A bill to be entitled

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 for administration of a third party risk assessment; providing for the establishment of computer security incident response teams within state agencies; providing for continuously updated agency incident response plans; providing for information technology security and cybersecurity awareness training; providing for the establishment of a collaborative STEM program for cybersecurity workforce development; establishing computer security incident response team responsibilities; requiring a third party risk assessment; establishing notification procedures and reporting timelines for an information technology security incident or breach; providing appropriations; 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. At least one member must be a cybersecurity expert. Four members ~~of the council~~ shall be appointed by the Governor, two of whom must be from the private sector. 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. Section 282.318, Florida Statutes, is amended to read:

282.318 Security of data and information technology.—

(1) This section may be cited as the "Information Technology Security Act."

(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.

(3) The Agency for State Technology is responsible for establishing standards and processes consistent with generally accepted best practices for information technology security and 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 and submitting completed assessments and audits to the Agency for State Technology.

4. Completing risk assessments administered by a third party and submitting completed assessments to the Agency for State Technology.

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

6.~~5.~~ Establishing procedures for accessing information and

data to ensure the confidentiality, integrity, and availability of such information and data.

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

8.~~7.~~ Establishing a computer security incident response team to respond to suspected ~~Responding to~~ information technology security incidents, including breaches of personal information containing confidential or exempt data. An agency's computer security incident response team must convene immediately upon notice of a suspected security incident and shall determine the appropriate response.

9.~~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.

10. Establishing an information technology security incident reporting process, which must include a procedure for notification of the Agency for State Technology and the Cybercrime Office of the Department of Law Enforcement. The notification procedure must provide for tiered reporting timeframes, with incidents of critical impact reported immediately, incidents of high impact reported within 4 hours, and incidents of low impact reported within 5 business days.

11. Incorporating lessons learned through detection and response activities into agency incident response plans to

continuously improve organizational response activities.

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

13.~~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.

14. Providing all agency employees with information technology security and cybersecurity awareness education and training within 30 days after commencing employment.

(c) Assist state agencies in complying with this section.

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

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

(f) Develop and establish a cutting-edge internship or work-study program in science, technology, engineering, and mathematics (STEM) that will produce a more skilled

cybersecurity workforce in the state. The program must be a collaborative effort involving negotiations between the Agency for State Technology, relevant Agency for State Technology partners, and the Florida Center for Cybersecurity.

(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.

1. The information security manager shall establish a computer security incident response team to respond to a suspected computer security incident.

2. Computer security incident response team members shall convene immediately upon notice of a suspected security incident.

3. Computer security incident response team members shall determine the appropriate response for a suspected computer security incident. An appropriate response includes taking action to prevent expansion or recurrence of an incident, mitigating the effects of an incident, and eradicating an incident. Newly identified risks must be mitigated or documented as an accepted risk by computer security incident response team members.

(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.

(c) Conduct, and update every 3 years, a comprehensive risk assessment 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 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.

(d) Conduct a risk assessment that must be administered by a third party and must be completed by July 31, 2017. Subject to legislative appropriation, additional risk assessments may periodically be completed.

(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. Procedures for reporting information technology security incidents and breaches must include notification procedures and reporting timeframes. 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 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 attain an appropriate level of cyber literacy and reduce those risks. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement. Agencies shall ensure that privileged users, third party stakeholders, senior executives, and physical and information security personnel understand their roles and responsibilities.

(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. Procedures for reporting information technology security incidents and breaches must include notification procedures.

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

(k) Improve organizational response activities by incorporating lessons learned from current and previous detection and response activities into response plans.

(5) The Agency for State Technology shall adopt rules

relating to information technology security and to administer this section.

Section 3. (1) For the 2016-2017 fiscal year, the sums of $650,000 in nonrecurring funds and $50,000 in recurring funds are appropriated from the General Revenue Fund to the Agency for State Technology to conduct training exercises in coordination with the Florida National Guard.

(2) For the 2016-2017 fiscal year, the sum of $12 million is appropriated from the General Revenue Fund to the Agency for State Technology for the purpose of implementing this act.

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