122778

LEGISLATIVE ACTION

Senate	.	House
Comm: FAV	.	
02/05/2014	.	
	.	
	.	
	.	

The Committee on Governmental Oversight and Accountability (Ring) recommended the following:

Senate Amendment (with title amendment)

Delete lines 948 - 1125

and insert:

generally accepted best practices for information technology security, and adopting rules that safeguard an agency's data, information, and information technology resources to ensure its availability, confidentiality, and integrity ~~rules and publishing guidelines for ensuring an appropriate level of security for all data and information technology resources for~~

122778

~~executive branch agencies~~. The agency shall also ~~perform the following duties and responsibilities~~:

(a) By June 30, 2015, develop~~,~~ and annually update a statewide ~~by February 1, 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 an information security framework for use by state agencies which, at a minimum, includes guidelines and processes ~~enterprise security rules and published guidelines~~ for:

1. Developing and using a risk assessment methodology that will apply to state agencies to identify the priorities, constraints, risk tolerance, and assumptions.

2.~~1.~~ Completing comprehensive risk assessments ~~analyses~~ and information technology security audits. Such assessments and audits shall be conducted by state agencies and reviewed by the Agency for State Technology ~~conducted by state agencies~~.

3. Identifying protection procedures to manage the protection of a state agency's information, data, and information technology resources.

4. Detecting threats through proactive monitoring of events, continuous security monitoring, and specified detection processes.

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


122778

6.~~3.~~ Developing state agency strategic and operational information technology security plans required under this section~~, including strategic security plans and security program plans~~.

7.~~4.~~ Recovering ~~The recovery of~~ information technology and data in response to an information technology security incident ~~following a disaster~~. The recovery may include recommended improvements to the processes, policies, or guidelines.

8.~~5.~~ Establishing ~~The~~ managerial, operational, and technical safeguards for protecting state government data and information technology resources which align with state agency risk management strategies for protecting the confidentiality, integrity, and availability of information technology and data.

9. Establishing procedures for accessing information technology resources and data in order to limit authorized users, processes, or devices to authorized activities and transactions to ensure the confidentiality, integrity, and availability of such information and data.

10. Establishing asset management procedures to ensure that information technology resources are identified and consistently managed with their relative importance to business objectives.

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

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

(d)~~(c)~~ In collaboration with the Cybercrime Office in 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 state ~~executive branch~~ agencies.

(3)~~(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 who, for the purposes of his or her information technology security duties, shall report to the agency head and shall ~~to~~ administer the information technology security program of the 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.

(b) Submit annually 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 security strategic plan created by the Agency for State ~~Enterprise Information~~ Technology and include performance metrics that can be objectively measured in order to gauge the state agency's progress in meeting the security goals and objectives identified in the strategic information technology

122778

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 toward ~~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 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 state agency. The risk assessment must comply with the risk assessment methodology developed by the Agency for State Technology. The risk assessment ~~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, and the Cybercrime Office in the Department of Law Enforcement ~~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 in the Department of Law Enforcement and ~~notifying~~ the Agency for State ~~Enterprise Information~~ Technology, and for those agencies under the jurisdiction of the Governor, to the Chief Inspector General ~~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 state 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 in the Department of Law Enforcement, and the Agency for State ~~Enterprise Information~~ Technology, and for those agencies under the jurisdiction of the Governor, to the Chief Inspector General ~~for performing postauditing duties~~.

(e) Implement the 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 in the Department of Law Enforcement, and the Agency for State ~~Enterprise Information~~ Technology ~~for performing postauditing duties~~.

(g) Include appropriate information technology security requirements in the written specifications for the solicitation

122778

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.

(h) Require that state agency employees complete the security awareness training offered by the Agency for State Technology in collaboration with the Cybercrime Office in the Department of Law Enforcement. Coordinate with state agencies to provide agency-specific security training aligned with the agency operational information technology security plan. ~~Provide security awareness training to employees and users of the agency's communication and information resources concerning information security risks and the responsibility of employees and users to comply with policies, standards, guidelines, and operating procedures adopted by the agency to reduce those risks.~~

(i) Develop processes ~~a process~~ for detecting, reporting, and responding to information technology ~~suspected or confirmed~~ security threats or breaches or information technology security incidents which 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 ~~Suspected or confirmed~~ information technology security incidents and breaches must be ~~immediately~~ reported to the Cybercrime Office in the Department of Law Enforcement and the Agency for State ~~Enterprise Information~~ Technology.

2. For information technology security ~~incidents involving~~ breaches, 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.~~

(4) ~~(6)~~ The Agency for State ~~Enterprise Information~~ Technology may adopt rules relating to information technology security and

========== T I T L E A M E N D M E N T ==========

And the title is amended as follows:

Delete line 36

and insert:

with respect to information technology security; repealing s.