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: Domestic Security Committee

BILL: PCS SB 856

SPONSOR: Senator Diaz de la Portilla

SUBJECT: Domestic Security

DATE: March 16, 2006 REVISED: _____ _____ _____ _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Pardue	Skelton	DS	**Pre-meeting**
2.			CJ	
3.			JA	
4.			WM	
5.			RC	
6.				

I. Summary:

This committee substitute provides for the reinstatement of the former State Technology Office's information technology security function within the Department of Management Services. The committee substitute assigns and clarifies certain information technology security responsibilities for the department and each state agency.

The Office of Information Security is created within the department and provides for the designation of a Chief Information Security Officer.

This committee substitute substantially amends section 282.318 of the Florida Statutes.

II. Present Situation:

The problem 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 very succinctly 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]

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 purpose of this chapter is to promulgate state policies regarding the security of data and information technology resources. 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.

The Legislature also created the Agency Chief Information Officers Council after finding that enhancing communication, consensus building, coordination, and facilitation of statewide enterprise resources is essential.[4] Membership of the council includes the Agency Chief Information Officers, including the Chief Information Officers of the agencies and governmental entities enumerated in s. 282.3031, F.S.[5]

III. Effect of Proposed Changes:

This committee substitute amends s. 282.318, F.S., to reflect the reinstatement of the former State Technology Office's information technology security function within the Department of Management Services. The committee substitute assigns and clarifies certain responsibilities for the department and each state agency.

---

[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.
[4] S. 282.315, F.S.
[5] Note: Certain organizations such as the state attorneys and the public defenders are limited to one representative from each respective group.

The committee substitute assigns responsibility to the department for coordinating, assessing, and setting minimum standard operating procedures for an adequate level of data and information technology security. The bill also provides that the department will assist each agency with the development of and revisions to written internal policies and procedures to assure the security of data, information, and information technology resources.

The committee substitute 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
- 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
- Include appropriate security requirements as determined by the department, in consultation with the Department of Law Enforcement, in written specifications for solicitation of information technology resources

The committee substitute likewise requires the department to include security requirements in the specifications it develops in solicitation for state information technology contracts.

The committee substitute requires the department to establish the Office of Information Security and designate a Chief Information Security Officer. The office will work with all branches of state government and coordinate with the Agency Chief Information Officers Council and the Executive Office of the Governor.

The committee substitute assigns responsibility to the Office of Information Security for:

- Security rule making and formulation of policy recommendations
- Security audit oversight
- Training of information security managers
- Coordination of domestic security funding for cybersecurity issues
- Setting minimum standards for the recovery of information technology following a disaster

The committee substitute conceptually provides that funding for the office will be provided with general revenue through the department.

The committee substitute provides the department the administrative authority to adopt rules relating to the security of data, information, and information technology pursuant to ss. 120.536 (1) and 120.54, F.S.

This committee substitute 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:

This bill creates the Office of Information Security within the Department of Management Services. Funding for the office is contingent upon appropriations.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Summary of Amendments:

None.