By the Committees on Governmental Oversight and Productivity; Domestic Security; and Senator Diaz de la Portilla

585-2347-06

A bill to be entitled

An act relating to domestic security; amending s. 282.318, F.S.; requiring the Department of Management Services to recommend minimum operating procedures for the security of data and information technology resources; requiring each agency to conduct certain procedures to assure the security of data, information, and information technology resources; requiring that the results of certain internal audits and evaluations be available to the Auditor General; requiring the department to establish an Office of Information Security and to designate a Chief Information Security Officer; requiring the office to develop a strategic plan; providing that the office is responsible for certain procedures and standards; providing legislative findings with respect to the provision of additional funds for enhancements and improvements to the radio system used by state law enforcement agencies; providing for the implementation of certain recommendations contingent upon appropriation; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 282.318, Florida Statutes, is amended to read:

282.318 Security of data and information technology resources.--

(1) This section may be cited as the "Security of Data and Information Technology Resources Act."

(2)~~(a)~~ The Department of Management Services, hereafter referred to as the department ~~The State Technology Office~~, in consultation with each agency head, is responsible for coordinating, assessing, and recommending minimum operating procedures for ~~and accountable for~~ assuring an adequate level of security for ~~all~~ data and information technology resources. To assist the department in carrying ~~of each agency and, to carry~~ out this responsibility, each agency shall, at a minimum:

(a)~~1.~~ Designate an information security manager who shall administer the security program of each agency for its data and information technology resources.

(b)~~2.~~ Conduct, and ~~periodically~~ update every 3 years, a comprehensive risk analysis to determine the security threats to the data, information, and information technology resources of each agency. The risk analysis information is confidential and exempt from the provisions of s. 119.07(1), except that such information shall be available to the Auditor General in performing his or her postauditing duties.

(c)~~3.~~ Develop, and periodically update, written internal policies and procedures that are consistent with the standard operating procedures recommended by the department to assure the security of the data and information technology resources of each agency. The internal policies and procedures which, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from the provisions of s. 119.07(1),

except that such information shall be available to the Auditor General in performing his or her postauditing duties.

(d)~~4.~~ Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from the identified risks to the data and information technology resources of each agency.

(e)~~5.~~ Ensure that periodic internal audits and evaluations of each security program for the data, information, and information technology resources of the agency are conducted. The results of such internal audits and evaluations are confidential information and exempt from the provisions of s. 119.07(1), except that such information shall be available to the Auditor General in performing his or her postauditing duties.

(f)~~6.~~ Include appropriate security requirements~~, as determined by the State Technology Office, in consultation with each agency head,~~ in the written specifications for the solicitation of information technology resources which are consistent with the standard security operating procedures as recommended by the department.

~~(b)~~ In those instances in which the department ~~State Technology Office~~ develops state contracts for use by state agencies, the department ~~office~~ shall include appropriate security requirements in the specifications for the solicitation for state contracts for procuring information technology resources.

(3) In order to ensure the security of data, information, and information technology resources, the department shall establish the Office of Information Security and shall designate a Chief Information Security Officer as the head of the office. The office shall coordinate its activities with the Agency Chief Information Officers Council

as established in s. 282.315. The office is responsible for developing a strategic plan for information technology security which shall be submitted by December 1, 2006, to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives; developing standards and templates for conducting comprehensive risk analyses and information security audits by state agencies; assisting agencies in their compliance with the provisions of this section; establishing minimum standards for the recovery of information technology following a disaster; and conducting training for agency information security managers. This subsection shall expire on June 30, 2007.

Section 2. The Legislature finds that infrastructure enhancements and improvements to the radio system used by state law enforcement agencies will provide increased protection to the residents of this state and should be considered for additional funding. In order to ensure continued, improved communication and protection by state and local law enforcement personnel, the recommendations of the Joint Task Force on State Agency Law Enforcement Communications, dated February 2005, or any subsequent recommendations of the joint task force, should be implemented contingent upon the appropriation of funds.

Section 3. This act shall take effect upon becoming a law.

STATEMENT OF SUBSTANTIAL CHANGES CONTAINED IN COMMITTEE SUBSTITUTE FOR CS for SB 856

Provides that the DMS will recommend minimum standard operating procedures for an adequate level of data and information technology security.

Requires agencies to develop IT security procedures consistent with the operating procedures recommended by the DMS.

Requires the Office of Information Security to develop and submit to the Legislature and the Governor by December 1, 2006, a strategic plan for information security.

Assigns to the OIS various responsibilities relating to IT security.

Provides that the section establishing the OIS expires on June 30, 2007.