HOUSE OF REPRESENTATIVES
FINAL BILL ANALYSIS

BILL #:	CS/CS/CS/HB 1033	**FINAL HOUSE FLOOR ACTION:**	
SPONSOR(S):	State Affairs Committee; Government Operations Appropriations Subcommittee; Government Operations Subcommittee; Artiles and others	111 **Y's**	0 **N's**
COMPANION BILLS:	HB 1035; CS/CS/HB 1037; CS/SB 7050	**GOVERNOR'S ACTION:**	Approved

SUMMARY ANALYSIS

CS/CS/CS/HB 1033 passed the House on March 7, 2016, and subsequently passed the Senate on March 7, 2016.

The Agency for State Technology (AST) is administratively housed within the Department of Management Services (DMS). 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 cybersecurity to be addressed in the standards and processes for information technology (IT) security established by the AST and provides that the AST is responsible for adopting rules that mitigate risks. Additionally, it 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 for notifying the AST and the Department of Law Enforcement (FDLE) of IT security incidents.

The bill requires the AST, in collaboration with the Cybercrime Office of FDLE, to provide training annually 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 to respond to an IT security incident and to 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 authorizes the AST, in collaboration with DMS, to:

- Establish an IT policy for all IT-related state contracts;
- Evaluate vendor responses for state term contract solicitations and invitations to negotiate;
- Answer vendor questions on state term contract solicitations; and
- Ensure that the established IT policy is included in all solicitations and contracts that are administratively executed by DMS.

This bill may have a fiscal impact on state agencies due to the new IT security training requirements provided in the bill. It does not appear to have a fiscal impact on local governments.

The bill was approved by the Governor on March 25, 2016, ch. 2016-138, L.O.F., and will become effective on July 1, 2016.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF 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]

In part, the 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;
- 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 the private sector; one member, appointed by each of the President of the Senate and the Speaker of

[1] The AST is administratively housed within 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] *See* s. 282.0051, F.S.
[9] Section 20.61(3), F.S.

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]

[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]

Agency Procurements

Agency[31] 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,[32] unless otherwise authorized by law:[33]

- 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.[34]
- 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.[35]
- 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.[36]

DMS is responsible for procuring state term contracts for commodities and contractual services from which state agencies must make purchases.[37]

Information Technology Procurement

Current law authorizes the AST, in collaboration with DMS, to establish best practices for the procurement of IT products in order to reduce costs, increase productivity, or improve services.[38] The

---

[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] Section 287.012(1), F.S., defines "agency" as any of the various state officers, departments, boards, commissions, divisions, bureaus, and councils and any other unit of organization, however designated, of the executive branch of state government. "Agency" does not include the university and college boards of trustees or the state universities and colleges.
[32] Section 287.012(6), F.S., defines "competitive solicitation" as the process of requesting and receiving two or more sealed bids, proposals, or replies submitted by responsive vendors in accordance with the terms of a competitive process, regardless of the method of procurement.
[33] *See* s. 287.057, F.S.
[34] Section 287.057(1)(a), F.S.
[35] Section 287.057(1)(b), F.S.
[36] Section 287.057(1)(c), F.S.
[37] Sections 287.042(2)(a) and 287.056(1), F.S.
[38] Section 282.0051(6), F.S.

best practices must include a provision requiring the AST to review all IT purchases made by state agencies that have a total cost of $250,000 or more, unless a purchase is specifically mandated by the Legislature, for compliance with the established standards.[39]

Additionally, the AST is authorized to participate with DMS in evaluating, conducting, and negotiating competitive solicitations for state term contracts for IT commodities, consultant services, or staff augmentation contractual services,[40] and the AST is authorized to collaborate with DMS in IT resource acquisition planning.[41] If DMS issues a competitive solicitation for IT commodities, consultant services, or staff augmentation contractual services, the AST must participate in such solicitations.[42]

Effect of the Bill

The bill authorizes the AST, in collaboration with DMS, to establish an IT policy for all IT-related state contracts, including state term contracts for IT commodities, consultant services, and staff augmentation services. 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.
- The term of each IT-related state term contract.[43]
- The maximum number of vendors authorized on each state term contract.

In addition, the AST, in collaboration with DMS, is authorized to evaluate vendor responses for state term contract solicitations and ITNs, to answer vendor questions on state term contract solicitations, and to ensure that the established IT policy is included in all solicitations and contracts that are administratively executed by DMS.

The bill requires cybersecurity to be addressed in the standards and processes for IT security established by the AST and provides that the AST is responsible for adopting rules that mitigate risks. Additionally, it requires the AST to develop and publish guidelines and processes for an IT security framework for use by state agencies that includes:

- Establishing agency computer security incident response teams and describing their responsibilities for responding to IT security incidents;
- Establishing an IT security incident reporting process that includes procedures and tiered reporting timeframes for notifying the AST and the Office of IT security incidents. The tiered reporting timeframes must be based upon the level of severity of the IT security incidents being reported; and
- Incorporating information obtained through detection and response activities into agency IT security incident response plans.

The bill also requires the AST, in collaboration with the Office, to provide training annually for state agency information security managers and computer security incident response team members.

[39] *Id*.
[40] Section 282.0051(7)(a), F.S.
[41] Section 282.0051(7)(b), F.S.
[42] Section 287.0591(4), F.S.
[43] Section 287.0591, F.S., currently provides that a state term contract for IT consultant services or IT staff augmentation contractual services must include a term that does not exceed 48 months. DMS may execute a state term contract for IT commodities, consultant services, or staff augmentation contractual services that exceeds the 48-month requirement if the Secretary of DMS and the executive director of the AST certify to the Executive Office of the Governor that a longer contract term is in the best interest of the state.

The bill requires each agency head to:

- Conduct IT security and 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 to respond to an IT security incident. Such team must convene upon notification of an IT security incident and must comply with the guidelines and processes 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 a private sector vendor may complete an agency's comprehensive risk assessment and IT security audit.

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

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   The bill may have a fiscal impact on the AST and the Office due to the requirement that they provide training annually for state agency information security managers and computer security incident response team members. In addition, it may have a fiscal impact on state agencies because of the requirement that they provide IT security and cybersecurity awareness training to all employees within 30 days of an employee commencing employment.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.