

1 A bill to be entitled

2 An act relating to public records and public meetings;
3 creating s. 1004.055, F.S.; creating an exemption from
4 public records requirements for certain records held
5 by a state university or Florida College System
6 institution which identify detection, investigation,
7 or response practices for suspected or confirmed
8 information technology security incidents; creating an
9 exemption from public records requirements for certain
10 portions of risk assessments, evaluations, audits, and
11 other reports of a university's or institution's
12 information technology security program; creating an
13 exemption from public meetings requirements for
14 portions of public meetings which would reveal such
15 data and information; providing an exemption from
16 public records requirements for a specified period for
17 the recording and transcript of a closed meeting;
18 authorizing disclosure of confidential and exempt
19 information to certain agencies and officers;
20 providing retroactive application; providing for
21 future legislative review and repeal of the
22 exemptions; providing statements of public necessity;
23 providing a directive to the Division of Law Revision
24 and Information; providing an effective date.

25

26 | Be It Enacted by the Legislature of the State of Florida:

27 |
 28 | Section 1. Section 1004.055, Florida Statutes, is created
 29 | to read:

30 | 1004.055 Security of data and information technology in
 31 | state postsecondary education institutions.-

32 | (1) All of the following data or information from
 33 | technology systems owned, under contract, or maintained by a
 34 | state university or a Florida College System institution are
 35 | confidential and exempt from s. 119.07(1) and s. 24(a), Art. I
 36 | of the State Constitution:

37 | (a) Records held by the university or institution which
 38 | identify detection, investigation, or response practices for
 39 | suspected or confirmed information technology security
 40 | incidents, including suspected or confirmed breaches, if the
 41 | disclosure of such records would facilitate unauthorized access
 42 | to or unauthorized modification, disclosure, or destruction of:

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

44 | 2. Information technology resources, which include:

45 | a. Information relating to the security of the
 46 | university's or institution's technologies, processes, and
 47 | practices designed to protect networks, computers, data
 48 | processing software, and data from attack, damage, or
 49 | unauthorized access; or

50 | b. Security information, whether physical or virtual,

51 which relates to the university's or institution's existing or
52 proposed information technology systems.

53 (b) Those portions of risk assessments, evaluations,
54 audits, and other reports of the university's or institution's
55 information technology security program for its data,
56 information, and information technology resources which are held
57 by the university or institution, if the disclosure of such
58 records would facilitate unauthorized access to or the
59 unauthorized modification, disclosure, or destruction of:

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

61 2. Information technology resources, which include:

62 a. Information relating to the security of the
63 university's or institution's technologies, processes, and
64 practices designed to protect networks, computers, data
65 processing software, and data from attack, damage, or
66 unauthorized access; or

67 b. Security information, whether physical or virtual,
68 which relates to the university's or institution's existing or
69 proposed information technology systems.

70 (2) Those portions of a public meeting as specified in s.
71 286.011 which would reveal data and information described in
72 subsection (1) are exempt from s. 286.011 and s. 24(b), Art. I
73 of the State Constitution. No exempt portion of an exempt
74 meeting may be off the record. All exempt portions of such a
75 meeting must be recorded and transcribed. The recording and

76 transcript of the meeting must remain confidential and exempt
77 from disclosure under s. 119.07(1) and s. 24(a), Art. 1 of the
78 State Constitution unless a court of competent jurisdiction,
79 following an in camera review, determines that the meeting was
80 not restricted to the discussion of data and information made
81 confidential and exempt by this section. In the event of such a
82 judicial determination, only that portion of the transcript
83 which reveals nonexempt data and information may be disclosed to
84 a third party.

85 (3) The records and portions of public meeting recordings
86 and transcripts described in subsection (1) must be available to
87 the Auditor General; the Cybercrime Office of the Department of
88 Law Enforcement; for a state university, the Board of Governors;
89 and for a Florida College System institution, the State Board of
90 Education. Such records and portions of meetings, recordings,
91 and transcripts may be made available to a state or federal
92 agency for security purposes or in furtherance of the agency's
93 official duties.

94 (4) The exemptions listed in this section apply to such
95 records or portions of public meetings, recordings, and
96 transcripts held by the university or institution before, on, or
97 after the effective date of this act.

98 (5) This section is subject to the Open Government Sunset
99 Review Act in accordance with s. 119.15 and shall stand repealed

100 on October 2, 2022, unless reviewed and saved from repeal
 101 through reenactment by the Legislature.

