SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: Governmental Oversight and Productivity Committee

BILL:	CS/CS/SB 856
SPONSOR:	Governmental Oversight and Productivity Committee, Domestic Security Committee and Senator Diaz de la Portilla
SUBJECT:	Domestic Security
DATE:	April 19, 2006 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Pardue	Skelton	DS	**Fav/CS**
2.	McKay	Wilson	GO	**Fav/CS**
3.			GA	
4.			WM	
5.				
6.				

I. Summary:

This bill provides that some information technology security functions formerly provided by the State Technology Office (STO) will be provided by the Department of Management Services (DMS). The bill assigns and clarifies certain information technology security responsibilities for the DMS and each state agency.

The bill creates the Office of Information Security (OIS) within the DMS, and provides that the Chief Information Security Officer is the head of the office.

The bill includes language that enhancements and improvements to the state law enforcement radio system should be considered based on joint task force recommendations and contingent upon appropriations.

This bill substantially amends section 282.318 of the Florida Statutes.

II. Present Situation:

The issue of maintaining the security of data, information, and information technology resources within state government is cause for concern. The U. S. Government Accountability Office summed up the problem thusly in a recent report:

> The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Because of the concern about attacks from individuals and groups, protecting the computer

> systems that support critical operations and infrastructures has never been more important. These concerns are well founded for a number of reasons, such as escalating threats of computer security incidents, the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks. According to experts from government and industry, during the first quarter of 2005, more than 600 new Internet security vulnerabilities were discovered, thereby placing organizations that use the Internet at risk.[1]

The GAO report goes on to say:

> IBM recently reported that there were over 54 million attacks against government computers from January 2005 to June 2005.[2] Without proper safeguards, there is risk that individuals and groups with malicious intent may intrude into inadequately protected systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.[3]

Organizational Structure of the Department of Management Services

The DMS is exempt from the requirements of s. 20.04(3), F.S., which provides standard terminology for the organizational structure of executive branch agencies. Pursuant to s. 20.22, F.S., the DMS contains the following divisions and programs:

- Facilities Program.
- State Technology Office.
- Workforce Program.
- Support Program.
- Federal Property Assistance Program.
- Administration Program.
- Division of Administrative Hearings.
- Division of Retirement.
- Division of State Group Insurance.

The statute provides that the STO operates and manages the Technology Resource Center.

As discussed herein below, the STO no longer in fact exists; its operational responsibilities have been assumed by what the DMS calls Enterprise Information Technology Services, which does not exist in statute.

[1] Government Accountability Office, GAO-06-31, October 2005, page 4.
[2] IBM, *Security Threats and Attack Trends Report:* January 2005 to June 2005.
[3] Government Accountability Office, GAO-06-31, October 2005, page 4.

The State Technology Office

During the 2000 and 2001 legislative sessions, the Legislature significantly amended statutes allowing for the consolidation and centralization of information technology assets and resources for executive branch agencies.[4] While other sections of statute were amended to accomplish this policy direction, the primary chapter amended was Chapter 282, Part I, to either: (1) take existing powers and duties assigned to the Department of Management Services and transfer these powers and duties to the State Technology Office; or, (2) prescribe additional powers and duties to the State Technology Office to accomplish the policy direction of consolidating and centralizing information technology within the State Technology Office (STO). These new or additional powers and duties included the following:

- Created the STO within the Department of Management Services (DMS) as a separate budget entity and required the STO to be headed by a Chief Information Officer (CIO) who is appointed by the Governor, is in the Senior Management Service, and who must be an agency head for all purposes;
- Required the STO to develop and implement service level agreements with each agency that the STO provides information technology services;
- Authorized the transfer of positions, associated rate and the amount of approved budget to the STO for those state agencies that entered into a memorandum of agreement;
- Established State Strategic Information Technology Alliance and required STO to promulgate rule implementing the policies and procedures for establishing strategic alliances;
- Required the STO to adopt rules for implementing policies and procedures providing best practices to be followed by agencies in acquiring, using, upgrading, modifying, replacing, or disposing of information technology;
- Allowed the CIO to appoint or contract for the agency chief information officer; and
- Allowed the STO to deploy an enterprise portal for governmental information & services.

Specifically, s. 282.318, F.S., the "Security of Data and Information Technology Resources Act," was amended to provide that the STO, in consultation with each agency head, was responsible for assuring an adequate level of security for all data and information technology resources.

In 2005, the Legislature passed Committee Substitute for Committee Substitute for Senate Bill 1494, which transferred operational responsibilities for wireless communications, SUNCOM, and data center management to the DMS, and placed the strategic planning and policy responsibilities of the STO with a successor entity, the Florida Technology Council. The bill was vetoed by the Governor, and the STO effectively ceased to exist. The DMS has subsequently provided for the operational responsibilities of the STO through an entity called Enterprise Information Technology Services (EITS).

