**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: | CS/SB 7050 |
| INTRODUCER: | Appropriations Committee (Recommended by Appropriations Subcommittee on General Government) and Governmental Oversight and Accountability Committee |
| SUBJECT: | Information Technology Security |
| DATE: | March 3, 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 | **Fav/CS** |

**Please see Section IX. for Additional Information:**

COMMITTEE SUBSTITUTE - Technical Changes

## I. Summary:


CS/SB 7050 revises the 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. Specifically the bill:

- Directs the AST to establish security standards and processes, including cybersecurity, to mitigate the risks;
- Provides the option for agencies to contract with a private sector vendor to complete risk assessments;
- Defines information technology resources to include mobile devices and print environments;
- Directs agencies to establish computer security incident response teams and processes to respond immediately to suspected technology security incidents, and the process must be tiered based on the severity of the suspected incident;
- Directs information learned from incident response activities to be incorporated into future plans;
- Directs agencies to provide incident and breach information to the AST and the Cybercrime Office within Florida Department of Law Enforcement; and
- Directs agencies to provide cyber security training to employees within 30 days of employment.

The bill revises the seven member AST Technology Advisory Council to require at least one member appointed by the Governor to be a cybersecurity expert.

The bill has no fiscal impact to state funds.

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.

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

- 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.

**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

[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). .

- Consulting with the AST in the adoption of rules relating to the information technology security provisions.[9]

## 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.

**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.

Specifically, this section requires the AST to:

- Develop and publish guidelines and processes relating to information technology security to be provided to state agencies for the completion of risk assessments that may be completed by a private sector vendor;
- Describe the responsibilities of the agency computer security incident response teams;
- Establish information technology security incident reporting processes including the procedure for notification to the AST and Cybercrime Office of the Florida Department of Law Enforcement (FDLE). The process must provide for a tiered reporting framework based on the level of severity of the incident;
- Incorporate information learned through detection and response activities into agency response plans; and
- Provide annual training to the state agencies' information security managers and incident response team members collaborating with the Cybercrime Office of the FDLE.

This section also requires state agency heads to:

- Establish a computer security incident response team, consulting with the AST and the Cybercrime Office of the FDLE, to respond to suspected information technology security incidents and the timeframe for convening a team to determine an appropriate response to comply with information technology guidelines established by AST;
- Provide the state agencies' comprehensive risk assessment may be completed by a private sector vendor;
- Specify mobile devices and print environments as information technology resources that will be included in the comprehensive risk assessment;
- Implement risk assessment remediation plans recommended by AST;
- Provide all state agency employees with information technology security and cybersecurity awareness education and training within 30 days after commencing employment;
- Direct all state agencies' information technology incidents and breaches be notified and reported to the AST and the Cybercrime Office of the FDLE; and
- Comply with information technology guidelines established by AST.

**Section 3** provides an effective date of July 1, 2016.

[9] Section 943.0415, F.S.

## IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

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:

The Agency for State Technology can handle the additional duties within existing resources.

## VI. Technical Deficiencies:

None.

## VII. Related Issues:

None.

## VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 20.61 and 282.318.

## IX. Additional Information:

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

**CS by Appropriations on March 1, 2016:**
The committee substitute:

- Removes the appropriation in the bill.

- Removes all provisions for Agency for State Technology (AST) to coordinate with the Florida Center for Cyber Security.
- Removes the requirement for state agencies' risk assessments be conducted by a private sector vendor subject to appropriations.
- Removes requirement for AST Technology Council to coordinate with Board of Governors on revision to STEM Unified plan.
- Removes provision for AST to establish a STEM internship program.
- Removes requirement for privileged users, senior executives, third party stakeholders and security personnel to be educated on their roles to attain an appropriate level of cyber security literacy.

B. Amendments:

None.