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 Appropriations

BILL:	PCS/SB 7050 (591178)
INTRODUCER:	Appropriations Committee (Recommended by Appropriations Subcommittee on General Government) and Governmental Oversight and Accountability Committee
SUBJECT:	Information Technology Security
DATE:	February 29, 2016 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
	Peacock	McVaney		**GO Submitted as Committee Bill**
1.	Wilson	DeLoach	AGG	**Recommend: Fav/CS**
2.	Wilson	Kynoch	AP	**Pre-meeting**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Technical Changes

I. Summary:

PCS/SB 7050 revises duties of the Agency for State Technology (AST) and requires the AST to develop guidelines and policies for state agencies regarding information technology and cybersecurity.

Subject to an annual appropriation, state agencies are required to:

- Conduct risk assessments administered by a third party,
- Establish computer security incident response teams and procedures to respond to suspected technology security incidents, and
- Provide cyber security training to employees.

The AST's Technology Advisory Council is required to collaborate with the State Board of Education in adopting a unified state plan on Science, Technology, Education and Mathematics (STEM) education and the Florida Center for Cybersecurity on various goals related to cybersecurity.

The bill appropriates $650,000 of nonrecurring funds and $50,000 of recurring funds from the General Revenue Fund to the AST to conduct training exercises in coordination with the Florida National Guard, and $12,000,000 from the General Revenue Fund to implement this act.

The bill is effective July 1, 2016.

II. Present Situation:

Agency for State Technology

The AST was created on July 1, 2014.[1] The executive director of the AST is appointed by the Governor and confirmed by the Senate. The duties and responsibilities include:[2]

- 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 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 a 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.
- 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.

[1] Chapter 2014-221, Laws of Florida.
[2] Section 282.0051, F.S.

Technology Advisory Council

The Technology Advisory Council,[3] consisting of seven members, is established within the AST: four members of the council are appointed by the Governor, two of which must be from the private sector. The President of the Senate and the Speaker of the House of Representatives each appoint one member of the council. The Attorney General, the Commissioner of Agriculture and Consumer Services, and the Chief Financial Officer jointly appoint one member by agreement of a majority of these officers.

The Technology Advisory Council considers and makes recommendations to the Executive Director on such matters as enterprise information technology policies, standards, services, and architecture.[4] The council may also identify and recommend opportunities for the establishment of public-private partnerships when considering technology infrastructure and services in order to accelerate project delivery and provide a source of new or increased project funding.[5]
The Executive Director consults with the council with regard to executing the duties and responsibilities of the agency related to statewide information technology strategic planning and policy.[6]

Cybercrime Office, Florida Department of Law Enforcement

The Cybercrime Office within the Florida Department of Law Enforcement (FDLE) was established in 2011 with the functions and personnel of the Department of Legal Affairs Cybercrime Office transferred to FDLE.[7] A cybercrime office has existed within FDLE since 1998.[8]

Some of the Cybercrime Office duties include:
- Monitoring state information technology resources and providing analysis on information technology security incidents, threats, and breaches;
- Investigating violations of state law pertaining to information technology security incidents and assisting in incident response and recovery;
- 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; and
- Consulting with the AST in the adoption of rules relating to the information technology security provisions.[9]

[3] Section 20.61(3), F.S.
[4] Section 20.61(3)(a), F.S.
[5] *Id*.
[6] Section 20.61(3)(b), F.S.
[7] Chapter 2011-132, Laws of Florida.
[8] Analysis for HB 5401 by the House Appropriations Committee (July 6, 2011)(copy on file with the Governmental Oversight and Accountability Committee). .
[9] Section 943.0415, F.S.

Unified State Plan for Science, Technology, Engineering, and Mathematics

Section 1001.03(17), F.S., requires the State Board of Education, in consultation with the Board of Governors and the Department of Economic Opportunity, to adopt a unified state plan to improve K-20 Science, Technology, Engineering, and Mathematics (STEM) education and prepare students for high-skill, high-wage, and high-demand employment in STEM and STEM-related fields.

Florida Center for Cybersecurity

The Florida Center for Cybersecurity was established in 2013 when the Legislature required the Board of Governors to submit a report to the Legislature and the Governor that provided a plan for the creation of a Florida Center for Cybersecurity to be located at the University of South Florida.[10]

The goals of the Florida Center for Cybersecurity are to:

- Position Florida as the national leader in cybersecurity and its related workforce through education, research, and community engagement;
- Assist in the creation of jobs in the state's cybersecurity industry and enhance the existing cybersecurity workforce;
- Act as a cooperative facilitator for state business and higher education communities to share cybersecurity knowledge, resources, and training;
- Seek out partnerships with major military installations to assist, when possible, in homeland cybersecurity defense initiatives; and
- Attract cybersecurity companies to the state with an emphasis on defense, finance, health care, transportation, and utility sectors.[11]

III. Effect of Proposed Changes:

Section 1 amends s. 20.61, F.S., to revise the membership of the Technology Advisory Council and requires that at least one of the four members appointed by the Governor be a cybersecurity expert. The bill also requires that the Technology Advisory Council, in coordination with the Florida Center for Cybersecurity, identify and recommend STEM training opportunities. These opportunities are for the establishment of cutting-edge educational and training programs for students consistent with the unified state STEM plan, in order to increase the cybersecurity workforce in the state, and to prepare cybersecurity professionals to possess a wide range of expertise.

