

By the Committee on Governmental Oversight and Accountability

585-02231-16

20167050\_\_

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; requiring the council, in  
6           coordination with the Florida Center for  
7           Cybersecurity, to identify and recommend STEM training  
8           opportunities; amending s. 282.318, F.S.; revising  
9           duties of the Agency for State Technology; providing  
10          for administration of a third-party risk assessment;  
11          providing for the establishment of computer security  
12          incident response teams within state agencies;  
13          establishing procedures for reporting information  
14          technology security incidents; providing for  
15          continuously updated agency incident response plans;  
16          providing for information technology security and  
17          cybersecurity awareness training; providing for the  
18          establishment of a collaborative STEM program for  
19          cybersecurity workforce development; establishing  
20          computer security incident response team  
21          responsibilities; requiring each state agency head to  
22          conduct a third-party administered risk assessment;  
23          establishing notification procedures and reporting  
24          timelines for an information technology security  
25          incident or breach; amending s. 1001.03, F.S.;  
26          revising entities directed to adopt a unified state  
27          plan for K-20 STEM education to include the Technology  
28          Advisory Council; amending s. 1004.444, F.S.;  
29          requiring the Florida Center for Cybersecurity to  
30          coordinate with the Technology Advisory Council;  
31          providing appropriations; providing an effective date.  
32

585-02231-16

20167050\_\_

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

34  
35 Section 1. Subsection (3) of section 20.61, Florida  
36 Statutes, is amended to read:

37 20.61 Agency for State Technology.—The Agency for State  
38 Technology is created within the Department of Management  
39 Services. The agency is a separate budget program and is not  
40 subject to control, supervision, or direction by the Department  
41 of Management Services, including, but not limited to,  
42 purchasing, transactions involving real or personal property,  
43 personnel, or budgetary matters.

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

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

585-02231-16

20167050\_\_

62 technology infrastructure and services in order to accelerate  
63 project delivery and provide a source of new or increased  
64 project funding.

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

69 (c) The council shall coordinate with the Florida Center  
70 for Cybersecurity to identify and recommend opportunities for  
71 establishing cutting-edge educational and training programs in  
72 science, technology, engineering, and mathematics (STEM) for  
73 students, consistent with the unified state plan adopted  
74 pursuant to s. 1001.03(17); increasing the cybersecurity  
75 workforce in the state; and preparing cybersecurity  
76 professionals to possess a wide range of expertise.

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

81 Section 2. Section 282.318, Florida Statutes, is amended to  
82 read:

83 282.318 Security of data and information technology.-

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

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

585-02231-16

20167050\_\_

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

98 (a) Develop, and annually update by February 1, a statewide  
99 information technology security strategic plan that includes  
100 security goals and objectives for the strategic issues of  
101 information technology security policy, risk management,  
102 training, incident management, and disaster recovery planning.

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

106 1. Establishing asset management procedures to ensure that  
107 an agency's information technology resources are identified and  
108 managed consistent with their relative importance to the  
109 agency's business objectives.

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

114 3. Completing comprehensive risk assessments and  
115 information technology security audits and submitting completed  
116 assessments and audits to the Agency for State Technology.

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

585-02231-16

20167050\_\_

120       ~~5.4.~~ Identifying protection procedures to manage the  
121 protection of an agency's information, data, and information  
122 technology resources.

123       ~~6.5.~~ Establishing procedures for accessing information and  
124 data to ensure the confidentiality, integrity, and availability  
125 of such information and data.

126       ~~7.6.~~ Detecting threats through proactive monitoring of  
127 events, continuous security monitoring, and defined detection  
128 processes.

129       ~~8.7.~~ Establishing a computer security incident response  
130 team to respond to suspected ~~Responding to~~ information  
131 technology security incidents, including breaches of personal  
132 information containing confidential or exempt data. An agency's  
133 computer security incident response team must convene as soon as  
134 practicable upon notice of a suspected security incident and  
135 shall determine the appropriate response.

136       ~~9.8.~~ Recovering information and data in response to an  
137 information technology security incident. The recovery may  
138 include recommended improvements to the agency processes,  
139 policies, or guidelines.