State Of Florida Chief Information Officers Council

The Legislature created the Chief Information Officers Council (CIO Council) in s. 282.315, F.S., to enhance communication, consensus building, coordination, and facilitation of

[4] Chapters 2000-164, and 2001-261, L.O.F.

statewide enterprise resource planning and management issues, and provided it with the following duties:

- Enhance communication among the Agency Chief Information Officers by sharing enterprise resource planning and management experiences and exchanging ideas.
- Facilitate the sharing of best practices that are characteristic of highly successful technology organizations, as well as exemplary information technology applications of state agencies.
- Identify efficiency opportunities among state agencies.
- Serve as an educational forum for enterprise resource planning and management issues.
- Assist the STO in identifying critical statewide issues and make recommendations for solving enterprise resource planning and management deficiencies.

Members of the council include agency Chief Information Officers, including the Chief Information Officers of the agencies and university boards of trustees, community college boards of trustees, the Supreme Court, and each state attorney and public defender, except that there is one Chief Information Officer selected by the state attorneys and one Chief Information Officer selected by the public defenders. The chairs, or their designees, of the Florida Financial Management Information System Coordinating Council, the Criminal and Juvenile Justice Information Systems Council, and the Health Information Systems Council represent their respective organizations on the Chief Information Officers Council as voting members.

The State Technology Office is to provide administrative support to the CIO Council.

Florida's Program for Information Technology Security

Section 282.318, F.S., is known as the "Security of Data and Information Technology Resources Act." This section provides a framework for the security of all data and information technology resources of each agency of the state. This section assigns responsibility to the State Technology Office for managing the information technology security programs of each state agency. Florida information resource security policies and standards are currently published by rule in Chapter 60DD-2, Florida Administrative Code. The rule defines minimum security standards for the protection of state information resources and is adopted under the authority of s. 282.102(2), F.S.

According to the Florida Department of Law Enforcement (FDLE), Florida's cyber security initiative includes the Florida Infrastructure Protection Center, Computer Incident Response Teams (CIRT) and Computer Security Incident Response Teams (CSIRT). The Florida Infrastructure Protection Center was appropriated $900,000 in FY 2002-2003; however, no statutory authority or duties have been provided or prescribed.

According to FDLE, the CSIRTs are "operationally" under the jurisdiction of FDLE's Computer Crime Center and the CSIRTs are "operationally" under the Office of Information Security, which currently does not exist in statute. Consideration should be given to reviewing and analyzing the appropriateness of including these entities into any information security legislation.

In addition to the budget issue for the OIS, the DMS also has a budget issue for funding a Network Operations Assurance Center (NOAC). An outstanding issue involving both of these budget issues is the operational relationship between the two proposed entities. Absent clearly defined proposed authority, duties, and roles of both entities (OIS & NOAC), moving forward with statutorily creating one, in isolation of the other, may warrant caution.

III. Effect of Proposed Changes:

Section 1. This bill amends s. 282.318, F.S., to reassign the former State Technology Office's data and information technology security function to the Department of Management Services. The bill assigns and clarifies certain responsibilities for the department and each state agency.

The bill assigns responsibility to the department for coordinating, assessing, and recommending minimum standard operating procedures for an adequate level of data and information technology security.

The bill clarifies the responsibility for information technology security by requiring that each agency:

- Designate an information security manager;
- Conduct and update a comprehensive risk analysis every three years;
- Develop and update policies and procedures that are consistent with the standard operating procedures recommended by the DMS to assure the security of data, information, and information technology resources;
- Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from the identified risks to data and information technology resources;
- Conduct periodic internal audits and evaluations of each data and information technology resources security program; and
- Include appropriate security requirements in written specifications for solicitation of information technology that are consistent with the standard operating procedures recommended by the DMS.

The bill likewise requires the department to include security requirements in the specifications it develops in solicitations for state contracts for information technology resources.

The bill requires the DMS to establish the Office of Information Security and designate a Chief Information Security Officer. The office will coordinate with the Agency Chief Information Officers Council and will develop a strategic plan for information technology security, to be submitted to the Legislature and the Governor by December 1, 2006.

The bill assigns responsibility to the Office of Information Security for:

- Developing standards for conducting risk analysis and security audits by state agencies;
- Assisting agencies with IT security issues;
- Establishing minimum standards for the recovery of information technology following a disaster; and
- Training of information security managers;

The subsection establishing the office expires on June 30, 2007.

Section 2. The bill finds that enhancements and improvements to the state law enforcement radio system should be considered for additional funding. The bill additionally finds that the recommendations of the Joint Task Force on State Agency Law Enforcement Communications should be implemented contingent upon the appropriation of funds.

Section 3. The bill provides for an effective date upon becoming a law.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

Costs for funding the Office of Information Security within the Department of Management Services are indeterminate.

The bill also finds that enhancements and improvements to the state law enforcement radio system should be considered. Such enhancements and improvements should be made based on the recommendations of the Joint Task Force on State Agency Law Enforcement Communications and be contingent upon appropriations.

VI. Technical Deficiencies:

None.

VII. Related Issues:

The language in Section 2 of the bill contains findings and intent language for possible legislation relating to the statewide law enforcement radio system. It is unclear what effect the language included in a bill relating to an Office of Information Security will have on a future Legislature.

VIII. Summary of Amendments:

None.