Section 2 amends s. 282.318, F.S., to require the AST to establish standards and processes consistent with best practices for both information technology security and cybersecurity and to adopt rules that mitigate risks.

This section requires the AST to develop and publish guidelines and processes in its information technology security framework provided to state agencies for:

[10] Chapter 2013-41, Laws of Florida. *Also, see* s. 1004.444, F.S.
[11] Section 1004.444(2), F.S.

- Completing risk assessments administered by a third party and submitting completed assessments to the AST.
- Establishing a computer security incident response team to respond to suspected information technology security incidents and the timeframe for convening a team to determine an appropriate response.
- Establishing an information technology security incident reporting process, to include a procedure for notification of the AST and Cybercrime Office of the Florida Department of Law Enforcement (FDLE). The notification procedure must provide for a tiered reporting framework with incidents of critical impact reported upon discovery, incidents of high impact reported within four hours of discovery, and incidents of low impact reported within five business days of discovery.
- Incorporating lessons learned through detection and response activities into agency response plans to continuously improve organizational response activities.
- Providing all state agency employees with information technology security and cybersecurity awareness education and training within 30 days after commencing employment.

In collaboration with the Cybercrime Office of the FDLE, the AST's training requirements are revised to require at least annual training on cybersecurity threats, trends, and best practices for state agency information security managers and computer security incident response team members.

This section also requires the AST, in collaboration with relevant partners and the Florida Center for Cybersecurity, to develop and establish a cutting-edge internship or work-study program in STEM to produce a more cybersecurity skilled state workforce.

The bill further requires that each state agency's information security manager establish a computer security incident response team to respond to suspected computer security incidents. The computer security incident response team members must convene as soon as practicable upon notice of a suspected security incident and determine an appropriate response. The response would include taking action to prevent the expansion or recurrence of an incident, mitigating the effects of an incident, and eradicating an incident. The newly identified risks must be mitigated or documented as an accepted risk by computer security incident response team members.

The bill specifies mobile devices and print environments as information technology resources that will be included in the comprehensive risk assessment.

The bill requires state agencies to:

- Conduct a risk assessment, subject to an annual legislative appropriation, by July 31, 2017, that is administered by a third party consistent with guidelines and processes prescribed by the AST. Additional risk assessments must be completed periodically.
- Develop and update written internal policies and procedures for reporting information technology security incidents and breaches to the Cybercrime Office of the FDLE and the AST to include notification procedures and reporting timeframes for information technology security incidents and breaches.
- Provide information technology security and cybersecurity awareness training to all state agency employees in the first 30 days after commencing employment for attainment of an

appropriate level of cyber literacy. State agencies must ensure that privileged users, third-party stakeholders, senior executives, and physical and information security personnel understand their roles and responsibilities.

- Provide training, in collaboration with the Cybercrime Office of the FDLE, at least annually, on cybersecurity threats, trends, and best practices to computer security incident response team members.
- Develop notification procedures for reporting information technology security incidents.
- Improve organizational response activities by incorporating lessons learned from current and previous detection and response activities into response plans.

Section 3 amends s. 1001.03, F.S., to include the Technology Advisory Council as one of the entities that consults with the State Board of Education in the adoption of a unified state plan to improve K-20 STEM education and prepare students for employment in STEM and STEM-related fields.

Section 4 amends s. 1004.444, F.S., to require the Florida Center for Cybersecurity to coordinate with the Technology Advisory Council in pursuit of certain goals.

Section 5 appropriates for Fiscal Year 2016-2017, the sums of $650,000 in nonrecurring funds and $50,000 in recurring funds from the General Revenue Fund to the AST to conduct training exercises in coordination with the Florida National Guard.

Section 6 appropriates for Fiscal Year 2016-2017, the sum of $12,000,000 from the General Revenue Fund to the AST to implement this act.

Section 7 provides an effective date of July 1, 2016.

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 a state tax shares 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:

The impact of PCS/SB 7050 is indeterminate. Firms providing third party risk assessments to state agencies will see an increase in revenues.

C. Government Sector Impact:

The bill appropriates the following amounts for Fiscal Year 2016-2017:

- $650,000 non-recurring from the General Revenue Fund to the AST to conduct training exercises with the Florida National Guard;
- $50,000 recurring from the General Revenue Fund to the AST to conduct training exercises with the Florida National Guard; and
- $12 million from the General Revenue Fund to the AST to implement the provisions of this bill (presumably the risk assessments conducted are for the state agencies).

VI. Technical Deficiencies:

Section 6 does not specify whether the $12 million appropriation from the General Revenue Fund is from a recurring or nonrecurring appropriation.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends sections 20.61, 282.318, 1001.03, and 1004.444 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.)

Recommended CS by Appropriations Subcommittee on General Government on February 11, 2016:
The CS specifically includes mobile devices and print environments as information technology resources to be included in the comprehensive risk assessment.

B. Amendments:

None.