

By the Committees on Appropriations; and Military and Veterans Affairs, Space, and Domestic Security; and Senator Hutson

576-03524-22

20221694c2

1                   A bill to be entitled  
2       An act relating to public records and public meetings;  
3       creating s. 119.0725, F.S.; providing definitions;  
4       providing an exemption from public records  
5       requirements for certain cybersecurity insurance  
6       information, critical infrastructure information, and  
7       certain cybersecurity-related information held by an  
8       agency; providing an exemption from public meetings  
9       requirements for portions of a meeting that would  
10      reveal certain cybersecurity-related information held  
11      by an agency; requiring the recording and  
12      transcription of exempt portions of such meetings;  
13      providing an exemption from public records  
14      requirements for such recordings and transcripts;  
15      providing retroactive application; authorizing the  
16      disclosure of confidential and exempt information  
17      under certain circumstances; authorizing agencies to  
18      report certain cybersecurity information in the  
19      aggregate; providing for future legislative review and  
20      repeal of the exemptions; amending ss. 98.015 and  
21      282.318, F.S.; conforming provisions to changes made  
22      by the act; providing a statement of public necessity;  
23      providing a contingent effective date.

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

26  
27       Section 1. Section 119.0725, Florida Statutes, is created  
28 to read:

29       119.0725 Agency cybersecurity information; public records

576-03524-22

20221694c2

30 exemption; public meetings exemption.-

31 (1) As used in this section, the term:

32 (a) "Breach" means unauthorized access of data in  
33 electronic form containing personal information. Good faith  
34 access of personal information by an employee or agent of an  
35 agency does not constitute a breach, provided that the  
36 information is not used for a purpose unrelated to the business  
37 or subject to further unauthorized use.

38 (b) "Critical infrastructure" means existing and proposed  
39 information technology and operational technology systems and  
40 assets, whether physical or virtual, the incapacity or  
41 destruction of which would negatively affect security, economic  
42 security, public health, or public safety.

43 (c) "Cybersecurity" has the same meaning as in s. 282.0041.

44 (d) "Data" has the same meaning as in s. 282.0041.

45 (e) "Incident" means a violation or imminent threat of  
46 violation, whether such violation is accidental or deliberate,  
47 of information technology resources, security, policies, or  
48 practices. As used in this paragraph, the term "imminent threat  
49 of violation" means a situation in which the agency has a  
50 factual basis for believing that a specific incident is about to  
51 occur.

52 (f) "Information technology" has the same meaning as in s.  
53 282.0041.

54 (g) "Operational technology" means the hardware and  
55 software that cause or detect a change through the direct  
56 monitoring or control of physical devices, systems, processes,  
57 or events.

58 (2) The following information held by an agency is

576-03524-22

20221694c2

59 confidential and exempt from s. 119.07(1) and s. 24(a), Art. I  
60 of the State Constitution:

61 (a) Coverage limits and deductible or self-insurance  
62 amounts of insurance or other risk mitigation coverages acquired  
63 for the protection of information technology systems,  
64 operational technology systems, or data of an agency.

65 (b) Information relating to critical infrastructure.

66 (c) Network schematics, hardware and software  
67 configurations, or encryption information or information that  
68 identifies detection, investigation, or response practices for  
69 suspected or confirmed cybersecurity incidents, including  
70 suspected or confirmed breaches, if the disclosure of such  
71 information would facilitate unauthorized access to or  
72 unauthorized modification, disclosure, or destruction of:

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

74 2. Information technology resources, which include an  
75 agency's existing or proposed information technology systems.

76 (3) Any portion of a meeting that would reveal information  
77 made confidential and exempt under subsection (2) is exempt from  
78 s. 286.011 and s. 24(b), Art. I of the State Constitution. An  
79 exempt portion of a meeting may not be off the record and must  
80 be recorded and transcribed. The recording and transcript are  
81 confidential and exempt from s. 119.07(1) and s. 24(a), Art. I  
82 of the State Constitution.

83 (4) The public records exemptions contained in this section  
84 apply to information held by an agency before, on, or after July  
85 1, 2022.

86 (5) (a) Information made confidential and exempt pursuant to  
87 this section shall be made available to a law enforcement

576-03524-22

20221694c2

88 agency, the Auditor General, the Cybercrime Office of the  
89 Department of Law Enforcement, the Florida Digital Service  
90 within the Department of Management Services, and, for agencies  
91 under the jurisdiction of the Governor, the Chief Inspector  
92 General.

93 (b) Such confidential and exempt information may be  
94 disclosed by an agency in the furtherance of its official duties  
95 and responsibilities or to another agency or governmental entity  
96 in the furtherance of its statutory duties and responsibilities.

97 (6) Agencies may report information about cybersecurity  
98 incidents in the aggregate.

99 (7) This section is subject to the Open Government Sunset  
100 Review Act in accordance with s. 119.15 and shall stand repealed  
101 on October 2, 2027, unless reviewed and saved from repeal  
102 through reenactment by the Legislature.

