

By the Committee on Governmental Oversight and Accountability

585-02050-26

20267024

A bill to be entitled

An act relating to a review under the Open Government Sunset Review Act; amending s. 119.0725, F.S.; revising definitions and defining terms; providing an exemption from public records requirements for the cybersecurity, information technology, and operational technology information held by an agency; providing an exemption from public meetings requirements for any portion of a meeting that would reveal such information; providing for retroactive application of the exemptions; providing for future legislative review and repeal of the exemptions; amending ss. 15.16, 24.1051, 101.5607, 106.0706, 112.31446, 119.07, 119.071, 119.0712, 119.0713, s. 119.0714, and 282.318, F.S.; conforming cross-references and provisions to changes made by the act; repealing s. 627.352, F.S., relating to security of data and information technology in the Citizens Property Insurance Corporation; repealing s. 1004.055, F.S., relating to security of data and information technology in state postsecondary education institutions; providing a statement of public necessity; providing an effective date.

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

Section 1. Section 119.0725, Florida Statutes, is amended to read:

119.0725 Agency cybersecurity information; public records

585-02050-26

20267024

30 exemption; public meetings exemption.—

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

32 (a) "Breach" means unauthorized access of data or in
33 ~~electronic form containing personal~~ information. Good faith
34 access of data or personal information by an employee or agent
35 of an agency does not constitute a breach, provided that the
36 data or information is not used for a purpose unrelated to the
37 business 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" means the protection afforded to
44 information technology or operational technology in order to
45 attain the applicable objectives of preserving the
46 confidentiality, integrity, and availability of such
47 technologies, data, and information has the same meaning as in
48 s. 282.0041.

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

50 (e) "Incident" means a violation or imminent threat of
51 violation, whether such violation is accidental or deliberate,
52 of an agency's cybersecurity, information technology, or
53 operational technology resources, security, policies, or
54 practices. As used in this paragraph, the term "imminent threat
55 of violation" means a situation in which the agency has a
56 factual basis for believing that a specific incident is about to
57 occur.

58 (f) "Information technology" has the same meaning as in s.

585-02050-26

20267024

59 282.0041.

60 (g) “Login credentials” means information used to
61 authenticate a user’s identity or otherwise authorize access
62 when logging into a computer, computer system, computer network,
63 electronic device, or online user account accessible over the
64 Internet through a mobile device, a website, or any other
65 electronic means, or for authentication or password or account
66 recovery.

67 (h) “Operational technology” means the hardware and
68 software that cause or detect a change through the direct
69 monitoring or control of physical devices, systems, processes,
70 or events.

71 (i) “Public-facing portal” means a web portal or computer
72 application accessible by the public over the Internet, whether
73 through a mobile device, website, or other electronic means.

74 (2) The following information held by an agency is
75 confidential and exempt from s. 119.07(1) and s. 24(a), Art. I
76 of the State Constitution:

77 (a) ~~Coverage limits and deductible or self-insurance~~
78 ~~amounts of insurance or other risk mitigation coverages acquired~~
79 ~~for the protection of information technology systems,~~
80 ~~operational technology systems, or data of an agency.~~

81 (b) Information relating to critical infrastructure.

82 (b) ~~(e)~~ Cybersecurity incident information reported pursuant
83 to s. 282.318 or s. 282.3185.

84 (c) ~~(d)~~ Network schematics, hardware and software
85 configurations, ~~or~~ encryption information, or any information
86 that identifies detection, investigation, or response practices
87 ~~related to for suspected or confirmed~~ cybersecurity incidents,

585-02050-26

20267024

88 including ~~suspected or confirmed~~ breaches, if the disclosure of
89 such information ~~could~~ ~~would~~ facilitate unauthorized access to
90 or unauthorized modification, disclosure, or destruction of
91 data, information, or existing or proposed information
92 technology or operational technology:

93 1. ~~Data or information, whether physical or virtual; or~~
94 2. ~~Information technology resources, which include an~~
95 ~~agency's existing or proposed information technology systems.~~

96 (d) Information relating to processes or practices designed
97 to protect data, information, or existing or proposed
98 information technology or operational technology if the
99 disclosure of such information could facilitate unauthorized
100 access to or unauthorized modification, disclosure, or
101 destruction of such data, information, or technology.

