

By Senator Baxley

12-01201-20

20201170__

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 which contain network schematics, hardware and
8 software configurations, or encryption; removing the
9 scheduled repeal of a certain public records
10 exemption; providing an exemption from public meetings
11 requirements for portions of meetings which would
12 reveal certain records; requiring the recording and
13 transcription of exempt portions of such meetings;
14 providing an exemption from public records
15 requirements for such recordings and transcripts;
16 providing an exception; revising applicability of
17 provisions requiring and authorizing certain records
18 to be made available to certain entities; providing
19 for future legislative review and repeal under the
20 Open Government Sunset Review Act of the exemptions;
21 providing for retroactive application of the
22 exemptions; providing statements of public necessity;
23 providing an effective date.

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

26
27 Section 1. Section 282.318, Florida Statutes, is amended to
28 read:

29 282.318 Security of data and information technology.—

12-01201-20

20201170__

30 (1) This section may be cited as the "Information
31 Technology Security Act."

32 (2) As used in this section, the term "state agency" has
33 the same meaning as provided in s. 282.0041, except that the
34 term includes the Department of Legal Affairs, the Department of
35 Agriculture and Consumer Services, and the Department of
36 Financial Services.

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

44 (a) Designate a state chief information security officer
45 who must have experience and expertise in security and risk
46 management for communications and information technology
47 resources.

48 (b) Develop, and annually update by February 1, a statewide
49 information technology security strategic plan that includes
50 security goals and objectives for the strategic issues of
51 information technology security policy, risk management,
52 training, incident management, and disaster recovery planning.

53 (c) Develop and publish for use by state agencies an
54 information technology security framework that, at a minimum,
55 includes guidelines and processes for:

56 1. Establishing asset management procedures to ensure that
57 an agency's information technology resources are identified and
58 managed consistent with their relative importance to the

12-01201-20

20201170__

59 agency's business objectives.

60 2. Using a standard risk assessment methodology that
61 includes the identification of an agency's priorities,
62 constraints, risk tolerances, and assumptions necessary to
63 support operational risk decisions.

64 3. Completing comprehensive risk assessments and
65 information technology security audits, which may be completed
66 by a private sector vendor, and submitting completed assessments
67 and audits to the department.

68 4. Identifying protection procedures to manage the
69 protection of an agency's information, data, and information
70 technology resources.

71 5. Establishing procedures for accessing information and
72 data to ensure the confidentiality, integrity, and availability
73 of such information and data.

74 6. Detecting threats through proactive monitoring of
75 events, continuous security monitoring, and defined detection
76 processes.

77 7. Establishing agency computer security incident response
78 teams and describing their responsibilities for responding to
79 information technology security incidents, including breaches of
80 personal information containing confidential or exempt data.

81 8. Recovering information and data in response to an
82 information technology security incident. The recovery may
83 include recommended improvements to the agency processes,
84 policies, or guidelines.

85 9. Establishing an information technology security incident
86 reporting process that includes procedures and tiered reporting
87 timeframes for notifying the department and the Department of

12-01201-20

20201170__

88 Law Enforcement of information technology security incidents.
89 The tiered reporting timeframes shall be based upon the level of
90 severity of the information technology security incidents being
91 reported.

92 10. Incorporating information obtained through detection
93 and response activities into the agency's information technology
94 security incident response plans.

95 11. Developing agency strategic and operational information
96 technology security plans required pursuant to this section.

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

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

103 (e) In collaboration with the Cybercrime Office of the
104 Department of Law Enforcement, annually provide training for
105 state agency information security managers and computer security
106 incident response team members that contains training on
107 information technology security, including cybersecurity,
108 threats, trends, and best practices.

109 (f) Annually review the strategic and operational
110 information technology security plans of executive branch
111 agencies.

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

113 (a) Designate an information security manager to administer
114 the information technology security program of the state agency.
115 This designation must be provided annually in writing to the
116 department by January 1. A state agency's information security

12-01201-20

20201170__

117 manager, for purposes of these information security duties,
118 shall report directly to the agency head.

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

127 (c) Submit to the department annually by July 31, the state
128 agency's strategic and operational information technology
129 security plans developed pursuant to rules and guidelines
130 established by the department.

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

142 2. The state agency operational information technology
143 security plan must include a progress report that objectively
144 measures progress made towards the prior operational information
145 technology security plan and a project plan that includes

12-01201-20

20201170__

146 activities, timelines, and deliverables for security objectives
147 that the state agency will implement during the current fiscal
148 year.

149 (d) Conduct, and update every 3 years, a comprehensive risk
150 assessment, which may be completed by a private sector vendor,
151 to determine the security threats to the data, information, and
152 information technology resources, including mobile devices and
153 print environments, of the agency. The risk assessment must
154 comply with the risk assessment methodology developed by the
155 department and is confidential and exempt from s. 119.07(1),
156 except that such information shall be available to the Auditor
157 General, the Division of State Technology within the department,
158 the Cybercrime Office of the Department of Law Enforcement, and,
159 for state agencies under the jurisdiction of the Governor, the
160 Chief Inspector General.

