

1 A bill to be entitled

2 An act relating to public records and meetings;
3 amending s. 282.318, F.S.; revising a provision to
4 reflect the abolishment of the Agency for State
5 Technology; providing an exemption from public records
6 requirements for portions of records held by a state
7 agency that contain network schematics, hardware and
8 software configurations, and encryption; providing an
9 exemption from public meetings requirements for
10 portions of meetings that would reveal such records;
11 requiring recording and transcription of exempt
12 portions of such meetings; providing an exemption from
13 public records requirements for such recordings and
14 transcripts; providing for future legislative review
15 and repeal of the exemptions under the Open Government
16 Sunset Review Act; providing for retroactive
17 application of the exemptions; providing a public
18 necessity statement; providing an effective date.

19
20 Be It Enacted by the Legislature of the State of Florida:

21
22 Section 1. Section 282.318, Florida Statutes, is amended
23 to read:

24 282.318 Security of data and information technology.—

25 (1) This section may be cited as the "Information

26 | Technology Security Act."

27 | (2) As used in this section, the term "state agency" has
28 | the same meaning as provided in s. 282.0041, except that the
29 | term includes the Department of Legal Affairs, the Department of
30 | Agriculture and Consumer Services, and the Department of
31 | Financial Services.

32 | (3) The department is responsible for establishing
33 | standards and processes consistent with generally accepted best
34 | practices for information technology security, to include
35 | cybersecurity, and adopting rules that safeguard an agency's
36 | data, information, and information technology resources to
37 | ensure availability, confidentiality, and integrity and to
38 | mitigate risks. The department shall also:

39 | (a) Designate a state chief information security officer
40 | who must have experience and expertise in security and risk
41 | management for communications and information technology
42 | resources.

43 | (b) Develop, and annually update by February 1, a
44 | statewide information technology security strategic plan that
45 | includes security goals and objectives for the strategic issues
46 | of information technology security policy, risk management,
47 | training, incident management, and disaster recovery planning.

48 | (c) Develop and publish for use by state agencies an
49 | information technology security framework that, at a minimum,
50 | includes guidelines and processes for:

51 1. Establishing asset management procedures to ensure that
52 an agency's information technology resources are identified and
53 managed consistent with their relative importance to the
54 agency's business objectives.

55 2. Using a standard risk assessment methodology that
56 includes the identification of an agency's priorities,
57 constraints, risk tolerances, and assumptions necessary to
58 support operational risk decisions.

59 3. Completing comprehensive risk assessments and
60 information technology security audits, which may be completed
61 by a private sector vendor, and submitting completed assessments
62 and audits to the department.

63 4. Identifying protection procedures to manage the
64 protection of an agency's information, data, and information
65 technology resources.

66 5. Establishing procedures for accessing information and
67 data to ensure the confidentiality, integrity, and availability
68 of such information and data.

69 6. Detecting threats through proactive monitoring of
70 events, continuous security monitoring, and defined detection
71 processes.

72 7. Establishing agency computer security incident response
73 teams and describing their responsibilities for responding to
74 information technology security incidents, including breaches of
75 personal information containing confidential or exempt data.

76 8. Recovering information and data in response to an
77 information technology security incident. The recovery may
78 include recommended improvements to the agency processes,
79 policies, or guidelines.

80 9. Establishing an information technology security
81 incident reporting process that includes procedures and tiered
82 reporting timeframes for notifying the department and the
83 Department of Law Enforcement of information technology security
84 incidents. The tiered reporting timeframes shall be based upon
85 the level of severity of the information technology security
86 incidents being reported.

87 10. Incorporating information obtained through detection
88 and response activities into the agency's information technology
89 security incident response plans.

90 11. Developing agency strategic and operational
91 information technology security plans required pursuant to this
92 section.

93 12. Establishing the managerial, operational, and
94 technical safeguards for protecting state government data and
95 information technology resources that align with the state
96 agency risk management strategy and that protect the
97 confidentiality, integrity, and availability of information and
98 data.

