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:
	Page 1 of 11

Page 1 of 11

CODING: Words stricken are deletions; words underlined are additions.

26	
27	Section 1. Section 119.0725, Florida Statutes, is created
28	to read:
29	119.0725 Agency cybersecurity information; public records
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.
44	282.0041.
45	(d) "Data" has the same meaning as in s. 282.0041.
46	(e) "Incident" means a violation or imminent threat of
47	violation, whether such violation is accidental or deliberate,
48	of information technology resources, security, policies, or
49	practices. As used in this paragraph, the term "imminent threat
50	of violation" means a situation in which the agency has a

Page 2 of 11

CODING: Words stricken are deletions; words underlined are additions.

51	factual basis for believing that a specific incident is about to
52	occur.
53	(f) "Information technology" has the same meaning as in s.
54	282.0041.
55	(g) "Operational technology" means the hardware and
56	software that cause or detect a change through the direct
57	monitoring or control of physical devices, systems, processes,
58	<u>or events.</u>
59	(2) The following information held by an agency is
60	confidential and exempt from s. 119.07(1) and s. 24(a), Art. I
61	of the State Constitution:
62	(a) Coverage limits and deductible or self-insurance
63	amounts of insurance or other risk mitigation coverages acquired
64	for the protection of information technology systems,
65	operational technology systems, or data of an agency.
66	(b) Information relating to critical infrastructure.
67	(c) Network schematics, hardware and software
68	configurations, or encryption information or information that
69	identifies detection, investigation, or response practices for
70	suspected or confirmed cybersecurity incidents, including
71	suspected or confirmed breaches, if the disclosure of such
72	information would facilitate unauthorized access to or
73	unauthorized modification, disclosure, or destruction of:
74	1. Data or information, whether physical or virtual; or
75	2. Information technology resources, which include an
	Page 3 of 11

CODING: Words stricken are deletions; words underlined are additions.

2022

76	agency's existing or proposed information technology systems.
77	(3) Any portion of a meeting that would reveal information
78	made confidential and exempt under subsection (2) is exempt from
79	s. 286.011 and s. 24(b), Art. I of the State Constitution. An
80	exempt portion of a meeting may not be off the record and must
81	be recorded and transcribed. The recording and transcript are
82	confidential and exempt from s. 119.07(1) and s. 24(a), Art. I
83	of the State Constitution.
84	(4) The public records exemptions contained in this
85	section apply to information held by an agency before, on, or
86	after July 1, 2022.
87	(5)(a) Information made confidential and exempt pursuant
88	to this section shall be made available to a law enforcement
89	agency, the Auditor General, the Cybercrime Office of the
90	Department of Law Enforcement, the Florida Digital Service
91	within the Department of Management Services, and, for agencies
92	under the jurisdiction of the Governor, the Chief Inspector
93	General.
94	(b) Such confidential and exempt information may be
95	disclosed by an agency in the furtherance of its official duties
96	and responsibilities or to another agency or governmental entity
97	in the furtherance of its statutory duties and responsibilities.
98	(6) Agencies may report information about cybersecurity
99	incidents in the aggregate.
100	(7) This section is subject to the Open Government Sunset
ļ	Page 4 of 11

CODING: Words stricken are deletions; words underlined are additions.

101 Review Act in accordance with s. 119.15 and shall stand repealed 102 on October 2, 2027, unless reviewed and saved from repeal 103 through reenactment by the Legislature. 104 Section 2. Subsection (13) of section 98.015, Florida 105 Statutes, is amended to read: 106 98.015 Supervisor of elections; election, tenure of 107 office, compensation, custody of registration-related documents, office hours, successor, seal; appointment of deputy 108 109 supervisors; duties; public records exemption.-(13) (a) Portions of records held by a supervisor of 110 111 elections which contain network schematics, hardware and 112 software configurations, or encryption, or which identify 113 detection, investigation, or response practices for suspected or 114 confirmed information technology security incidents, including 115 suspected or confirmed breaches, are confidential and exempt 116 from s. 119.07(1) and s. 24(a), Art. I of the State 117 Constitution, if the disclosure of such records would facilitate 118 unauthorized access to or the unauthorized modification, 119 disclosure, or destruction of: 120 1. Data or information, whether physical or virtual; or 2. Information technology resources as defined in s. 121 119.011(9), which includes: 122 123 a. Information relating to the security of a supervisor of 124 elections' technology, processes, and practices designed to 125 protect networks, computers, data processing software, and data

Page 5 of 11

CODING: Words stricken are deletions; words underlined are additions.

