

1                   A bill to be entitled  
2           An act relating to information technology security;  
3           amending s. 20.61, F.S.; revising the membership of  
4           the Technology Advisory Council to include a  
5           cybersecurity expert; amending s. 282.318, F.S.;  
6           revising the duties of the Agency for State  
7           Technology; providing that risk assessments and  
8           security audits may be completed by a private vendor;  
9           providing for the establishment of computer security  
10          incident response teams within state agencies;  
11          providing for the establishment of an information  
12          technology security incident reporting process;  
13          providing for information technology security and  
14          cybersecurity awareness training; revising duties of  
15          state agency heads; establishing computer security  
16          incident response team responsibilities; establishing  
17          notification procedures and reporting timelines for an  
18          information technology security incident or breach;  
19          providing an effective date.

20  
21   Be It Enacted by the Legislature of the State of Florida:

22  
23           Section 1. Subsection (3) of section 20.61, Florida  
24   Statutes, is amended to read:

25           20.61 Agency for State Technology.—The Agency for State  
26   Technology is created within the Department of Management

27 Services. The agency is a separate budget program and is not  
28 subject to control, supervision, or direction by the Department  
29 of Management Services, including, but not limited to,  
30 purchasing, transactions involving real or personal property,  
31 personnel, or budgetary matters.

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

45 (a) The council shall consider and make recommendations to  
46 the executive director on such matters as enterprise information  
47 technology policies, standards, services, and architecture. The  
48 council may also identify and recommend opportunities for the  
49 establishment of public-private partnerships when considering  
50 technology infrastructure and services in order to accelerate  
51 project delivery and provide a source of new or increased  
52 project funding.

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

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

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

63 282.318 Security of data and information technology.—

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

71 (a) Develop, and annually update by February 1, a  
72 statewide information technology security strategic plan that  
73 includes security goals and objectives for the strategic issues  
74 of information technology security policy, risk management,  
75 training, incident management, and disaster recovery planning.

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

79 | 1. Establishing asset management procedures to ensure that  
80 | an agency's information technology resources are identified and  
81 | managed consistent with their relative importance to the  
82 | agency's business objectives.

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

87 | 3. Completing comprehensive risk assessments and  
88 | information technology security audits, which may be completed  
89 | by a private sector vendor, and submitting completed assessments  
90 | and audits to the Agency for State Technology.

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

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

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

100 | 7. Establishing agency computer security incident response  
101 | teams and describing their responsibilities for responding to  
102 | information technology security incidents, including breaches of  
103 | personal information containing confidential or exempt data.

104 | 8. Recovering information and data in response to an

105 information technology security incident. The recovery may  
 106 include recommended improvements to the agency processes,  
 107 policies, or guidelines.

108 9. Establishing an information technology security  
 109 incident reporting process that includes procedures and tiered  
 110 reporting timeframes for notifying the Agency for State  
 111 Technology and the Department of Law Enforcement of information  
 112 technology security incidents. The tiered reporting timeframes  
 113 shall be based upon the level of severity of the information  
 114 technology security incidents being reported.

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

118 ~~11.9.~~ Developing agency strategic and operational  
 119 information technology security plans required pursuant to this  
 120 section.

121 ~~12.10.~~ Establishing the managerial, operational, and  
 122 technical safeguards for protecting state government data and  
 123 information technology resources that align with the state  
 124 agency risk management strategy and that protect the  
 125 confidentiality, integrity, and availability of information and  
 126 data.

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

128 (d) In collaboration with the Cybercrime Office of the  
 129 Department of Law Enforcement, annually provide training for  
 130 state agency information security managers and computer security

131 incident response team members that contains training on  
132 information technology security, including cybersecurity,  
133 threats, trends, and best practices.