99 (d) Assist state agencies in complying with this section.

100 (e) In collaboration with the Cybercrime Office of the

101 Department of Law Enforcement, annually provide training for
102 state agency information security managers and computer security
103 incident response team members that contains training on
104 information technology security, including cybersecurity,
105 threats, trends, and best practices.

106 (f) Annually review the strategic and operational
107 information technology security plans of executive branch
108 agencies.

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

110 (a) Designate an information security manager to
111 administer the information technology security program of the
112 state agency. This designation must be provided annually in
113 writing to the department by January 1. A state agency's
114 information security manager, for purposes of these information
115 security duties, shall report directly to the agency head.

116 (b) In consultation with the department and the Cybercrime
117 Office of the Department of Law Enforcement, establish an agency
118 computer security incident response team to respond to an
119 information technology security incident. The agency computer
120 security incident response team shall convene upon notification
121 of an information technology security incident and must comply
122 with all applicable guidelines and processes established
123 pursuant to paragraph (3)(c).

124 (c) Submit to the department annually by July 31, the
125 state agency's strategic and operational information technology

126 security plans developed pursuant to rules and guidelines
127 established by the department.

128 1. The state agency strategic information technology
129 security plan must cover a 3-year period and, at a minimum,
130 define security goals, intermediate objectives, and projected
131 agency costs for the strategic issues of agency information
132 security policy, risk management, security training, security
133 incident response, and disaster recovery. The plan must be based
134 on the statewide information technology security strategic plan
135 created by the department and include performance metrics that
136 can be objectively measured to reflect the status of the state
137 agency's progress in meeting security goals and objectives
138 identified in the agency's strategic information security plan.

139 2. The state agency operational information technology
140 security plan must include a progress report that objectively
141 measures progress made towards the prior operational information
142 technology security plan and a project plan that includes
143 activities, timelines, and deliverables for security objectives
144 that the state agency will implement during the current fiscal
145 year.

146 (d) Conduct, and update every 3 years, a comprehensive
147 risk assessment, which may be completed by a private sector
148 vendor, to determine the security threats to the data,
149 information, and information technology resources, including
150 mobile devices and print environments, of the agency. The risk

151 assessment must comply with the risk assessment methodology
152 developed by the department and is confidential and exempt from
153 s. 119.07(1), except that such information shall be available to
154 the Auditor General, the Division of State Technology within the
155 department, the Cybercrime Office of the Department of Law
156 Enforcement, and, for state agencies under the jurisdiction of
157 the Governor, the Chief Inspector General.

158 (e) Develop, and periodically update, written internal
159 policies and procedures, which include procedures for reporting
160 information technology security incidents and breaches to the
161 Cybercrime Office of the Department of Law Enforcement and the
162 Division of State Technology within the department. Such
163 policies and procedures must be consistent with the rules,
164 guidelines, and processes established by the department to
165 ensure the security of the data, information, and information
166 technology resources of the agency. The internal policies and
167 procedures that, if disclosed, could facilitate the unauthorized
168 modification, disclosure, or destruction of data or information
169 technology resources are confidential information and exempt
170 from s. 119.07(1), except that such information shall be
171 available to the Auditor General, the Cybercrime Office of the
172 Department of Law Enforcement, the Division of State Technology
173 within the department, and, for state agencies under the
174 jurisdiction of the Governor, the Chief Inspector General.

175 (f) Implement managerial, operational, and technical

176 safeguards and risk assessment remediation plans recommended by
177 the department to address identified risks to the data,
178 information, and information technology resources of the agency.

179 (g) Ensure that periodic internal audits and evaluations
180 of the agency's information technology security program for the
181 data, information, and information technology resources of the
182 agency are conducted. The results of such audits and evaluations
183 are confidential information and exempt from s. 119.07(1),
184 except that such information shall be available to the Auditor
185 General, the Cybercrime Office of the Department of Law
186 Enforcement, the Division of State Technology within the
187 department, and, for agencies under the jurisdiction of the
188 Governor, the Chief Inspector General.

