



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

1
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 amending s. 282.0051, F.S.; requiring the agency to
20 establish an information technology policy for certain
21 state contracts; providing policy requirements;
22 providing an effective date.

23
24 Be It Enacted by the Legislature of the State of Florida:

25
26 Section 1. Subsection (3) of section 20.61, Florida



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

27 Statutes, is amended to read:

28 20.61 Agency for State Technology.—The Agency for State
29 Technology is created within the Department of Management
30 Services. The agency is a separate budget program and is not
31 subject to control, supervision, or direction by the Department
32 of Management Services, including, but not limited to,
33 purchasing, transactions involving real or personal property,
34 personnel, or budgetary matters.

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

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



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

53 | technology infrastructure and services in order to accelerate
54 | project delivery and provide a source of new or increased
55 | project funding.

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

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

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

66 | 282.318 Security of data and information technology.—

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

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



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

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

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

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

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

94 4. Identifying protection procedures to manage the
95 protection of an agency's information, data, and information
96 technology resources.

97 5. Establishing procedures for accessing information and
98 data to ensure the confidentiality, integrity, and availability
99 of such information and data.

100 6. Detecting threats through proactive monitoring of
101 events, continuous security monitoring, and defined detection
102 processes.

103 7. Establishing agency computer security incident response
104 teams and describing their responsibilities for responding to



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

105 | information technology security incidents, including breaches of
106 | personal information containing confidential or exempt data.

107 | 8. Recovering information and data in response to an
108 | information technology security incident. The recovery may
109 | include recommended improvements to the agency processes,
110 | policies, or guidelines.

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

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

121 | ~~11.9.~~ Developing agency strategic and operational
122 | information technology security plans required pursuant to this
123 | section.

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

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



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

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

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

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

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

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

156 (c) ~~(b)~~ Submit to the Agency for State Technology annually



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

157 | by July 31, the state agency's strategic and operational
158 | information technology security plans developed pursuant to
159 | rules and guidelines established by the Agency for State
160 | Technology.

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

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

180 | ~~(d)-(e)~~ Conduct, and update every 3 years, a comprehensive
181 | risk assessment, which may be completed by a private sector
182 | vendor, to determine the security threats to the data,



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

183 information, and information technology resources, including
184 mobile devices and print environments, of the agency. The risk
185 assessment must comply with the risk assessment methodology
186 developed by the Agency for State Technology and is confidential
187 and exempt from s. 119.07(1), except that such information shall
188 be available to the Auditor General, the Agency for State
189 Technology, the Cybercrime Office of the Department of Law
190 Enforcement, and, for state agencies under the jurisdiction of
191 the Governor, the Chief Inspector General.

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



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

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

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

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

230 (i)~~(h)~~ Provide information technology security and
231 cybersecurity awareness training to all state agency employees
232 in the first 30 days after commencing employment concerning
233 information technology security risks and the responsibility of
234 employees to comply with policies, standards, guidelines, and



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

235 | operating procedures adopted by the state agency to reduce those
236 | risks. The training may be provided in collaboration with the
237 | Cybercrime Office of the Department of Law Enforcement.

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

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

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

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

253 | 282.0051 Agency for State Technology; powers, duties, and
254 | functions.—The Agency for State Technology shall have the
255 | following powers, duties, and functions:

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

258 | (a) Establish an information technology policy for all
259 | information technology-related state contracts, including state
260 | term contracts for information technology commodities,



ENROLLED

CS/CS/CS/HB 1033, Engrossed 1

2016 Legislature

261 consultant services, and staff augmentation services. The
262 information technology policy must include:

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

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

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

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

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

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

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

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

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