



237354

LEGISLATIVE ACTION

Senate	.	House
Comm: RCS	.	
12/01/2015	.	
	.	
	.	
	.	

The Committee on Governmental Oversight and Accountability
(Hays) recommended the following:

Senate Amendment (with title amendment)

Delete everything after the enacting clause
and insert:

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

282.318 Security of data and information technology.—

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



237354

11 (i) Develop a process for detecting, reporting, and
12 responding to threats, breaches, or information technology
13 security incidents which is ~~that are~~ consistent with the
14 security rules, guidelines, and processes established by the
15 Agency for State Technology.

16 1. All information technology security incidents and
17 breaches must be reported to the Agency for State Technology.

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

20 3. Records held by a state agency which identify detection,
21 investigation, or response practices for suspected or confirmed
22 information technology security incidents, including suspected
23 or confirmed breaches, are confidential and exempt from s.
24 119.07(1) and s. 24(a), Art. I of the State Constitution, if the
25 disclosure of such records would facilitate unauthorized access
26 to or the unauthorized modification, disclosure, or destruction
27 of:

28 a. Data or information, whether physical or virtual; or

29 b. Information technology resources, which includes:

30 (I) Information relating to the security of the agency's
31 technologies, processes, and practices designed to protect
32 networks, computers, data processing software, and data from
33 attack, damage, or unauthorized access; or

34 (II) Security information, whether physical or virtual,
35 which relates to the agency's existing or proposed information
36 technology systems.

37
38 Such records shall be available to the Auditor General, the
39 Agency for State Technology, the Cybercrime Office of the



237354

40 Department of Law Enforcement, and, for state agencies under the
41 jurisdiction of the Governor, the Chief Inspector General. Such
42 records may be made available to a local government, another
43 state agency, or a federal agency for information technology
44 security purposes or in furtherance of the state agency's
45 official duties. This exemption applies to such records held by
46 a state agency before, on, or after the effective date of this
47 exemption. This subparagraph is subject to the Open Government
48 Sunset Review Act in accordance with s. 119.15 and shall stand
49 repealed on October 2, 2021, unless reviewed and saved from
50 repeal through reenactment by the Legislature.

51 (5) The portions of risk assessments, evaluations, external
52 audits, and other reports of a state agency's information
53 technology security program for the data, information, and
54 information technology resources of the state agency which are
55 held by a state agency are confidential and exempt from s.
56 119.07(1) and s. 24(a), Art. I of the State Constitution if the
57 disclosure of such portions of records would facilitate
58 unauthorized modification, disclosure, or destruction of:

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

60 (b) Information technology resources, which include:

61 1. Information relating to the security of the agency's
62 technologies, processes, and practices designed to protect
63 networks, computers, data processing software, and data from
64 attack, damage, or unauthorized access; or

65 2. Security information, whether physical or virtual, which
66 relates to the agency's existing or proposed information
67 technology systems.

68



237354

69 Such portions of records shall be available to the Auditor
70 General, the Cybercrime Office of the Department of Law
71 Enforcement, the Agency for State Technology, and, for agencies
72 under the jurisdiction of the Governor, the Chief Inspector
73 General. Such portions of records may be made available to a
74 local government, another state agency, or a federal agency for
75 information technology security purposes or in furtherance of
76 the state agency's official duties. For purposes of this
77 subsection, "external audit" means an audit that is conducted by
78 an entity other than the state agency that is the subject of the
79 audit. This exemption applies to such records held by a state
80 agency before, on, or after the effective date of this
81 exemption. This subsection is subject to the Open Government
82 Sunset Review Act in accordance with s. 119.15 and shall stand
83 repealed on October 2, 2021, unless reviewed and saved from
84 repeal through reenactment by the Legislature.

85 Section 2. (1) (a) The Legislature finds that it is a public
86 necessity that public records held by a state agency which
87 identify detection, investigation, or response practices for
88 suspected or confirmed information technology security
89 incidents, including suspected or confirmed breaches, be made
90 confidential and exempt from s. 119.07(1), Florida Statutes, and
91 s. 24(a), Article I of the State Constitution if the disclosure
92 of such records would facilitate unauthorized access to or the
93 unauthorized modification, disclosure, or destruction of:

- 94 1. Data or information, whether physical or virtual; or
95 2. Information technology resources, which includes:
96 a. Information relating to the security of the agency's
97 technologies, processes, and practices designed to protect



237354

98 networks, computers, data processing software, and data from
99 attack, damage, or unauthorized access; or

100 b. Security information, whether physical or virtual, which
101 relates to the agency's existing or proposed information
102 technology systems.