189 (h) Ensure that the information technology security and
190 cybersecurity requirements in both the written specifications
191 for the solicitation and service-level agreement of information
192 technology and information technology resources and services
193 meet or exceed the applicable state and federal laws,
194 regulations, and standards for information technology security
195 and cybersecurity. Service-level agreements must identify
196 service provider and state agency responsibilities for privacy
197 and security, protection of government data, personnel
198 background screening, and security deliverables with associated
199 frequencies.

200 (i) Provide information technology security and

201 cybersecurity awareness training to all state agency employees
 202 in the first 30 days after commencing employment concerning
 203 information technology security risks and the responsibility of
 204 employees to comply with policies, standards, guidelines, and
 205 operating procedures adopted by the state agency to reduce those
 206 risks. The training may be provided in collaboration with the
 207 Cybercrime Office of the Department of Law Enforcement.

208 (j) Develop a process for detecting, reporting, and
 209 responding to threats, breaches, or information technology
 210 security incidents which is consistent with the security rules,
 211 guidelines, and processes established by the Division of State
 212 Technology within the department ~~Agency for State Technology~~.

213 1. All information technology security incidents and
 214 breaches must be reported to the Division of State Technology
 215 within the department and the Cybercrime Office of the
 216 Department of Law Enforcement and must comply with the
 217 notification procedures and reporting timeframes established
 218 pursuant to paragraph (3) (c).

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

221 ~~(5)3-~~ Portions of records held by a state agency which
 222 contain network schematics, hardware and software
 223 configurations, or encryption, or which identify detection,
 224 investigation, or response practices for suspected or confirmed
 225 information technology security incidents, including suspected

226 or confirmed breaches, are confidential and exempt from s.
 227 119.07(1) and s. 24(a), Art. I of the State Constitution, if the
 228 disclosure of such records would facilitate unauthorized access
 229 to or the unauthorized modification, disclosure, or destruction
 230 of:

- 231 (a)~~a.~~ Data or information, whether physical or virtual; or
- 232 (b)~~b.~~ Information technology resources, which includes:
 - 233 1.~~(I)~~ Information relating to the security of the agency's
 - 234 technologies, processes, and practices designed to protect
 - 235 networks, computers, data processing software, and data from
 - 236 attack, damage, or unauthorized access; or
 - 237 2.~~(II)~~ Security information, whether physical or virtual,
 - 238 which relates to the agency's existing or proposed information
 - 239 technology systems.

240

~~Such records shall be available to the Auditor General, the~~
 241 ~~Division of State Technology within the department, the~~
 242 ~~Cybercrime Office of the Department of Law Enforcement, and, for~~
 243 ~~state agencies under the jurisdiction of the Governor, the Chief~~
 244 ~~Inspector General. Such records may be made available to a local~~
 245 ~~government, another state agency, or a federal agency for~~
 246 ~~information technology security purposes or in furtherance of~~
 247 ~~the state agency's official duties. This exemption applies to~~
 248 ~~such records held by a state agency before, on, or after the~~
 249 ~~effective date of this exemption. This subparagraph is subject~~
 250

251 ~~to the Open Government Sunset Review Act in accordance with s.~~
252 ~~119.15 and shall stand repealed on October 2, 2021, unless~~
253 ~~reviewed and saved from repeal through reenactment by the~~
254 ~~Legislature.~~

255 (6)~~(5)~~ The portions of risk assessments, evaluations,
256 external audits, and other reports of a state agency's
257 information technology security program for the data,
258 information, and information technology resources of the state
259 agency which are held by a state agency are confidential and
260 exempt from s. 119.07(1) and s. 24(a), Art. I of the State
261 Constitution if the disclosure of such portions of records would
262 facilitate unauthorized access to or the unauthorized
263 modification, disclosure, or destruction of:

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

265 (b) Information technology resources, which include:

266 1. Information relating to the security of the agency's
267 technologies, processes, and practices designed to protect
268 networks, computers, data processing software, and data from
269 attack, damage, or unauthorized access; or

270 2. Security information, whether physical or virtual,
271 which relates to the agency's existing or proposed information
272 technology systems. For purposes of this subsection, "external
273 audit" means an audit that is conducted by an entity other than
274 the state agency that is the subject of the audit.