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

585-02231-16

20167050\_\_

149 11. Incorporating lessons learned through detection and  
150 response activities into agency incident response plans to  
151 continuously improve organizational response activities.

152 ~~12.9.~~ Developing agency strategic and operational  
153 information technology security plans required pursuant to this  
154 section.

155 ~~13.10.~~ Establishing the managerial, operational, and  
156 technical safeguards for protecting state government data and  
157 information technology resources that align with the state  
158 agency risk management strategy and that protect the  
159 confidentiality, integrity, and availability of information and  
160 data.

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

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

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

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

174 (f) Develop and establish a cutting-edge internship or  
175 work-study program in science, technology, engineering, and  
176 mathematics (STEM), which will produce a more skilled  
177 cybersecurity workforce in the state. The program must be a

585-02231-16

20167050\_\_

178 collaborative effort involving negotiations between the Agency  
179 for State Technology, relevant Agency for State Technology  
180 partners, and the Florida Center for Cybersecurity.

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

182 (a) Designate an information security manager to administer  
183 the information technology security program of the state agency.  
184 This designation must be provided annually in writing to the  
185 Agency for State Technology by January 1. A state agency's  
186 information security manager, for purposes of these information  
187 security duties, shall report directly to the agency head.

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

191 2. Computer security incident response team members shall  
192 convene as soon as practicable upon notice of a suspected  
193 security incident.

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

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

585-02231-16

20167050\_\_

207           1. The state agency strategic information technology  
208 security plan must cover a 3-year period and, at a minimum,  
209 define security goals, intermediate objectives, and projected  
210 agency costs for the strategic issues of agency information  
211 security policy, risk management, security training, security  
212 incident response, and disaster recovery. The plan must be based  
213 on the statewide information technology security strategic plan  
214 created by the Agency for State Technology and include  
215 performance metrics that can be objectively measured to reflect  
216 the status of the state agency's progress in meeting security  
217 goals and objectives identified in the agency's strategic  
218 information security plan.

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

226           (c) Conduct, and update every 3 years, a comprehensive risk  
227 assessment to determine the security threats to the data,  
228 information, and information technology resources of the agency.  
229 The risk assessment must comply with the risk assessment  
230 methodology developed by the Agency for State Technology and is  
231 confidential and exempt from s. 119.07(1), except that such  
232 information shall be available to the Auditor General, the  
233 Agency for State Technology, the Cybercrime Office of the  
234 Department of Law Enforcement, and, for state agencies under the  
235 jurisdiction of the Governor, the Chief Inspector General.



585-02231-16

20167050\_\_

236 (d) Subject to annual legislative appropriation, conduct a  
237 risk assessment that must be administered by a third party  
238 consistent with the guidelines and processes prescribed by the  
239 Agency for State Technology. An initial risk assessment must be  
240 completed by July 31, 2017. Additional risk assessments shall be  
241 completed periodically consistent with the guidelines and  
242 processes prescribed by the Agency for State Technology.

243 (e)~~(d)~~ Develop, and periodically update, written internal  
244 policies and procedures, which include procedures for reporting  
245 information technology security incidents and breaches to the  
246 Cybercrime Office of the Department of Law Enforcement and the  
247 Agency for State Technology. Procedures for reporting  
248 information technology security incidents and breaches must  
249 include notification procedures and reporting timeframes. Such  
250 policies and procedures must be consistent with the rules,  
251 guidelines, and processes established by the Agency for State  
252 Technology to ensure the security of the data, information, and  
253 information technology resources of the agency. The internal  
254 policies and procedures that, if disclosed, could facilitate the  
255 unauthorized modification, disclosure, or destruction of data or  
256 information technology resources are confidential information  
257 and exempt from s. 119.07(1), except that such information shall  
258 be available to the Auditor General, the Cybercrime Office of  
259 the Department of Law Enforcement, the Agency for State  
260 Technology, and, for state agencies under the jurisdiction of  
261 the Governor, the Chief Inspector General.

262 (f)~~(e)~~ Implement managerial, operational, and technical  
263 safeguards established by the Agency for State Technology to  
264 address identified risks to the data, information, and

585-02231-16

20167050\_\_

265 information technology resources of the agency.