102 (e) Portions of risk assessments, evaluation, audits, and
103 other reports of an agency's cybersecurity program if the
104 disclosure of such information could facilitate unauthorized
105 access to or unauthorized modification, disclosure, or
106 destruction of data, information, or existing or proposed
107 information technology or operational technology.

108 (f) Login credentials.

109 (g) Internet protocol addresses, geolocation data, and
110 other information that describes the location, computer,
111 computer system, or computer network from which a user accesses
112 a public-facing portal, and the dates and times that a user
113 accesses a public-facing portal.

114 (h) Agency-produced data processing software that is
115 sensitive.

116 (i) Insurance and self-insurance coverage limits and

585-02050-26

20267024

117 deductibles, as well as any other risk mitigation coverages
118 acquired for the protection of information technology,
119 operational technology, or data of an agency.

120 (3) Any portion of a meeting that would reveal information
121 made confidential and exempt under subsection (2) is exempt from
122 s. 286.011 and s. 24(b), Art. I of the State Constitution. An
123 exempt portion of a meeting may not be off the record and must
124 be recorded and transcribed. The recording and transcript are
125 confidential and exempt from s. 119.07(1) and s. 24(a), Art. I
126 of the State Constitution.

127 (4) The public records exemptions contained in this section
128 apply to information held by an agency before, on, or after the
129 effective date of the exemptions July 1, 2022.

130 (5) (a) Information made confidential and exempt pursuant to
131 this section shall be made available to a law enforcement
132 agency, the Auditor General, the Cybercrime Office of the
133 Department of Law Enforcement, the Florida Digital Service
134 within the Department of Management Services, and, for agencies
135 under the jurisdiction of the Governor, the Chief Inspector
136 General.

137 (b) Such confidential and exempt information may be
138 disclosed by an agency in the furtherance of its official duties
139 and responsibilities or to another agency or governmental entity
140 in the furtherance of the agency's or governmental entity's
141 official its statutory duties and responsibilities.

142 (6) Agencies may report information about cybersecurity
143 incidents in the aggregate.

144 (7) This section is subject to the Open Government Sunset
145 Review Act in accordance with s. 119.15 and shall stand repealed

585-02050-26

20267024

146 on October 2, 2031 2026, unless reviewed and saved from repeal
147 through reenactment by the Legislature.

148 Section 2. Subsection (3) of section 15.16, Florida
149 Statutes, is amended to read:

150 15.16 Reproduction of records; admissibility in evidence;
151 electronic receipt and transmission of records; certification;
152 acknowledgment.—

153 (3) (a) The Department of State may cause to be received
154 electronically any records that are required or authorized to be
155 filed with it pursuant to chapter 48, chapter 55, chapter 117,
156 chapter 118, chapter 495, chapter 605, chapter 606, chapter 607,
157 chapter 610, chapter 617, chapter 620, chapter 621, chapter 679,
158 chapter 713, or chapter 865, through facsimile or other
159 electronic transfers, for the purpose of filing such records.
160 The originals of all such electronically transmitted records
161 must be executed in the manner provided in paragraph (5) (b). The
162 receipt of such electronic transfer constitutes delivery to the
163 department as required by law. The department may use electronic
164 transmissions for purposes of notice in the administration of
165 chapters 48, 55, 117, 118, 495, 605, 606, 607, 610, 617, 620,
166 621, 679, and 713 and s. 865.09. The Department of State may
167 collect e-mail addresses for purposes of notice and
168 communication in the performance of its duties and may require
169 filers and registrants to furnish such e-mail addresses when
170 presenting documents for filing.

