By the Committee on Domestic Security; and Senator Diaz de la Portilla

583-1960-06

A bill to be entitled

An act relating to domestic security; amending s. 282.318, F.S.; requiring the Department of Management Services to set minimum standard operating procedures for the security of data and information technology resources; providing for the department to require 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 Office of Information Security; requiring the department to establish an Office of Information Security and to designate a Chief Information Security Officer; providing that the office is responsible for certain procedures and standards; providing for the office to be funded by general revenue; authorizing the department to adopt rules; 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 setting minimum standard operating procedures for ~~and accountable for assuring~~ an adequate level of security for all data and information technology resources of each agency and, to carry out this responsibility, will ~~shall~~, at a minimum:

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

(b)~~2.~~ Require that each agency conduct and update every 3 years ~~Conduct, and periodically update,~~ 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.~~ Assist each agency with the development and provide revisions of ~~Develop, and periodically update,~~ written internal policies and procedures to assure the security of the data, information, 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.~~ Require each agency to 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.~~ Require each agency to ensure that periodic internal audits and evaluations of each security program for the data 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 and to the Office of Information Security for performance of its coordination and assessment duties.

(f)~~6.~~ Require that each agency include appropriate security requirements, as determined by the Department of Management Services ~~the State Technology Office~~, in consultation with the Department of Law Enforcement ~~each agency head~~, in the written specifications for the solicitation of information technology resources.

~~(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 enterprise information, 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 work with all branches of state government and coordinate with the Agency Chief Information Officers Council and the Executive Office of the Governor. The office is responsible for security rulemaking and formulation of policy recommendations, security audit oversight, training of information security managers, coordination of domestic security funding for cybersecurity issues, and shall set minimum standards for the recovery of information technology following a disaster. The funding for this office and the associated positions shall be provided with general revenue and is the responsibility of the department.

(4) The department may adopt rules relating to the security of data, information, and information technology pursuant to ss. 120.536(1) and 120.54 to administer this part.

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
Senate Bill 0856

Senate Bill 856 as originally filed stated the intent to revise laws relating to domestic security.

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.

The committee substitute finds that enhancements and improvements to the state law enforcement radio system should be considered based on joint task force recommendations. Recommendations implementation should be contingent upon appropriations.