266 (g)~~(f)~~ Ensure that periodic internal audits and evaluations  
267 of the agency's information technology security program for the  
268 data, information, and information technology resources of the  
269 agency are conducted. The results of such audits and evaluations  
270 are confidential information and exempt from s. 119.07(1),  
271 except that such information shall be available to the Auditor  
272 General, the Cybercrime Office of the Department of Law  
273 Enforcement, the Agency for State Technology, and, for agencies  
274 under the jurisdiction of the Governor, the Chief Inspector  
275 General.

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

282 (i)~~(h)~~ Provide information technology security and  
283 cybersecurity awareness training to all state agency employees  
284 in the first 30 days after commencing employment concerning  
285 information technology security risks and the responsibility of  
286 employees to comply with policies, standards, guidelines, and  
287 operating procedures adopted by the state agency to attain an  
288 appropriate level of cyber literacy and reduce those risks. The  
289 training may be provided in collaboration with the Cybercrime  
290 Office of the Department of Law Enforcement. Agencies shall  
291 ensure that privileged users, third-party stakeholders, senior  
292 executives, and physical and information security personnel  
293 understand their roles and responsibilities.

585-02231-16

20167050\_\_

294 (j) In collaboration with the Cybercrime Office of the  
295 Department of Law Enforcement, provide training on cybersecurity  
296 threats, trends, and best practices to computer security  
297 incident response team members at least annually.

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

303 1. All information technology security incidents and  
304 breaches must be reported to the Agency for State Technology.  
305 Procedures for reporting information technology security  
306 incidents and breaches must include notification procedures.

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

309 (l) Improve organizational response activities by  
310 incorporating lessons learned from current and previous  
311 detection and response activities into response plans.

312 (5) The Agency for State Technology shall adopt rules  
313 relating to information technology security and to administer  
314 this section.

315 Section 3. Subsection (17) of section 1001.03, Florida  
316 Statutes, is amended to read:

317 1001.03 Specific powers of State Board of Education.—

318 (17) UNIFIED STATE PLAN FOR SCIENCE, TECHNOLOGY,  
319 ENGINEERING, AND MATHEMATICS (STEM).—The State Board of  
320 Education, in consultation with the Board of Governors, the  
321 Technology Advisory Council, and the Department of Economic  
322 Opportunity, shall adopt a unified state plan to improve K-20

585-02231-16

20167050\_\_

323 STEM education and prepare students for high-skill, high-wage,  
324 and high-demand employment in STEM and STEM-related fields.

325 Section 4. Section 1004.444, Florida Statutes, is amended  
326 to read:

327 1004.444 Florida Center for Cybersecurity.—

328 (1) The Florida Center for Cybersecurity is established  
329 within the University of South Florida.

330 (2) The goals of the center are to:

331 (a) Position Florida as the national leader in  
332 cybersecurity and its related workforce through education,  
333 research, and community engagement. The center shall coordinate  
334 with the Technology Advisory Council in pursuit of this goal.

335 (b) Assist in the creation of jobs in the state's  
336 cybersecurity industry and enhance the existing cybersecurity  
337 workforce. The center shall coordinate with the Technology  
338 Advisory Council in pursuit of this goal.

339 (c) Act as a cooperative facilitator for state business and  
340 higher education communities to share cybersecurity knowledge,  
341 resources, and training. The center shall coordinate with the  
342 Technology Advisory Council in pursuit of this goal.

343 (d) Seek out partnerships with major military installations  
344 to assist, when possible, in homeland cybersecurity defense  
345 initiatives.

346 (e) Attract cybersecurity companies to the state with an  
347 emphasis on defense, finance, health care, transportation, and  
348 utility sectors.

349 Section 5. For the 2016-2017 fiscal year, the sums of  
350 \$650,000 in nonrecurring funds and \$50,000 in recurring funds  
351 are appropriated from the General Revenue Fund to the Agency for

585-02231-16

20167050\_\_

352 State Technology to conduct training exercises in coordination  
353 with the Florida National Guard.

354 Section 6. For the 2016-2017 fiscal year, the sum of \$12  
355 million is appropriated from the General Revenue Fund to the  
356 Agency for State Technology for the purpose of implementing this  
357 act.

358 Section 7. This act shall take effect July 1, 2016.