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

12-01201-20

20201170__

175 Department of Law Enforcement, the Division of State Technology
176 within the department, and, for state agencies under the
177 jurisdiction of the Governor, the Chief Inspector General.

178 (f) Implement managerial, operational, and technical
179 safeguards and risk assessment remediation plans recommended by
180 the department to address identified risks to the data,
181 information, and information technology resources of the agency.

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

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

203 (i) Provide information technology security and

12-01201-20

20201170__

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

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

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

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

224 ~~(5)3.~~ Portions of records held by a state agency which
225 contain network schematics, hardware and software
226 configurations, or encryption, or which identify detection,
227 investigation, or response practices for suspected or confirmed
228 information technology security incidents, including suspected
229 or confirmed breaches, are confidential and exempt from s.
230 119.07(1) and s. 24(a), Art. I of the State Constitution, if the
231 disclosure of such records would facilitate unauthorized access
232 to or the unauthorized modification, disclosure, or destruction

12-01201-20

20201170__

233 of:

234 (a)~~a.~~ Data or information, whether physical or virtual; or235 (b)~~b.~~ Information technology resources, which includes:236 1.~~(I)~~ Information relating to the security of the agency's
237 technologies, processes, and practices designed to protect
238 networks, computers, data processing software, and data from
239 attack, damage, or unauthorized access; or240 2.~~(II)~~ Security information, whether physical or virtual,
241 which relates to the agency's existing or proposed information
242 technology systems.

243

244 ~~Such records shall be available to the Auditor General, the~~
245 ~~Division of State Technology within the department, the~~
246 ~~Cybercrime Office of the Department of Law Enforcement, and, for~~
247 ~~state agencies under the jurisdiction of the Governor, the Chief~~
248 ~~Inspector General. Such records may be made available to a local~~
249 ~~government, another state agency, or a federal agency for~~
250 ~~information technology security purposes or in furtherance of~~
251 ~~the state agency's official duties. This exemption applies to~~
252 ~~such records held by a state agency before, on, or after the~~
253 ~~effective date of this exemption. This subparagraph is subject~~
254 ~~to the Open Government Sunset Review Act in accordance with s.~~
255 ~~119.15 and shall stand repealed on October 2, 2021, unless~~
256 ~~reviewed and saved from repeal through reenactment by the~~
257 ~~Legislature.~~

258 (6)~~(5)~~ The portions of risk assessments, evaluations,
259 external audits, and other reports of a state agency's
260 information technology security program for the data,
261 information, and information technology resources of the state

12-01201-20

20201170__

262 agency which are held by a state agency are confidential and
263 exempt from s. 119.07(1) and s. 24(a), Art. I of the State
264 Constitution if the disclosure of such portions of records would
265 facilitate unauthorized access to or the unauthorized
266 modification, disclosure, or destruction of:

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

268 (b) Information technology resources, which include:

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

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

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

12-01201-20

20201170__

291 recording and transcript which reveals nonexempt data and
292 information may be disclosed to a third party.

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

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

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

314 (11)~~(6)~~ The department shall adopt rules relating to
315 information technology security and to administer this section.

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

12-01201-20

20201170__

320 Constitution:

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

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

330 b. Information technology resources, which include:

331 (I) Information relating to the security of the agency's
332 technologies, processes, and practices designed to protect
333 networks, computers, data processing software, and data from
334 attack, damage, or unauthorized access; or

335 (II) Security information, whether physical or virtual,
336 which relates to the agency's existing or proposed information
337 technology systems.

338 2. Portions of risk assessments, evaluations, external
339 audits, and other reports of a state agency's information
340 technology security programs, if the disclosure of such portions
341 of records would facilitate unauthorized access to or the
342 unauthorized modification, disclosure, or destruction of:

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

344 b. Information technology resources, which include:

345 (I) Information relating to the security of the state
346 agency's technologies, processes, and practices designed to
347 protect networks, computers, data processing software, and data
348 from attack, damage, or unauthorized access; or

12-01201-20

20201170__

349 (II) Security information, whether physical or virtual,
350 which relates to the agency's existing or proposed information
351 technology systems.

352 (b) Such records must be made confidential and exempt from
353 public records requirements for the following reasons:

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

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

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

377 4. Such records are likely to contain proprietary

12-01201-20

20201170__

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

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

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

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

406 2. Such meetings must be made exempt from open meetings

12-01201-20

20201170__

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

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

421 2. It is necessary that the resulting recordings and
422 transcripts be made confidential and exempt from public record
423 requirements in order to protect state information technology
424 systems, resources, and data. The disclosure of such recordings
425 and transcripts would clearly identify a state agency's
426 information technology systems and its vulnerabilities. This
427 disclosure would jeopardize the information technology security
428 of the agency and compromise the integrity and availability of
429 state data and information technology resources, which would
430 significantly impair the administration of state programs.

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

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