102 Section 2. (1) (a) The Legislature finds that it is a
 103 public necessity that the following data or information from
 104 technology systems owned, under contract, or maintained by a
 105 state university or a Florida College System institution be
 106 confidential and exempt from s. 119.07(1), Florida Statutes, and
 107 s. 24(a), Article I of the State Constitution:

108 1. Records held by the university or institution which
 109 identify detection, investigation, or response practices for
 110 suspected or confirmed information technology security
 111 incidents, including suspected or confirmed breaches, if the
 112 disclosure of such records would facilitate unauthorized access
 113 to or unauthorized modification, disclosure, or destruction of:

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

115 b. Information technology resources, which include:

116 (I) Information relating to the security of the
 117 university's or institution's technologies, processes, and
 118 practices designed to protect networks, computers, data
 119 processing software, and data from attack, damage, or
 120 unauthorized access; or

121 (II) Security information, whether physical or virtual,
 122 which relates to the university's or institution's existing or
 123 proposed information technology systems.

124 2. Those portions of risk assessments, evaluations,

125 audits, and other reports of the university's or institution's
126 information technology security program for its data,
127 information, and information technology resources which are held
128 by the university or institution, if the disclosure of such
129 records would facilitate unauthorized access to or the
130 unauthorized modification, disclosure, or destruction of:

131 a. Data or information, whether physical or virtual; or
132 b. Information technology resources, which include:

133 (I) Information relating to the security of the
134 university's or institution's technologies, processes, and
135 practices designed to protect networks, computers, data
136 processing software, and data from attack, damage, or
137 unauthorized access; or

138 (II) Security information, whether physical or virtual,
139 which relates to the university's or institution's existing or
140 proposed information technology systems.

141 (b) The Legislature also finds that those portions of a
142 public meeting as specified in s. 286.011, Florida Statutes,
143 which would reveal data and information described in subsection
144 (1) are exempt from s. 286.011, Florida Statutes, and s. 24(b),
145 Article I of the State Constitution. The recording and
146 transcript of the meeting must remain confidential and exempt
147 from disclosure under s. 119.07(1), Florida Statutes, and s.
148 24(a), Article 1 of the State Constitution unless a court of
149 competent jurisdiction, following an in camera review,

150 determines that the meeting was not restricted to the discussion
151 of data and information made confidential and exempt by this
152 section. In the event of such a judicial determination, only
153 that portion of the transcript which reveals nonexempt data and
154 information may be disclosed to a third party.

155 (c) The Legislature further finds that it is a public
156 necessity that records held by a state university or Florida
157 College System institution which identify detection,
158 investigation, or response practices for suspected or confirmed
159 information technology security incidents, including suspected
160 or confirmed breaches, be made confidential and exempt from s.
161 119.07(1), Florida Statutes, and s. 24(a), Article I of the
162 State Constitution if the disclosure of such records would
163 facilitate unauthorized access to or the unauthorized
164 modification, disclosure, or destruction of:

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

166 2. Information technology resources, which include:

167 a. Information relating to the security of the
168 university's or institution's technologies, processes, and
169 practices designed to protect networks, computers, data
170 processing software, and data from attack, damage, or
171 unauthorized access; or

172 b. Security information, whether physical or virtual,
173 which relates to the university's or institution's existing or
174 proposed information technology systems.

175 (d) Such records must be made confidential and exempt for
176 the following reasons:

177 1. Records held by a state university or Florida College
178 System institution which identify information technology
179 detection, investigation, or response practices for suspected or
180 confirmed information technology security incidents or breaches
181 are likely to be used in the investigations of the incidents or
182 breaches. The release of such information could impede the
183 investigation and impair the ability of reviewing entities to
184 effectively and efficiently execute their investigative duties.
185 In addition, the release of such information before an active
186 investigation is completed could jeopardize the ongoing
187 investigation.

188 2. An investigation of an information technology security
189 incident or breach is likely to result in the gathering of
190 sensitive personal information, including identification
191 numbers, personal financial and health information, and
192 educational records exempt from disclosure under the Family
193 Educational Rights and Privacy Act, 20 U.S.C. s. 1232g, and ss.
194 1002.225 and 1006.52, Florida Statutes. Such information could
195 be used to commit identity theft or other crimes. In addition,
196 release of such information could subject possible victims of
197 the security incident or breach to further harm.

