

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

601-2384-06

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

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
appropriation and authorizing positions;
prescribing requirements for fire hydrants to
prevent backflow contamination of the domestic
water supply; providing an effective date.

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

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

3 282.318 Security of data and information technology
4 resources.--

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

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

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

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

26 ~~(c)3-~~ Develop, and periodically update, written
27 internal policies and procedures that are consistent with the
28 standard operating procedures recommended by the department to
29 assure the security of the data and information technology
30 resources of each agency. The internal policies and
31 procedures which, if disclosed, could facilitate the

1 unauthorized modification, disclosure, or destruction of data
2 or information technology resources are confidential
3 information and exempt from the provisions of s. 119.07(1),
4 except that such information shall be available to the Auditor
5 General in performing his or her postauditing duties.

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

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

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

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

29 (3) In order to ensure the security of data,
30 information, and information technology resources, the
31 department shall establish the Office of Information Security

1 and shall designate a Chief Information Security Officer as
2 the head of the office. The office shall coordinate its
3 activities with the Agency Chief Information Officers Council
4 as established in s. 282.315. The office is responsible for
5 developing a strategic plan for information technology
6 security which shall be submitted by December 1, 2006, to the
7 Executive Office of the Governor, the President of the Senate,
8 and the Speaker of the House of Representatives; developing
9 standards and templates for conducting comprehensive risk
10 analyses and information security audits by state agencies;
11 assisting agencies in their compliance with the provisions of
12 this section; establishing minimum standards for the recovery
13 of information technology following a disaster; and conducting
14 training for agency information security managers. This
15 subsection shall expire on June 30, 2007.

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

27 Section 3. For the 2006-2007 fiscal year, the sums of
28 \$529,387 in recurring funds and \$25,863 in nonrecurring funds
29 are appropriated from the General Revenue Fund to the
30 Department of Management Services for the Office of
31

1 Information Security, and five full-time equivalent positions
2 and an associated salary rate of 339,405 are authorized.

3 Section 4. All new and replacement fire hydrants in
4 this state shall have an internal hydrant valve device
5 installed which will prevent intentional or accidental
6 backflow contamination of the domestic water supply. Such
7 device may in no way delay access to the water supply for fire
8 protection.

9 Section 5. This act shall take effect upon becoming a
10 law.

11

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

15

16 Appropriates \$555,250 in general revenue and provides five
17 positions and associated salary rate of 339,405 to the
18 Department of Management Services for the Office of
19 Information Security.

20

21 Requires that all new and replacement fire hydrants have an
22 internal hydrant valve device installed to prevent backflow
23 contamination of the domestic water supply.

24

25

26

27

28

29

30

31