103 Section 2. Subsection (13) of section 98.015, Florida  
104 Statutes, is amended to read:

105 98.015 Supervisor of elections; election, tenure of office,  
106 compensation, custody of registration-related documents, office  
107 hours, successor, seal; appointment of deputy supervisors;  
108 duties; ~~public records exemption.~~-

109 ~~(13)(a) Portions of records held by a supervisor of~~  
110 ~~elections which contain network schematics, hardware and~~  
111 ~~software configurations, or encryption, or which identify~~  
112 ~~detection, investigation, or response practices for suspected or~~  
113 ~~confirmed information technology security incidents, including~~  
114 ~~suspected or confirmed breaches, are confidential and exempt~~  
115 ~~from s. 119.07(1) and s. 24(a), Art. I of the State~~  
116 ~~Constitution, if the disclosure of such records would facilitate~~

576-03524-22

20221694c2

117 ~~unauthorized access to or the unauthorized modification,~~  
118 ~~disclosure, or destruction of:~~

119 ~~1. Data or information, whether physical or virtual; or~~

120 ~~2. Information technology resources as defined in s.~~

121 ~~119.011(9), which includes:~~

122 ~~a. Information relating to the security of a supervisor of~~  
123 ~~elections' technology, processes, and practices designed to~~  
124 ~~protect networks, computers, data processing software, and data~~  
125 ~~from attack, damage, or unauthorized access; or~~

126 ~~b. Security information, whether physical or virtual, which~~  
127 ~~relates to a supervisor of elections' existing or proposed~~  
128 ~~information technology systems.~~

129 ~~(b) The portions of records made confidential and exempt in~~  
130 ~~paragraph (a) shall be available to the Auditor General and may~~  
131 ~~be made available to another governmental entity for information~~  
132 ~~technology security purposes or in the furtherance of the~~  
133 ~~entity's official duties.~~

134 ~~(c) The public record exemption in paragraph (a) applies to~~  
135 ~~records held by a supervisor of elections before, on, or after~~  
136 ~~the effective date of the exemption.~~

137 ~~(d) This subsection is subject to the Open Government~~  
138 ~~Sunset Review Act in accordance with s. 119.15 and shall stand~~  
139 ~~repealed on October 2, 2026, unless reviewed and saved from~~  
140 ~~repeal through reenactment by the Legislature.~~

141 Section 3. Subsections (6) and (11) of section 282.318,  
142 Florida Statutes, are renumbered as subsections (5) and (10),  
143 respectively, and present subsections (5), (7), (8), (9), and  
144 (10) of that section are amended to read:

145 282.318 Cybersecurity.—

576-03524-22

20221694c2

146 ~~(5) Portions of records held by a state agency which~~  
147 ~~contain network schematics, hardware and software~~  
148 ~~configurations, or encryption, or which identify detection,~~  
149 ~~investigation, or response practices for suspected or confirmed~~  
150 ~~cybersecurity incidents, including suspected or confirmed~~  
151 ~~breaches, are confidential and exempt from s. 119.07(1) and s.~~  
152 ~~24(a), Art. I of the State Constitution, if the disclosure of~~  
153 ~~such records would facilitate unauthorized access to or the~~  
154 ~~unauthorized modification, disclosure, or destruction of:~~

155 ~~(a) Data or information, whether physical or virtual; or~~

156 ~~(b) Information technology resources, which includes:~~

157 ~~1. Information relating to the security of the agency's~~  
158 ~~technologies, processes, and practices designed to protect~~  
159 ~~networks, computers, data processing software, and data from~~  
160 ~~attack, damage, or unauthorized access; or~~

161 ~~2. Security information, whether physical or virtual, which~~  
162 ~~relates to the agency's existing or proposed information~~  
163 ~~technology systems.~~

164 ~~(6)~~(7) Those portions of a public meeting as specified in  
165 s. 286.011 which would reveal records which are confidential and  
166 exempt under subsection (5) ~~or subsection (6)~~ are exempt from s.  
167 286.011 and s. 24(b), Art. I of the State Constitution. No  
168 exempt portion of an exempt meeting may be off the record. All  
169 exempt portions of such meeting shall be recorded and  
170 transcribed. Such recordings and transcripts are confidential  
171 and exempt from disclosure under s. 119.07(1) and s. 24(a), Art.  
172 I of the State Constitution unless a court of competent  
173 jurisdiction, after an in camera review, determines that the  
174 meeting was not restricted to the discussion of data and

576-03524-22

20221694c2

175 information made confidential and exempt by this section. In the  
176 event of such a judicial determination, only that portion of the  
177 recording and transcript which reveals nonexempt data and  
178 information may be disclosed to a third party.

179 ~~(7)~~~~(8)~~ The portions of records made confidential and exempt  
180 in subsections (5) and~~(6)~~~~and~~~~(7)~~ shall be available to the  
181 Auditor General, the Cybercrime Office of the Department of Law  
182 Enforcement, the Florida Digital Service within the department,  
183 and, for agencies under the jurisdiction of the Governor, the  
184 Chief Inspector General. Such portions of records may be made  
185 available to a local government, another state agency, or a  
186 federal agency for cybersecurity purposes or in furtherance of  
187 the state agency's official duties.

