

1 A bill to be entitled
2 An act relating to public records; amending s.
3 282.318, F.S.; creating exemptions from public records
4 requirements for certain records held by a state
5 agency which identify detection, investigation, or
6 response practices for suspected or confirmed
7 information technology security incidents and for
8 certain portions of risk assessments, evaluations,
9 external audits, and other reports of a state agency's
10 information technology program; authorizing disclosure
11 of confidential and exempt information to certain
12 agencies and officers; providing for retroactive
13 application; providing for future legislative review
14 and repeal of the exemptions; providing statements of
15 public necessity; providing a contingent effective
16 date.

17
18 Be It Enacted by the Legislature of the State of Florida:

19
20 Section 1. Paragraph (i) of subsection (4) of section
21 282.318, Florida Statutes, is amended, present subsection (5) of
22 that section is renumbered as subsection (6), and a new
23 subsection (5) is added to that section, to read:

24 282.318 Security of data and information technology.—

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

26 (i) Develop a process for detecting, reporting, and

27 | responding to threats, breaches, or information technology
28 | security incidents which is ~~that are~~ consistent with the
29 | security rules, guidelines, and processes established by the
30 | Agency for State Technology.

31 | 1. All information technology security incidents and
32 | breaches must be reported to the Agency for State Technology.

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

35 | 3. Records held by a state agency which identify
36 | detection, investigation, or response practices for suspected or
37 | confirmed information technology security incidents, including
38 | suspected or confirmed breaches, are confidential and exempt
39 | from s. 119.07(1) and s. 24(a), Art. I of the State
40 | Constitution, if the disclosure of such records would facilitate
41 | unauthorized access to or the unauthorized modification,
42 | disclosure, or destruction of:

43 | a. Data or information, whether physical or virtual; or

44 | b. Information technology resources, which includes:

45 | (I) Information relating to the security of the agency's
46 | technologies, processes, and practices designed to protect
47 | networks, computers, data processing software, and data from
48 | attack, damage, or unauthorized access; or

49 | (II) Security information, whether physical or virtual,
50 | which relates to the agency's existing or proposed information
51 | technology systems.

52 |

53 Such records shall be available to the Auditor General, the
54 Agency for State Technology, the Cybercrime Office of the
55 Department of Law Enforcement, and, for state agencies under the
56 jurisdiction of the Governor, the Chief Inspector General. Such
57 records may be made available to a local government, another
58 state agency, or a federal agency for information technology
59 security purposes or in furtherance of the state agency's
60 official duties. This exemption applies to such records held by
61 a state agency before, on, or after the effective date of this
62 exemption. This subparagraph is subject to the Open Government
63 Sunset Review Act in accordance with s. 119.15 and shall stand
64 repealed on October 2, 2021, unless reviewed and saved from
65 repeal through reenactment by the Legislature.

66 (5) The portions of risk assessments, evaluations,
67 external audits, and other reports of a state agency's
68 information technology security program for the data,
69 information, and information technology resources of the state
70 agency which are held by a state agency are confidential and
71 exempt from s. 119.07(1) and s. 24(a), Art. I of the State
72 Constitution if the disclosure of such portions of records would
73 facilitate unauthorized access to or the unauthorized
74 modification, disclosure, or destruction of:

75 (a) Data or information, whether physical or virtual; or

76 (b) Information technology resources, which include:

77 1. Information relating to the security of the agency's
78 technologies, processes, and practices designed to protect

79 networks, computers, data processing software, and data from
80 attack, damage, or unauthorized access; or

81 2. Security information, whether physical or virtual,
82 which relates to the agency's existing or proposed information
83 technology systems.

84
85 Such portions of records shall be available to the Auditor
86 General, the Cybercrime Office of the Department of Law
87 Enforcement, the Agency for State Technology, and, for agencies
88 under the jurisdiction of the Governor, the Chief Inspector
89 General. Such portions of records may be made available to a
90 local government, another state agency, or a federal agency for
91 information technology security purposes or in furtherance of
92 the state agency's official duties. For purposes of this
93 subsection, "external audit" means an audit that is conducted by
94 an entity other than the state agency that is the subject of the
95 audit. This exemption applies to such records held by a state
96 agency before, on, or after the effective date of this
97 exemption. This subsection is subject to the Open Government
98 Sunset Review Act in accordance with s. 119.15 and shall stand
99 repealed on October 2, 2021, unless reviewed and saved from
100 repeal through reenactment by the Legislature.

