693796

LEGISLATIVE ACTION

| Senate | . | House |
|---|---|---|
| Comm: RCS | . | |
| 03/13/2014 | . | |
| | . | |
| | . | |
| | . | |

The Committee on Appropriations (Ring) recommended the following:

**Senate Amendment (with title amendment)**

Delete lines 987 - 1189
and insert:
Section 11. Section 282.318, Florida Statutes, is amended to read:
282.318 ~~Enterprise~~ Security of data and information technology.—
(1) This section may be cited as the "~~Enterprise Security of Data and~~ Information Technology Security Act."

693796

(2) As used in this section, the term "state agency" has the same meaning as provided in s. 282.0041, except that the term includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

~~(2) Information technology security is established as an enterprise information technology service as defined in s. 282.0041.~~

(3) The Agency for State ~~Enterprise Information~~ Technology is responsible for establishing standards and processes consistent with generally accepted best practices for information technology security and adopting rules that safeguard an agency's data, information, and information technology resources to ensure availability, confidentiality, and integrity ~~and publishing guidelines for ensuring an appropriate level of security for all data and information technology resources for executive branch agencies~~. The agency shall also ~~perform the following duties and responsibilities~~:

(a) Develop, and annually update by February 1, a statewide ~~an enterprise~~ information technology security strategic plan that includes security goals and objectives for the strategic issues of information technology security policy, risk management, training, incident management, and disaster recovery ~~survivability~~ planning.

(b) Develop and publish for use by state agencies an information technology security framework that, at a minimum, includes ~~enterprise security rules and published~~ guidelines and processes for:

1. Establishing asset management procedures to ensure that

693796

an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

3.~~1.~~ Completing comprehensive risk assessments ~~analyses~~ and information technology security audits and submitting completed assessments and audits to the Agency for State Technology ~~conducted by state agencies~~.

4. Identifying protection procedures to manage the protection of an agency's information, data, and information technology resources.

5. Establishing procedures for accessing information and data to ensure the confidentiality, integrity, and availability of such information and data.

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.

7.~~2.~~ Responding to information technology ~~suspected or confirmed information~~ security incidents, including ~~suspected or confirmed~~ breaches of personal information containing confidential or exempt data.

8. Recovering information and data in response to an information technology security incident. The recovery may include recommended improvements to the agency processes, policies, or guidelines.

9.~~3.~~ Developing agency strategic and operational

693796

information technology security plans required pursuant to this section~~, including strategic security plans and security program plans~~.

~~4. The recovery of information technology and data following a disaster.~~

10.~~5.~~ Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources that align with the state agency risk management strategy and that protect the confidentiality, integrity, and availability of information and data.

(c) Assist state agencies in complying with ~~the provisions of~~ this section.

~~(d) Pursue appropriate funding for the purpose of enhancing domestic security.~~

(d)~~(e)~~ In collaboration with the Cybercrime Office of the Department of Law Enforcement, provide training for state agency information security managers.

(e)~~(f)~~ Annually review the strategic and operational information technology security plans of executive branch agencies.

(4) ~~To assist the Agency for Enterprise Information Technology in carrying out its responsibilities,~~ Each state agency head shall, at a minimum:

(a) Designate an information security manager to administer the information technology security program of the state agency ~~for its data and information technology resources~~. This designation must be provided annually in writing to the Agency for State ~~Enterprise Information~~ Technology by January 1. A

693796

state agency's information security manager, for purposes of these information security duties, shall report directly to the agency head.

(b) Submit to the Agency for State ~~Enterprise Information~~ Technology annually by July 31, the state agency's strategic and operational information technology security plans developed pursuant to ~~the~~ rules and guidelines established by the Agency for State ~~Enterprise Information~~ Technology.