126	from attack, damage, or unauthorized access; or
127	b. Security information, whether physical or virtual,
128	which relates to a supervisor of elections' existing or proposed
129	information technology systems.
130	(b) The portions of records made confidential and exempt
131	in paragraph (a) shall be available to the Auditor General and
132	may be made available to another governmental entity for
133	information technology security purposes or in the furtherance
134	of the entity's official duties.
135	(c) The public record exemption in paragraph (a) applies
136	to records held by a supervisor of elections before, on, or
137	after the effective date of the exemption.
138	(d) This subsection is subject to the Open Government
139	Sunset Review Act in accordance with s. 119.15 and shall stand
140	repealed on October 2, 2026, unless reviewed and saved from
141	repeal through reenactment by the Legislature.
142	Section 3. Subsections (6) and (11) of section 282.318,
143	Florida Statutes, are renumbered as subsections (5) and (10),
144	respectively, and present subsections (5), (7), (8), (9), and
145	(10) of that section are amended to read:
146	282.318 Cybersecurity
147	(5) Portions of records held by a state agency which
148	contain network schematics, hardware and software
149	configurations, or encryption, or which identify detection,
150	investigation, or response practices for suspected or confirmed
	Page 6 of 11

CODING: Words stricken are deletions; words underlined are additions.

151	cybersecurity incidents, including suspected or confirmed
152	breaches, are confidential and exempt from s. 119.07(1) and s.
153	24(a), Art. I of the State Constitution, if the disclosure of
154	such records would facilitate unauthorized access to or the
155	unauthorized modification, disclosure, or destruction of:
156	(a) Data or information, whether physical or virtual; or
157	(b) Information technology resources, which includes:
158	1. Information relating to the security of the agency's
159	technologies, processes, and practices designed to protect
160	networks, computers, data processing software, and data from
161	attack, damage, or unauthorized access; or
162	2. Security information, whether physical or virtual,
163	which relates to the agency's existing or proposed information
164	technology systems.
165	<u>(6)</u> Those portions of a public meeting as specified in
166	s. 286.011 which would reveal records which are confidential and
167	exempt under subsection (5) $\frac{1}{2}$ or subsection (6) are exempt from s.
168	286.011 and s. 24(b), Art. I of the State Constitution. No
169	exempt portion of an exempt meeting may be off the record. All
170	exempt portions of such meeting shall be recorded and
171	transcribed. Such recordings and transcripts are confidential
172	and exempt from disclosure under s. 119.07(1) and s. 24(a), Art.
173	I of the State Constitution unless a court of competent
174	jurisdiction, after an in camera review, determines that the
175	meeting was not restricted to the discussion of data and
	Dave 7 (44
	Page 7 of 11

CODING: Words stricken are deletions; words underlined are additions.

176 information made confidential and exempt by this section. In the 177 event of such a judicial determination, only that portion of the 178 recording and transcript which reveals nonexempt data and 179 information may be disclosed to a third party.

180 (7) (8) The portions of records made confidential and exempt in subsections (5) and $_{r}$ (6) $_{r}$ and (7) shall be available 181 182 to the Auditor General, the Cybercrime Office of the Department 183 of Law Enforcement, the Florida Digital Service within the 184 department, and, for agencies under the jurisdiction of the 185 Governor, the Chief Inspector General. Such portions of records may be made available to a local government, another state 186 agency, or a federal agency for cybersecurity purposes or in 187 furtherance of the state agency's official duties. 188

189 <u>(8)(9)</u> The exemptions contained in subsections (5) and, 190 (6), and (7) apply to records held by a state agency before, on, 191 or after the effective date of this exemption.