198 3. Disclosure of a record, including a computer forensic
199 analysis, or other information that would reveal weaknesses in a

200 state university's or Florida College System institution's data
201 security could compromise that security in the future if such
202 information were available upon conclusion of an investigation
203 or once an investigation ceased to be active.

204 4. Such records are likely to contain proprietary
205 information about the security of the system at issue. The
206 disclosure of such information could result in the
207 identification of vulnerabilities and further breaches of that
208 system. In addition, the release of such information could give
209 business competitors an unfair advantage and weaken the security
210 technology supplier supplying the proprietary information in the
211 marketplace.

212 5. The disclosure of such records could potentially
213 compromise the confidentiality, integrity, and availability of
214 state university and Florida College System institution data and
215 information technology resources, which would significantly
216 impair the administration of vital educational programs. It is
217 necessary that this information be made confidential in order to
218 protect the technology systems, resources, and data of the
219 universities and institutions. The Legislature further finds
220 that this public records exemption be given retroactive
221 application because it is remedial in nature.

222 (2) (a) The Legislature also finds that it is a public
223 necessity that portions of risk assessments, evaluations,
224 audits, and other reports of a state university's or Florida

225 College System institution's information technology security
226 program for its data, information, and information technology
227 resources which are held by the university or institution be
228 made confidential and exempt from s. 119.07(1), Florida
229 Statutes, and s. 24(a), Article I of the State Constitution if
230 the disclosure of such portions of records would facilitate
231 unauthorized access to or the unauthorized modification,
232 disclosure, or destruction of:

233 1. Data or information, whether physical or virtual; or
234 2. Information technology resources, which include:

235 a. Information relating to the security of the
236 university's or institution's technologies, processes, and
237 practices designed to protect networks, computers, data
238 processing software, and data from attack, damage, or
239 unauthorized access; or

240 b. Security information, whether physical or virtual,
241 which relates to the university's or institution's existing or
242 proposed information technology systems.

243 (b) The Legislature finds that it is valuable, prudent,
244 and critical to a state university or Florida College System
245 institution to have an independent entity conduct a risk
246 assessment, an audit, or an evaluation or complete a report of
247 the university's or institution's information technology program
248 or related systems. Such documents would likely include an
249 analysis of the university's or institution's current

250 information technology program or systems which could clearly
251 identify vulnerabilities or gaps in current systems or processes
252 and propose recommendations to remedy identified
253 vulnerabilities.

254 (3) (a) The Legislature further finds that it is a public
255 necessity that those portions of a public meeting which could
256 reveal information described in subsections (1) and (2) be made
257 exempt from s. 286.011, Florida Statutes, and s. 24(b), Article
258 I of the State Constitution. It is necessary that such meetings
259 be made exempt from the open meetings requirements in order to
260 protect institutional information technology systems, resources,
261 and data. The information disclosed during portions of meetings
262 would clearly identify a state university's or Florida College
263 System institution's information technology systems and its
264 vulnerabilities. This disclosure would jeopardize the
265 information technology security of the institution and
266 compromise the integrity and availability of state university or
267 Florida College System institution data and information
268 technology resources, which would significantly impair the
269 administration of educational programs.

270 (b) The Legislature further finds that it is a public
271 necessity that the recording and transcript of those portions of
272 meetings specified in paragraph (a) be made confidential and
273 exempt from s. 119.07(1), Florida Statutes, and s. 24(a),
274 Article I of the State Constitution unless a court determines

275 that the meeting was not restricted to the discussion of data
276 and information made confidential and exempt by this act. It is
277 necessary that the resulting recordings and transcripts be made
278 confidential and exempt from the public record requirements in
279 order to protect institutional information technology systems,
280 resources, and data. The disclosure of such recordings and
281 transcripts would clearly identify a state university's or
282 Florida College System institution's information technology
283 systems and its vulnerabilities. This disclosure would
284 jeopardize the information technology security of the
285 institution and compromise the integrity and availability of
286 state university or Florida College System institution data and
287 information technology resources, which would significantly
288 impair the administration of educational programs.

289 (c) The Legislature further finds that this public meeting
290 and public records exemption must be given retroactive
291 application because it is remedial in nature.

292 Section 3. The Division of Law Revision and Information is
293 directed to replace the phrase "the effective date of this act"
294 wherever it occurs in this act with the date this act becomes a
295 law.

296 Section 4. This act shall take effect upon becoming a law.