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

105 1. Records held by a state agency which identify
106 information technology detection, investigation, or response
107 practices for suspected or confirmed information technology
108 incidents or breaches are likely to be used in the investigation
109 of the incident or breach. The release of such information could
110 impede the investigation and impair the ability of reviewing
111 entities to effectively and efficiently execute their
112 investigative duties. In addition, the release of such
113 information before completion of an active investigation could
114 jeopardize the ongoing investigation.

115 2. An investigation of an information technology security
116 incident or breach is likely to result in the gathering of
117 sensitive personal information, including identification numbers
118 and personal financial and health information not otherwise
119 exempt or confidential and exempt from public records
120 requirements under any other law. Such information could be used
121 for the purpose of identity theft or other crimes. In addition,
122 release of such information could subject possible victims of
123 the incident or breach to further harm.

124 3. Disclosure of a risk assessment or evaluation, including
125 computer forensic analysis, or other information that would
126 reveal weaknesses in a state agency's data security could



237354

127 compromise the future security of that agency or other entities
128 if such information were available upon conclusion of an
129 investigation or once an investigation ceased to be active. The
130 disclosure of such a report or information could compromise the
131 security of state agencies and make those state agencies
132 susceptible to future data incidents or breaches.

133 4. Such records are likely to contain proprietary
134 information about the security of the system at issue. The
135 disclosure of such information could result in the
136 identification of vulnerabilities and further breaches of that
137 system. In addition, the release of such information could give
138 business competitors an unfair advantage and weaken the position
139 of the entity supplying the proprietary information in the
140 marketplace.

141 5. The disclosure of such records could potentially
142 compromise the confidentiality, integrity, and availability of
143 state agency data and information technology resources, which
144 would significantly impair the administration of vital
145 governmental programs. It is necessary that this information be
146 made confidential in order to protect the technology systems,
147 resources, and data of state agencies. The Legislature further
148 finds that this public records exemption be given retroactive
149 application because it is remedial in nature.

150 (2) (a) The Legislature also finds that it is a public
151 necessity that portions of risk assessments, evaluations,
152 external audits, and other reports of a state agency's
153 information technology security program for the data,
154 information, and information technology resources of the state
155 agency which are held by a state agency be made confidential and



237354

156 exempt from s. 119.07(1), Florida Statutes, and s. 24(a),
157 Article I of the State Constitution if the disclosure of such
158 portions of records would facilitate unauthorized access to or
159 the unauthorized modification, disclosure, or destruction of:
160 1. Data or information, whether physical or virtual; or
161 2. Information technology resources, which includes:
162 a. Information relating to the security of the agency's
163 technologies, processes, and practices designed to protect
164 networks, computers, data processing software, and data from
165 attack, damage, or unauthorized access; or
166 b. Security information, whether physical or virtual, which
167 relates to the agency's existing or proposed information
168 technology systems.
169 (b) The Legislature finds that it may be valuable, prudent,
170 or critical to a state agency to have an independent entity
171 conduct a risk assessment, an audit, or an evaluation or
172 complete a report of the state agency's information technology
173 program or related systems. Such documents would likely include
174 an analysis of the state agency's current information technology
175 program or systems which could clearly identify vulnerabilities
176 or gaps in current systems or processes and propose
177 recommendations to remedy identified vulnerabilities. The
178 disclosure of such portions of records would jeopardize the
179 information technology security of the state agency, and
180 compromise the integrity and availability of agency data and
181 information technology resources, which would significantly
182 impair the administration of governmental programs. It is
183 necessary that such portions of records be made confidential and
184 exempt from public records requirements in order to protect



237354

185 agency technology systems, resources, and data. The Legislature
186 further finds that this public records exemption shall be given
187 retroactive application because it is remedial in nature.

188 Section 3. This act shall take effect upon becoming a law.
189

190 ===== T I T L E A M E N D M E N T =====

191 And the title is amended as follows:

192 Delete everything before the enacting clause
193 and insert:

194 A bill to be entitled
195 An act relating to public records; amending s.
196 282.318, F.S.; creating exemptions from public records
197 requirements for certain records held by a state
198 agency which identify detection, investigation, or
199 response practices for suspected or confirmed
200 information technology security incidents and for
201 certain portions of risk assessments, evaluations,
202 external audits, and other reports of a state agency's
203 information technology program; authorizing disclosure
204 of confidential and exempt information to certain
205 agencies and officers; providing for retroactive
206 application; providing for future legislative review
207 and repeal of the exemptions; providing statements of
208 public necessity; providing an effective date.