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

137 (4) Each state agency head shall, at a minimum:

138 (a) Designate an information security manager to  
139 administer the information technology security program of the  
140 state agency. This designation must be provided annually in  
141 writing to the Agency for State Technology by January 1. A state  
142 agency's information security manager, for purposes of these  
143 information security duties, shall report directly to the agency  
144 head.

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

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

157 Technology.

158 1. The state agency strategic information technology  
159 security plan must cover a 3-year period and, at a minimum,  
160 define security goals, intermediate objectives, and projected  
161 agency costs for the strategic issues of agency information  
162 security policy, risk management, security training, security  
163 incident response, and disaster recovery. The plan must be based  
164 on the statewide information technology security strategic plan  
165 created by the Agency for State Technology and include  
166 performance metrics that can be objectively measured to reflect  
167 the status of the state agency's progress in meeting security  
168 goals and objectives identified in the agency's strategic  
169 information security plan.

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

177 (d)~~(e)~~ Conduct, and update every 3 years, a comprehensive  
178 risk assessment, which may be completed by a private sector  
179 vendor, to determine the security threats to the data,  
180 information, and information technology resources of the agency.  
181 The risk assessment must comply with the risk assessment  
182 methodology developed by the Agency for State Technology and is

183 confidential and exempt from s. 119.07(1), except that such  
 184 information shall be available to the Auditor General, the  
 185 Agency for State Technology, the Cybercrime Office of the  
 186 Department of Law Enforcement, and, for state agencies under the  
 187 jurisdiction of the Governor, the Chief Inspector General.

188 (e)~~(d)~~ Develop, and periodically update, written internal  
 189 policies and procedures, which include procedures for reporting  
 190 information technology security incidents and breaches to the  
 191 Cybercrime Office of the Department of Law Enforcement and the  
 192 Agency for State Technology. Such policies and procedures must  
 193 be consistent with the rules, guidelines, and processes  
 194 established by the Agency for State Technology to ensure the  
 195 security of the data, information, and information technology  
 196 resources of the agency. The internal policies and procedures  
 197 that, if disclosed, could facilitate the unauthorized  
 198 modification, disclosure, or destruction of data or information  
 199 technology resources are confidential information and exempt  
 200 from s. 119.07(1), except that such information shall be  
 201 available to the Auditor General, the Cybercrime Office of the  
 202 Department of Law Enforcement, the Agency for State Technology,  
 203 and, for state agencies under the jurisdiction of the Governor,  
 204 the Chief Inspector General.

205 (f)~~(e)~~ Implement managerial, operational, and technical  
 206 safeguards and risk assessment remediation plans recommended  
 207 ~~established~~ by the Agency for State Technology to address  
 208 identified risks to the data, information, and information



209 technology resources of the agency.

210 (g)~~(f)~~ Ensure that periodic internal audits and  
211 evaluations of the agency's information technology security  
212 program for the data, information, and information technology  
213 resources of the agency are conducted. The results of such  
214 audits and evaluations are confidential information and exempt  
215 from s. 119.07(1), except that such information shall be  
216 available to the Auditor General, the Cybercrime Office of the  
217 Department of Law Enforcement, the Agency for State Technology,  
218 and, for agencies under the jurisdiction of the Governor, the  
219 Chief Inspector General.

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

226 (i)~~(h)~~ Provide information technology security and  
227 cybersecurity awareness training to all state agency employees  
228 in the first 30 days after commencing employment concerning  
229 information technology security risks and the responsibility of  
230 employees to comply with policies, standards, guidelines, and  
231 operating procedures adopted by the state agency to reduce those  
232 risks. The training may be provided in collaboration with the  
233 Cybercrime Office of the Department of Law Enforcement.

234 (j)~~(i)~~ Develop a process for detecting, reporting, and

235 | responding to threats, breaches, or information technology  
236 | security incidents that are consistent with the security rules,  
237 | guidelines, and processes established by the Agency for State  
238 | Technology.

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

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

246 |       Section 3. This act shall take effect July 1, 2016.