101 Section 2. (1)(a) The Legislature finds that it is a
102 public necessity that public records held by a state agency
103 which identify detection, investigation, or response practices
104 for suspected or confirmed information technology security

105 incidents, including suspected or confirmed breaches, be made
106 confidential and exempt from s. 119.07(1), Florida Statutes, and
107 s. 24(a), Article I of the State Constitution if the disclosure
108 of such records would facilitate unauthorized access to or the
109 unauthorized modification, disclosure, or destruction of:

110 1. Data or information, whether physical or virtual; or

111 2. Information technology resources, which includes:

112 a. Information relating to the security of the agency's
113 technologies, processes, and practices designed to protect
114 networks, computers, data processing software, and data from
115 attack, damage, or unauthorized access; or

116 b. Security information, whether physical or virtual,
117 which relates to the agency's existing or proposed information
118 technology systems.

119 (b) Such records shall be made confidential and exempt for
120 the following reasons:

121 1. Records held by a state agency which identify
122 information technology detection, investigation, or response
123 practices for suspected or confirmed information technology
124 incidents or breaches are likely to be used in the investigation
125 of the incident or breach. The release of such information could
126 impede the investigation and impair the ability of reviewing
127 entities to effectively and efficiently execute their
128 investigative duties. In addition, the release of such
129 information before completion of an active investigation could
130 jeopardize the ongoing investigation.

131 2. An investigation of an information technology security
132 incident or breach is likely to result in the gathering of
133 sensitive personal information, including identification numbers
134 and personal financial and health information not otherwise
135 exempt or confidential and exempt from public records
136 requirements under any other law. Such information could be used
137 for the purpose of identity theft or other crimes. In addition,
138 release of such information could subject possible victims of
139 the incident or breach to further harm.

140 3. Disclosure of a record, including a computer forensic
141 analysis, or other information that would reveal weaknesses in a
142 state agency's data security could compromise the future
143 security of that agency or other entities if such information
144 were available upon conclusion of an investigation or once an
145 investigation ceased to be active. The disclosure of such a
146 record or information could compromise the security of state
147 agencies and make those state agencies susceptible to future
148 data incidents or breaches.

149 4. Such records are likely to contain proprietary
150 information about the security of the system at issue. The
151 disclosure of such information could result in the
152 identification of vulnerabilities and further breaches of that
153 system. In addition, the release of such information could give
154 business competitors an unfair advantage and weaken the position
155 of the entity supplying the proprietary information in the
156 marketplace.

157 5. The disclosure of such records could potentially
158 compromise the confidentiality, integrity, and availability of
159 state agency data and information technology resources, which
160 would significantly impair the administration of vital
161 governmental programs. It is necessary that this information be
162 made confidential in order to protect the technology systems,
163 resources, and data of state agencies. The Legislature further
164 finds that this public records exemption be given retroactive
165 application because it is remedial in nature.

166 (2) (a) The Legislature also finds that it is a public
167 necessity that portions of risk assessments, evaluations,
168 external audits, and other reports of a state agency's
169 information technology security program for the data,
170 information, and information technology resources of the state
171 agency which are held by a state agency be made confidential and
172 exempt from s. 119.07(1), Florida Statutes, and s. 24(a),
173 Article I of the State Constitution if the disclosure of such
174 portions of records would facilitate unauthorized access to or
175 the unauthorized modification, disclosure, or destruction of:

176 1. Data or information, whether physical or virtual; or

177 2. Information technology resources, which includes:

178 a. Information relating to the security of the agency's
179 technologies, processes, and practices designed to protect
180 networks, computers, data processing software, and data from
181 attack, damage, or unauthorized access; or

182 b. Security information, whether physical or virtual,

183 which relates to the agency's existing or proposed information
184 technology systems.

185 (b) The Legislature finds that it may be valuable,
186 prudent, or critical to a state agency to have an independent
187 entity conduct a risk assessment, an audit, or an evaluation or
188 complete a report of the state agency's information technology
189 program or related systems. Such documents would likely include
190 an analysis of the state agency's current information technology
191 program or systems which could clearly identify vulnerabilities
192 or gaps in current systems or processes and propose
193 recommendations to remedy identified vulnerabilities. The
194 disclosure of such portions of records would jeopardize the
195 information technology security of the state agency, and
196 compromise the integrity and availability of agency data and
197 information technology resources, which would significantly
198 impair the administration of governmental programs. It is
199 necessary that such portions of records be made confidential and
200 exempt from public records requirements in order to protect
201 agency technology systems, resources, and data. The Legislature
202 further finds that this public records exemption shall be given
203 retroactive application because it is remedial in nature.

204 Section 3. This act shall take effect upon becoming a law,
205 if CS/CS/CS/HB 1033 or similar legislation is adopted in the
206 same legislative session or an extension thereof and becomes
207 law.