CHAPTER 2016-138

Committee Substitute for Committee Substitute for Committee Substitute for House Bill No. 1033

An act relating to information technology security; amending s. 20.61, F.S.; revising the membership of the Technology Advisory Council to include a cybersecurity expert; amending s. 282.318, F.S.; revising the duties of the Agency for State Technology; providing that risk assessments and security audits may be completed by a private vendor; providing for the establishment of computer security incident response teams within state agencies; providing for the establishment of an information technology security incident reporting process; providing for information technology security and cybersecurity awareness training; revising duties of state agency heads; establishing computer security incident response team responsibilities; establishing notification procedures and reporting timelines for an information technology security incident or breach; amending s. 282.0051, F.S.; requiring the agency to establish an information technology policy for certain state contracts; providing policy requirements; providing an effective date.

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

Section 1. Subsection (3) of section 20.61, Florida Statutes, is amended to read:

20.61 Agency for State Technology.—The Agency for State Technology is created within the Department of Management Services. The agency is a separate budget program and is not subject to control, supervision, or direction by the Department of Management Services, including, but not limited to, purchasing, transactions involving real or personal property, personnel, or budgetary matters.

(3) The Technology Advisory Council, consisting of seven members, is established within the Agency for State Technology and shall be maintained pursuant to s. 20.052. Four members of the council shall be appointed by the Governor, two of whom must be from the private sector <u>and one of whom must be a cybersecurity expert</u>. The President of the Senate and the Speaker of the House of Representatives shall each appoint one member of the council. The Attorney General, the Commissioner of Agriculture and Consumer Services, and the Chief Financial Officer shall jointly appoint one member by agreement of a majority of these officers. Upon initial establishment of the council, two of the Governor's appointments shall be for 2-year terms. Thereafter, all appointments shall be for 4-year terms.

(a) The council shall consider and make recommendations to the executive director on such matters as enterprise information technology policies, standards, services, and architecture. The council may also identify and recommend opportunities for the establishment of public-private

partnerships when considering technology infrastructure and services in order to accelerate project delivery and provide a source of new or increased project funding.

(b) The executive director shall consult with the council with regard to executing the duties and responsibilities of the agency related to statewide information technology strategic planning and policy.

(c) The council shall be governed by the Code of Ethics for Public Officers and Employees as set forth in part III of chapter 112, and each member must file a statement of financial interests pursuant to s. 112.3145.

Section 2. Subsections (3) and (4) of section 282.318, Florida Statutes, are amended to read:

282.318 Security of data and information technology.—

(3) The Agency for State Technology is responsible for establishing standards and processes consistent with generally accepted best practices for information technology security, to include cybersecurity, and adopting rules that safeguard an agency's data, information, and information technology resources to ensure availability, confidentiality, and integrity and to mitigate risks. The agency shall also:

(a) Develop, and annually update by February 1, a statewide 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 planning.

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

1. Establishing asset management procedures to ensure that 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. Completing comprehensive risk assessments and information technology security audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the Agency for State Technology.

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. Establishing agency computer security incident response teams and describing their responsibilities for responding to information technology security incidents, including 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. Establishing an information technology security incident reporting process that includes procedures and tiered reporting timeframes for notifying the Agency for State Technology and the Department of Law Enforcement of information technology security incidents. The tiered reporting timeframes shall be based upon the level of severity of the information technology security incidents being reported.

10. Incorporating information obtained through detection and response activities into the agency's information technology security incident response plans.

11.~~9.~~ Developing agency strategic and operational information technology security plans required pursuant to this section.

12.~~10.~~ 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 this section.

(d) In collaboration with the Cybercrime Office of the Department of Law Enforcement, annually provide training for state agency information security managers and computer security incident response team members that contains training on information technology security, including cybersecurity, threats, trends, and best practices.

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

(4) 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. This designation must be provided annually in writing to the Agency for State Technology

by January 1. A state agency's information security manager, for purposes of these information security duties, shall report directly to the agency head.

(b) In consultation with the Agency for State Technology and the Cybercrime Office of the Department of Law Enforcement, establish an agency computer security incident response team to respond to an information technology security incident. The agency computer security incident response team shall convene upon notification of an information technology security incident and must comply with all applicable guidelines and processes established pursuant to paragraph (3)(b).

(c)~~(b)~~ Submit to the Agency for State Technology annually by July 31, the state agency's strategic and operational information technology security plans developed pursuant to rules and guidelines established by the Agency for State 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. The plan must be based on the statewide information technology security strategic plan created by the Agency for State 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.

2. The state agency operational information technology security plan must include a progress report that objectively measures progress made towards the prior operational information technology security plan and a project plan that includes activities, timelines, and deliverables for security objectives that the state agency will implement during the current fiscal year.

(d)~~(c)~~ Conduct, and update every 3 years, a comprehensive risk assessment, which may be completed by a private sector vendor, to determine the security threats to the data, information, and information technology resources, including mobile devices and print environments, of the agency. The risk assessment must comply with the risk assessment methodology developed by the Agency for State Technology and is confidential and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Agency for State Technology, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(e)~~(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 the Agency for State Technology. Such policies and procedures must be consistent with the rules, guidelines, and processes

established by the Agency for State 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 the Department of Law Enforcement, the Agency for State Technology, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(f)~~(e)~~ Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended ~~established~~ by the Agency for State Technology to address identified risks to the data, information, and information technology resources of the agency.

(g)~~(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, the Agency for State Technology, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

(h)~~(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 Technology in collaboration with the Department of Management Services.

(i)~~(h)~~ Provide information technology security and cybersecurity awareness training to all state agency employees in the first 30 days after commencing employment concerning information technology security risks and the responsibility of employees 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.

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

1. All information technology security incidents and breaches must be reported to the Agency for State Technology and the Cybercrime Office of the Department of Law Enforcement and must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(b).

2. For information technology security breaches, state agencies shall provide notice in accordance with s. 501.171.

Section 3. Subsection (18) of section 282.0051, Florida Statutes, is renumbered as subsection (19), and a new subsection (18) is added to that section to read:

282.0051 Agency for State Technology; powers, duties, and functions. The Agency for State Technology shall have the following powers, duties, and functions:

(18) In collaboration with the Department of Management Services:

(a) Establish an information technology policy for all information technology-related state contracts, including state term contracts for information technology commodities, consultant services, and staff augmentation services. The information technology policy must include:

1. Identification of the information technology product and service categories to be included in state term contracts.

2. Requirements to be included in solicitations for state term contracts.

3. Evaluation criteria for the award of information technology-related state term contracts.

4. The term of each information technology-related state term contract.

5. The maximum number of vendors authorized on each state term contract.

(b) Evaluate vendor responses for state term contract solicitations and invitations to negotiate.

(c) Answer vendor questions on state term contract solicitations.

(d) Ensure that the information technology policy established pursuant to paragraph (a) is included in all solicitations and contracts which are administratively executed by the department.

Section 4. This act shall take effect July 1, 2016.

Approved by the Governor March 25, 2016.

Filed in Office Secretary of State March 25, 2016.