188 ~~(8)~~~~(9)~~ The exemptions contained in subsections (5) and~~(6)~~~~and~~~~(7)~~  
189 ~~(6)~~~~and~~~~(7)~~ apply to records held by a state agency before, on,  
190 or after the effective date of this exemption.

191 ~~(9)~~~~(10)~~ Subsections (5) and~~(6)~~~~and~~~~(7)~~ are subject to  
192 the Open Government Sunset Review Act in accordance with s.  
193 119.15 and shall stand repealed on October 2, 2025, unless  
194 reviewed and saved from repeal through reenactment by the  
195 Legislature.

196 Section 4. (1) The Legislature finds that it is a public  
197 necessity that the following information held by an agency be  
198 made confidential and exempt from s. 119.07(1), Florida  
199 Statutes, and s. 24(a), Article I of the State Constitution:

200 (a) Coverage limits and deductible or self-insurance  
201 amounts of insurance or other risk mitigation coverages acquired  
202 for the protection of information technology systems,  
203 operational technology systems, or data of an agency.

576-03524-22

20221694c2

204       (b) Information relating to critical infrastructure.  
205       (c) Network schematics, hardware and software  
206 configurations, or encryption information or information that  
207 identifies detection, investigation, or response practices for  
208 suspected or confirmed cybersecurity incidents, including  
209 suspected or confirmed breaches, if the disclosure of such  
210 information would facilitate unauthorized access to or  
211 unauthorized modification, disclosure, or destruction of:  
212       1. Data or information, whether physical or virtual; or  
213       2. Information technology resources, which include an  
214 agency's existing or proposed information technology systems.  
215  
216 Release of such information could place an agency at greater  
217 risk of breaches, cybersecurity incidents, and ransomware  
218 attacks. Such information could be used by criminals to identify  
219 any vulnerabilities that may exist in an agency's security  
220 system, thereby compromising the integrity of the agency's  
221 information technology, operational technology, and data. If  
222 information related to the coverage limits and deductible or  
223 self-insurance amounts of cybersecurity insurance were  
224 disclosed, it could give cybercriminals an understanding of the  
225 monetary sum an agency can afford or may be willing to pay as a  
226 result of a ransomware attack at the expense of the taxpayer. In  
227 addition, critical infrastructure information is a vital  
228 component of public safety and, if made publicly available,  
229 could aid in the planning of, training for, and execution of  
230 cyberattacks, thereby increasing the ability of persons to harm  
231 individuals in this state. The recent cybersecurity hacking and  
232 shutdown of the Colonial Pipeline by the criminal enterprise



576-03524-22

20221694c2

233 DarkSide in 2021 and the infiltration of the Bowman Avenue Dam  
234 in Rye Brook, New York, by Iranian hackers in 2013 provide  
235 evidence that such criminal capabilities exist. These events  
236 also show the crippling effect that cyberattacks on critical  
237 infrastructure may have. Further, the release of network  
238 schematics, hardware and software configurations, or encryption  
239 information or information that identifies detection,  
240 investigation, or response practices for suspected or confirmed  
241 cybersecurity incidents, including suspected or confirmed  
242 breaches, would facilitate unauthorized access to or the  
243 unauthorized modification, disclosure, or destruction of data or  
244 information, whether physical or virtual, or information  
245 technology resources. Such information also includes proprietary  
246 information about the security of an agency's system. The  
247 disclosure of such information could compromise the integrity of  
248 an agency's data, information, or information technology  
249 resources, which would significantly impair the administration  
250 of vital governmental programs. Therefore, this information  
251 should be made confidential and exempt in order to protect the  
252 agency's data, information, and information technology  
253 resources.

254 (2) The Legislature also finds that it is a public  
255 necessity that any portion of a meeting that would reveal the  
256 confidential and exempt information be made exempt from s.  
257 286.011, Florida Statutes, and s. 24(b), Article I of the State  
258 Constitution, and that any recordings and transcripts of the  
259 closed portion of a meeting be made confidential and exempt from  
260 s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the  
261 State Constitution. The failure to close that portion of a

576-03524-22

20221694c2

262 meeting at which confidential and exempt information would be  
263 revealed, and prevent the disclosure of the recordings and  
264 transcripts of those portions of a meeting, would defeat the  
265 purpose of the underlying public records exemption and could  
266 result in the release of highly sensitive information related to  
267 the cybersecurity of an agency system.

268 (3) For these reasons, the Legislature finds that these  
269 public records and public meetings exemptions are of the utmost  
270 importance and are a public necessity.

271 Section 5. This act shall take effect on the same date that  
272 SB 1670 or similar legislation takes effect, if such legislation  
273 is adopted in the same legislative session or an extension  
274 thereof and becomes law.