275 (7) Those portions of a public meeting as specified in s.

276 286.011 which would reveal records which are confidential and
277 exempt under subsection (5) or subsection (6) are exempt from s.
278 286.011 and s. 24(b), Art. I of the State Constitution. No
279 exempt portion of an exempt meeting may be off the record. All
280 exempt portions of such meeting shall be recorded and
281 transcribed. Such recordings and transcripts are confidential
282 and exempt from disclosure under s. 119.07(1) and s. 24(a), Art.
283 I of the State Constitution unless a court of competent
284 jurisdiction, after an in camera review, determines that the
285 meeting was not restricted to the discussion of data and
286 information made confidential and exempt by this section. In the
287 event of such a judicial determination, only that portion of the
288 recording and transcript which reveals nonexempt data and
289 information may be disclosed to a third party.

290 (8) The ~~Such~~ portions of records made confidential and
291 exempt in subsections (5), (6), and (7) shall be available to
292 the Auditor General, the Cybercrime Office of the Department of
293 Law Enforcement, the Division of State Technology within the
294 department, and, for agencies under the jurisdiction of the
295 Governor, the Chief Inspector General. Such portions of records
296 may be made available to a local government, another state
297 agency, or a federal agency for information technology security
298 purposes or in furtherance of the state agency's official
299 duties. ~~For purposes of this subsection, "external audit" means~~
300 ~~an audit that is conducted by an entity other than the state~~

301 ~~agency that is the subject of the audit.~~

302 (9) The exemptions contained in subsections (5), (6), and
 303 (7) apply ~~This exemption applies to such~~ records held by a state
 304 agency before, on, or after the effective date of this
 305 exemption.

306 (10) Subsections (5), (6), and (7) are ~~This subsection is~~
 307 subject to the Open Government Sunset Review Act in accordance
 308 with s. 119.15 and shall stand repealed on October 2, 2025 ~~2021~~,
 309 unless reviewed and saved from repeal through reenactment by the
 310 Legislature.

311 (11) ~~(6)~~ The department shall adopt rules relating to
 312 information technology security and to administer this section.

313 Section 2. (1) (a) The Legislature finds it is a public
 314 necessity that the following data or information held by a state
 315 agency be made confidential and exempt from s. 119.07(1),
 316 Florida Statutes, and s. 24(a), Article I of the State
 317 Constitution:

318 1. Portions of records held by a state agency which
 319 contain network schematics, hardware and software
 320 configurations, encryption, or which identify detection,
 321 investigation, or response practices for suspected or confirmed
 322 information technology security incidents, including suspected
 323 or confirmed information technology security incidents,
 324 including suspected or confirmed breaches, if the disclosure of
 325 such records would facilitate unauthorized access to or the

326 unauthorized modification, disclosure, or destruction of:
327 a. Data or information, whether physical or virtual; or
328 b. Information technology resources, which includes:
329 (I) Information relating to the security of the agency's
330 technologies, processes, and practices designed to protect
331 networks, computers, data processing software, and data from
332 attack, damage, or unauthorized access; or
333 (II) Security information, whether physical or virtual,
334 which relates to the agency's existing or proposed information
335 technology systems.

336 2. Portions of risk assessments, evaluations, external
337 audits, and other reports of a state agency's information
338 technology security programs, if the disclosure of such portions
339 of records would facilitate unauthorized access to or the
340 unauthorized modification, disclosure, or destruction of:
341 a. Data or information, whether physical or virtual; or
342 b. Information technology resources, which include:
343 (I) Information relating to the security of the state
344 agency's technologies, processes, and practices designed to
345 protect networks, computers, data processing software, and data
346 from attack, damage, or unauthorized access; or
347 (II) Security information, whether physical or virtual,
348 which relates to the agency's existing or proposed information
349 technology systems.