171 (b) The department may implement a password-protected
172 system for any record electronically received pursuant to
173 paragraph (a) and may require filers to produce supplemental
174 materials to use such system, including, but not limited to, an

585-02050-26

20267024

175 original signature of the filer and verification of credentials.
176 The department may also implement a password-protected system
177 that allows entities organized under the chapters specified in
178 paragraph (a) to identify authorized account holders for the
179 purpose of electronically filing records related to the entity.
180 If the department implements such a system, it must send to each
181 e-mail address on file with the Division of Corporations on
182 January 1, 2024, a code to participate in a password-protected
183 system. The department may require verification of the identity
184 of an authorized account holder before the account holder is
185 authorized to electronically file a record with the department.

186 (c)1. E-mail addresses collected by the Department of State
187 pursuant to this subsection are exempt from s. 119.07(1) and s.
188 24(a), Art. I of the State Constitution. This exemption applies
189 to e-mail addresses held by the Department of State before, on,
190 or after the effective date of the exemption.

191 ~~2. Secure login credentials held by the Department of State~~
192 ~~for the purpose of allowing a person to electronically file~~
193 ~~records under this subsection are exempt from s. 119.07(1) and~~
194 ~~s. 24(a), Art. I of the State Constitution. This exemption~~
195 ~~applies to secure login credentials held by the Department of~~
196 ~~State before, on, or after the effective date of the exemption.~~
197 ~~For purposes of this subparagraph, the term "secure login~~
198 ~~credentials" means information held by the department for~~
199 ~~purposes of authenticating a user logging into a user account on~~
200 ~~a computer, a computer system, a computer network, or an~~
201 ~~electronic device; an online user account accessible over the~~
202 ~~Internet, whether through a mobile device, a website, or any~~
203 ~~other electronic means; or information used for authentication~~

585-02050-26

20267024

204 ~~or password recovery.~~205 3. This paragraph is subject to the Open Government Sunset
206 Review Act in accordance with s. 119.15 and shall stand repealed
207 on October 2, 2028, unless reviewed and saved from repeal
208 through reenactment by the Legislature.209 Section 3. Subsection (1) of section 24.1051, Florida
210 Statutes, is amended to read:211 24.1051 Exemptions from inspection or copying of public
212 records.—213 (1) (a) The following information held by the department is
214 confidential and exempt from s. 119.07(1) and s. 24(a), Art. I
215 of the State Constitution:216 1. Information that, if released, could harm the security
217 or integrity of the department, including:218 a. ~~Information relating to the security of the department's~~
219 ~~technologies, processes, and practices designed to protect~~
220 ~~networks, computers, data processing software, data, and data~~
221 ~~systems from attack, damage, or unauthorized access. This sub-~~
222 ~~paragraph is subject to the Open Government Sunset Review Act~~
223 ~~in accordance with s. 119.15 and shall stand repealed on October~~
224 ~~2, 2027, unless reviewed and saved from repeal through~~
225 ~~reenactment by the Legislature.~~226 b. Security information or information that would reveal
227 security measures of the department, whether physical or
228 virtual.229 b.e. Information about lottery games, promotions, tickets,
230 and ticket stock, including information concerning the
231 description, design, production, printing, packaging, shipping,
232 delivery, storage, and validation of such games, promotions,

585-02050-26

20267024

233 tickets, and stock.

234 c.d. Information concerning terminals, machines, and
235 devices that issue tickets.

236 2. Information that must be maintained as confidential in
237 order for the department to participate in a multistate lottery
238 association or game.

239 3. Personal identifying information obtained by the
240 department when processing background investigations of current
241 or potential retailers or vendors.

242 4. Financial information about an entity which is not
243 publicly available and is provided to the department in
244 connection with its review of the financial responsibility of
245 the entity pursuant to s. 24.111 or s. 24.112, provided that the
246 entity marks such information as confidential. However,
247 financial information related to any contract or agreement, or
248 an addendum thereto, with the department, including the amount
249 of money paid, any payment structure or plan, expenditures,
250 incentives, bonuses, fees, and penalties, shall be public
251 record.

252 (b) This exemption is remedial in nature, and it is the
253 intent of the Legislature that this exemption apply to
254 information held by the department before, on, or after May 14,
255 2019.