1. The state agency strategic information technology security plan must cover a 3-year period and, at a minimum, define security goals, intermediate objectives, and projected agency costs for the strategic issues of agency information security policy, risk management, security training, security incident response, and disaster recovery ~~survivability~~. The plan must be based on the statewide ~~enterprise strategic~~ information technology security strategic plan created by the Agency for State ~~Enterprise Information~~ Technology and include performance metrics that can be objectively measured to reflect the status of the state agency's progress in meeting security goals and objectives identified in the agency's strategic information security plan. ~~Additional issues may be included.~~

2. The state agency operational information technology security plan must include a progress report that objectively measures progress made towards ~~for~~ the prior operational information technology security plan and a project plan that includes activities, timelines, and deliverables for security objectives that~~, subject to current resources,~~ the state agency will implement during the current fiscal year. ~~The cost of implementing the portions of the plan which cannot be funded~~

693796

~~from current resources must be identified in the plan.~~

(c) Conduct, and update every 3 years, a comprehensive risk assessment ~~analysis~~ to determine the security threats to the data, information, and information technology resources of the agency. The risk assessment must comply with the risk assessment methodology developed by the Agency for State Technology and ~~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, ~~and~~ the Agency for State ~~Enterprise Information~~ Technology, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General ~~for performing postauditing duties~~.

(d) Develop, and periodically update, written internal policies and procedures, which include procedures for reporting information technology security incidents and breaches to the Cybercrime Office of the Department of Law Enforcement and ~~notifying~~ the Agency for State ~~Enterprise Information~~ Technology ~~when a suspected or confirmed breach, or an information security incident, occurs~~. Such policies and procedures must be consistent with the rules, ~~and~~ guidelines, and processes established by the Agency for State ~~Enterprise Information~~ Technology to ensure the security of the data, information, and information technology resources of the agency. The internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of

693796

the Department of Law Enforcement, ~~and~~ the Agency for State ~~Enterprise Information~~ Technology, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General ~~for performing postauditing duties~~.

(e) Implement managerial, operational, and technical ~~appropriate cost-effective~~ safeguards established by the Agency for State Technology to address identified risks to the data, information, and information technology resources of the agency.

(f) Ensure that periodic internal audits and evaluations of the agency's information technology security program for the data, information, and information technology resources of the agency are conducted. The results of such audits and evaluations are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, ~~and~~ the Agency for State ~~Enterprise Information~~ Technology, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General ~~for performing postauditing duties~~.

(g) Include appropriate information technology security requirements in the written specifications for the solicitation of information technology and information technology resources and services, which are consistent with the rules and guidelines established by the Agency for State ~~Enterprise Information~~ Technology in collaboration with the Department of Management Services.

(h) Provide information technology security awareness training to all state agency employees ~~and users of the agency's communication and information resources~~ concerning information

693796

technology security risks and the responsibility of employees ~~and users~~ to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement.

(i) Develop a process for detecting, reporting, and responding to threats, breaches, or information technology security ~~suspected or confirmed security~~ incidents that are~~,~~ ~~including suspected or confirmed breaches~~ consistent with the security rules, ~~and~~ guidelines, and processes established by the Agency for State ~~Enterprise Information~~ Technology.

1. All information technology ~~Suspected or confirmed information~~ security incidents and breaches must be ~~immediately~~ reported to the Agency for State ~~Enterprise Information~~ Technology.

2. For information technology security ~~incidents involving~~ breaches, state agencies shall provide notice in accordance with s. 817.5681 ~~and to the Agency for Enterprise Information Technology in accordance with this subsection~~.

~~(5) Each state agency shall include appropriate security requirements in the specifications for the solicitation of contracts for procuring information technology or information technology resources or services which are consistent with the rules and guidelines established by the Agency for Enterprise Information Technology.~~

(5)~~(6)~~ The Agency for State ~~Enterprise Information~~ Technology shall ~~may~~ adopt rules relating to information technology security and to administer ~~the provisions of~~ this section.

693796

214
215 ========== T I T L E A M E N D M E N T ==========
216 And the title is amended as follows:
217 Delete lines 33 - 36
218 and insert:
219 to the Southwood Shared Resource Center; amending s.
220 282.318, F.S.; changing the name of the Enterprise
221 Security of Data and Information Technology Act;
222 defining the term "agency" as used in the act;
223 requiring the Agency for State Technology to establish
224 and publish certain security standards and processes;
225 requiring state agencies to perform certain security-
226 related duties; requiring the agency to adopt rules;
227 conforming provisions;