350 (b) Such records must be made confidential and exempt from

351 public records requirements for the following reasons:

352 1. Portions of records held by a state agency which
353 contain network schematics, hardware and software
354 configurations, encryption, or which identify information
355 technology detection, investigation, or response practices for
356 suspected or confirmed information technology security incidents
357 or breaches are likely to be used in the investigations of the
358 incidents or breaches. The release of such information could
359 impede the investigation and impair the ability of reviewing
360 entities to effectively and efficiently execute their
361 investigative duties. In addition, the release of such
362 information before an active investigation is completed could
363 jeopardize the ongoing investigation.

364 2. An investigation of an information technology security
365 incident or breach is likely to result in the gathering of
366 sensitive personal information, including identification numbers
367 and personal financial and health information. Such information
368 could be used to commit identity theft or other crimes. In
369 addition, release of such information could subject possible
370 victims of the security incident or breach to further harm.

371 3. Disclosure of a record, including a computer forensic
372 analysis, or other information that would reveal weaknesses in a
373 state agency's data security could compromise that security in
374 the future if such information were available upon conclusion of
375 an investigation or once an investigation ceased to be active.

376 4. Such records are likely to contain proprietary
377 information about the security of the system at issue. The
378 disclosure of such information could result in the
379 identification of vulnerabilities and further breaches of that
380 system. In addition, the release of such information could give
381 business competitors an unfair advantage and weaken the security
382 technology supplier supplying the proprietary information in the
383 marketplace.

384 5. The disclosure of such records could potentially
385 compromise the confidentiality, integrity, and availability of
386 state agency data and information technology resources, which
387 would significantly impair the administration of vital state
388 programs. It is necessary that this information be made
389 confidential in order to protect the technology systems,
390 resources, and data of state agencies.

391 6. It is valuable, prudent, and critical to a state agency
392 to have an independent entity conduct a risk assessment, an
393 audit, or an evaluation or complete a report of the agency's
394 information technology program or related systems. Such
395 documents would likely include an analysis of the agency's
396 current information technology program or systems which could
397 clearly identify vulnerabilities or gaps in current systems or
398 processes and propose recommendations to remedy identified
399 vulnerabilities.

400 (2) (a) 1. The Legislature also finds that it is a public

401 necessity that those portions of a public meeting which would
402 reveal data and information described in paragraph (1)(a) be
403 made exempt from s. 286.011, Florida Statutes, and s. 24(b),
404 Article I of the State Constitution.

405 2. Such meetings must be made exempt from open meetings
406 requirements in order to protect agency information technology
407 systems, resources, and data. This information would clearly
408 identify a state agency's information technology systems and its
409 vulnerabilities and disclosure of such information would
410 jeopardize the information technology security of the state
411 agency and compromise the integrity and availability of state
412 agency data and information technology resources. Such
413 disclosure would significantly impair the administration of
414 state programs.

415 (b)1. The Legislature further finds that it is a public
416 necessity that the recordings and transcripts of the portions of
417 meetings specified in subparagraph (a)1. be made confidential
418 and exempt from s. 119.07(1), Florida Statutes, and s. 24(a),
419 Article I of the State Constitution.

420 2. It is necessary that the resulting recordings and
421 transcripts be made confidential and exempt from public record
422 requirements in order to protect state information technology
423 systems, resources, and data. The disclosure of such recordings
424 and transcripts would clearly identify a state agency's
425 information technology systems and its vulnerabilities. This

HB 821

2020

426 | disclosure would jeopardize the information technology security
427 | of the agency and compromise the integrity and availability of
428 | state data and information technology resources, which would
429 | significantly impair the administration of state programs.

430 | (3) The Legislature further finds that these public
431 | meeting and public records exemptions must be given retroactive
432 | application because they are remedial in nature.

433 | Section 3. This act shall take effect upon becoming a law.