256 (c) Information made confidential and exempt under this
257 subsection may be released to other governmental entities as
258 needed in connection with the performance of their duties. The
259 receiving governmental entity shall maintain the confidential
260 and exempt status of such information.

261 Section 4. Paragraph (d) of subsection (1) of section

585-02050-26

20267024

262 101.5607, Florida Statutes, is amended to read:

263 101.5607 Department of State to maintain voting system
264 information; prepare software.—

265 (1)

266 (d) Section 119.0725(2)(h) ~~119.071(1)(f)~~ applies to all
267 software on file with the Department of State.

268 Section 5. Section 106.0706, Florida Statutes, is amended
269 to read:

270 106.0706 Electronic filing of campaign finance reports;
271 public records exemption.—

272 ~~(1) All user identifications and passwords held by the
273 Department of State pursuant to s. 106.0705 are confidential and
274 exempt from s. 119.07(1) and s. 24(a), Art. I of the State
275 Constitution.~~

276 ~~(2)(a) Information entered in the electronic filing system
277 for purposes of generating a report pursuant to s. 106.0705 is
278 exempt from s. 119.07(1) and s. 24(a), Art. I of the State
279 Constitution.~~

280 ~~(2)(b) Information entered in the electronic filing system
281 is no longer exempt once the report is generated and filed with
282 the Division of Elections.~~

283 Section 6. Subsection (6) of section 112.31446, Florida
284 Statutes, is amended to read:

285 112.31446 Electronic filing system for financial
286 disclosure.—

287 ~~(6)(a) All secure login credentials held by the commission
288 for the purpose of allowing access to the electronic filing
289 system are exempt from s. 119.07(1) and s. 24(a), Art. I of the
290 State Constitution.~~

585-02050-26

20267024

291 (b) Information entered in the electronic filing system for
292 purposes of financial disclosure is exempt from s. 119.07(1) and
293 s. 24(a), Art. I of the State Constitution. Information entered
294 in the electronic filing system is no longer exempt once the
295 disclosure of financial interests or statement of financial
296 interests is submitted to the commission or, in the case of a
297 candidate, filed with a qualifying officer, whichever occurs
298 first.

299 Section 7. Paragraph (g) of subsection (1) of section
300 119.07, Florida Statutes, is amended to read:

301 119.07 Inspection and copying of records; photographing
302 public records; fees; exemptions.—

303 (1)

304 (g) In any civil action in which an exemption to this
305 section is asserted, if the exemption is alleged to exist under
306 or by virtue of s. 119.071(1) (d) ~~or (f)~~, (2) (d), (e), or (f), or
307 (4) (c), the public record or part thereof in question shall be
308 submitted to the court for an inspection in camera. If an
309 exemption is alleged to exist under or by virtue of s.
310 119.071(2) (c), an inspection in camera is discretionary with the
311 court. If the court finds that the asserted exemption is not
312 applicable, it shall order the public record or part thereof in
313 question to be immediately produced for inspection or copying as
314 requested by the person seeking such access.

315 Section 8. Paragraph (f) of subsection (1) of section
316 119.071, Florida Statutes, is amended to read:

317 119.071 General exemptions from inspection or copying of
318 public records.—

319 (1) AGENCY ADMINISTRATION.—

585-02050-26

20267024

320 (f) ~~Agency produced data processing software that is~~
321 ~~sensitive is exempt from s. 119.07(1) and s. 24(a), Art. I of~~
322 ~~the State Constitution. The designation of agency-produced~~
323 ~~software as sensitive does not prohibit an agency head from~~
324 ~~sharing or exchanging such software with another public agency.~~

325 Section 9. Paragraph (f) of subsection (2) of section
326 119.0712, Florida Statutes, is amended to read:

327 119.0712 Executive branch agency-specific exemptions from
328 inspection or copying of public records.—

