comprehensive risk assessment to include a determination of security threats to mobile devices and print environments. Additionally, the bill specifies that an agency's comprehensive risk assessment and IT security audit may be completed by a private sector vendor. The bill also requires that one of the Governor's appointments to the Technology Advisory Council be a cybersecurity expert.

The bill requires covered entities that have experienced a breach of security to include the following additional information in their notice to affected individuals:

- Information on how to obtain free health care record monitoring if personal health information[38] was accessed or reasonably believed to have been accessed; and
- Information indicating whether the covered entity is required or otherwise chooses to offer free financial credit monitoring to affected individuals.

B. SECTION DIRECTORY:

Section 1 amends s. 20.61, F.S., relating to the AST.

Section 2 amends s. 282.318, F.S., relating to security of data and information technology.

Section 3 amends s. 501.171, F.S., relating to security of confidential personal information.

Section 4 provides an effective date of July 1, 2016.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   There might be a negative fiscal impact on state government associated with researching information regarding how to obtain free health care record monitoring for the purpose of providing that information to affected individuals whose personal health information has been accessed in a

[38] The term "personal health information" is described as any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional as well as an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. *See* s. 501.171(1)(g)1.a. (IV) –(V), F.S.

security breach. However, the impact might be insignificant or absorbed in the already mandated notice requirements following a security breach.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

There might be a negative fiscal impact on local governments associated with researching information regarding how to obtain free health care record monitoring for the purpose of providing that information to affected individuals whose personal health information has been accessed in a security breach. However, the impact might be insignificant or absorbed in the already mandated notice requirements following a security breach.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

There might be a negative economic impact on private sector entities associated with researching information regarding how to obtain free health care record monitoring for the purpose of providing that information to affected individuals whose personal health information has been accessed in a security breach. However, the impact might be insignificant or absorbed in the already mandated notice requirements following a security breach.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. The bill does not affect county or municipal governments.

2. Other:

None.

A. RULE-MAKING AUTHORITY:

None.

B. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On January 26, 2016, the Government Operations Subcommittee adopted one amendment and reported the bill favorably as a committee substitute. The amendment clarified that state agencies must have a third party risk assessment completed by July 31, 2017, and, subject to legislative appropriation, may have additional assessments performed. The bill removed:

- Provisions reassigning certain the AST responsibilities to the chief information security officer;
- The authorization for AST to impose a 10 percent service charge upon each state agency for IT projects it oversees;
- The requirement that a public or private entity notify the agency of a security breach affecting 500 or more individuals in the state;

- Duplicative provisions related to cybersecurity training; and
- The requirement that the Technology Advisory Council coordinate with the Florida Center for Cybersecurity regarding certain cybersecurity activities, and the requirement that the council coordinate with the State Board of Education on STEM training.

On February 8, 2016, the Government Operations Appropriations Subcommittee adopted one amendment and reported the bill favorably as a committee substitute. The amendment clarified that one of the Governor's appointments to the Technology Advisory Council must be a cybersecurity expert. The bill removed:

- Requirements that state agencies have a third party complete a risk assessment by July 1, 2017;
- Specific tiered reporting timeframes for different IT security incidents;
- A requirement for the AST to establish an internship or work study program; and
- Appropriations to the AST within the bill.

On February 18, 2016, the State Affairs Committee adopted two amendments and reported the bill favorably as a committee substitute. The amendments required:

- An agency's comprehensive risk assessment to include a determination of the security threats to mobile devices and print environments.
- A covered entity's notice of a breach of security to affected individuals to include information on how to obtain free health care record monitoring, if the individual's personal health information was compromised, and information indicating whether a covered entity offers free financial credit monitoring.

This analysis is drafted to the committee substitute as approved by the State Affairs Committee.