192 (9)(10) Subsections (5) and, (6), and (7) are subject to 193 the Open Government Sunset Review Act in accordance with s. 194 119.15 and shall stand repealed on October 2, 2025, unless 195 reviewed and saved from repeal through reenactment by the 196 Legislature.

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

Page 8 of 11

CODING: Words stricken are deletions; words underlined are additions.

201 (a) Coverage limits and deductible or self-insurance 202 amounts of insurance or other risk mitigation coverages acquired 203 for the protection of information technology systems, 204 operational technology systems, or data of an agency. 205 Information relating to critical infrastructure. (b) (c) Network schematics, hardware and software 206 207 configurations, or encryption information or information that identifies detection, investigation, or response practices for 208 209 suspected or confirmed cybersecurity incidents, including 210 suspected or confirmed breaches, if the disclosure of such 211 information would facilitate unauthorized access to or 212 unauthorized modification, disclosure, or destruction of: 213 1. Data or information, whether physical or virtual; or 214 2. Information technology resources, which include an 215 agency's existing or proposed information technology systems. 216 217 Release of such information could place an agency at greater 218 risk of breaches, cybersecurity incidents, and ransomware 219 attacks. Such information could be used by criminals to identify 220 any vulnerabilities that may exist in an agency's security 221 system, thereby compromising the integrity of the agency's information technology, operational technology, and data. If 222 223 information related to the coverage limits and deductible or 224 self-insurance amounts of cybersecurity insurance were 225 disclosed, it could give cybercriminals an understanding of the

Page 9 of 11

CODING: Words stricken are deletions; words underlined are additions.

2022

226	monetary sum an agency can afford or may be willing to pay as a
227	result of a ransomware attack at the expense of the taxpayer. In
228	addition, critical infrastructure information is a vital
229	component of public safety and, if made publicly available,
230	could aid in the planning of, training for, and execution of
231	cyberattacks, thereby increasing the ability of persons to harm
232	individuals in this state. The recent cybersecurity hacking and
233	shutdown of the Colonial Pipeline by the criminal enterprise
234	DarkSide in 2021 and the infiltration of the Bowman Avenue Dam
235	in Rye Brook, New York, by Iranian hackers in 2013 provide
236	evidence that such criminal capabilities exist. These events
237	also show the crippling effect that cyberattacks on critical
238	infrastructure may have. Further, the release of network
239	schematics, hardware and software configurations, or encryption
240	information or information that identifies detection,
241	investigation, or response practices for suspected or confirmed
242	cybersecurity incidents, including suspected or confirmed
243	breaches, would facilitate unauthorized access to or the
244	unauthorized modification, disclosure, or destruction of data or
245	information, whether physical or virtual, or information
246	technology resources. Such information also includes proprietary
247	information about the security of an agency's system. The
248	disclosure of such information could compromise the integrity of
249	an agency's data, information, or information technology
250	resources, which would significantly impair the administration
	Dego 10 of 11

Page 10 of 11

CODING: Words stricken are deletions; words underlined are additions.

2022

2.51 of vital governmental programs. Therefore, this information 252 should be made confidential and exempt in order to protect the 253 agency's data, information, and information technology 254 resources. 255 (2) The Legislature also finds that it is a public 256 necessity that any portion of a meeting that would reveal the confidential and exempt information be made exempt from s. 257 258 286.011, Florida Statutes, and s. 24(b), Article I of the State 259 Constitution, and that any recordings and transcripts of the 260 closed portion of a meeting be made confidential and exempt from 261 s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the 262 State Constitution. The failure to close that portion of a 263 meeting at which confidential and exempt information would be 264 revealed, and prevent the disclosure of the recordings and 265 transcripts of those portions of a meeting, would defeat the 266 purpose of the underlying public records exemption and could 267 result in the release of highly sensitive information related to 268 the cybersecurity of an agency system. 269 (3) For these reasons, the Legislature finds that these 270 public records and public meetings exemptions are of the utmost importance and are a public necessity. 271 272 Section 5. This act shall take effect on the same date 273 that HB 7055 or similar legislation takes effect, if such 274 legislation is adopted in the same legislative session or an 275 extension thereof and becomes law.

Page 11 of 11

CODING: Words stricken are deletions; words underlined are additions.