329 (2) DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES.—

330 (f) 1. ~~Secure login credentials held by the Department of~~
331 ~~Highway Safety and Motor Vehicles are exempt from s. 119.07(1)~~
332 ~~and s. 24(a), Art. I of the State Constitution. This exemption~~
333 ~~applies to secure login credentials held by the department~~
334 ~~before, on, or after the effective date of the exemption. For~~
335 ~~purposes of this subparagraph, the term "secure login~~
336 ~~credentials" means information held by the department for~~
337 ~~purposes of authenticating a user logging into a user account on~~
338 ~~a computer, a computer system, a computer network, or an~~
339 ~~electronic device; an online user account accessible over the~~
340 ~~Internet, whether through a mobile device, a website, or any~~
341 ~~other electronic means; or information used for authentication~~
342 ~~or password recovery.~~

343 2. ~~Internet protocol addresses, geolocation data, and other~~
344 ~~information held by the Department of Highway Safety and Motor~~
345 ~~Vehicles which describes the location, computer, computer~~
346 ~~system, or computer network from which a user accesses a public-~~
347 ~~facing portal, and the dates and times that a user accesses a~~
348 ~~public-facing portal, are exempt from s. 119.07(1) and s. 24(a),~~

585-02050-26

20267024

349 ~~Art. I of the State Constitution. This exemption applies to such~~
350 ~~information held by the department before, on, or after the~~
351 ~~effective date of the exemption. For purposes of this~~
352 ~~subparagraph, the term "public-facing portal" means a web portal~~
353 ~~or computer application accessible by the public over the~~
354 ~~Internet, whether through a mobile device, website, or other~~
355 ~~electronic means, which is established for administering chapter~~
356 ~~319, chapter 320, chapter 322, chapter 328, or any other~~
357 ~~provision of law conferring duties upon the department.~~

358 ~~3. This paragraph is subject to the Open Government Sunset~~
359 ~~Review Act in accordance with s. 119.15 and shall stand repealed~~
360 ~~on October 2, 2026, unless reviewed and saved from repeal~~
361 ~~through reenactment by the Legislature.~~

362 Section 10. Subsection (5) of section 119.0713, Florida
363 Statutes, is amended to read:

364 119.0713 Local government agency exemptions from inspection
365 or copying of public records.—

366 (5) ~~(a) Customer meter-derived data and billing information~~
367 ~~in increments less than one billing cycle~~ ~~The following~~
368 ~~information held by a utility owned or operated by a unit of~~
369 ~~local government~~ ~~are~~ ~~is~~ ~~exempt from s. 119.07(1) and s. 24(a),~~
370 ~~Art. I of the State Constitution.~~

371 1. ~~Information related to the security of the technology,~~
372 ~~processes, or practices of a utility owned or operated by a unit~~
373 ~~of local government that are designed to protect the utility's~~
374 ~~networks, computers, programs, and data from attack, damage, or~~
375 ~~unauthorized access, which information, if disclosed, would~~
376 ~~facilitate the alteration, disclosure, or destruction of such~~
377 ~~data or information technology resources.~~

585-02050-26

20267024

378 2. ~~Information related to the security of existing or~~
379 ~~proposed information technology systems or industrial control~~
380 ~~technology systems of a utility owned or operated by a unit of~~
381 ~~local government, which, if disclosed, would facilitate~~
382 ~~unauthorized access to, and alteration or destruction of, such~~
383 ~~systems in a manner that would adversely impact the safe and~~
384 ~~reliable operation of the systems and the utility.~~

385 3. ~~Customer meter-derived data and billing information in~~
386 ~~increments less than one billing cycle.~~

387 (a) ~~(b)~~ This exemption applies to such data and information
388 held by a utility owned or operated by a unit of local
389 government before, on, or after the effective date of this
390 exemption.

391 (b) ~~(e)~~ This subsection is ~~Subparagraphs (a)1. and 2. are~~
392 subject to the Open Government Sunset Review Act in accordance
393 with s. 119.15 and shall stand repealed on October 2, 2027,
394 unless reviewed and saved from repeal through reenactment by the
395 Legislature.

396 Section 11. Paragraph (b) of subsection (1) of section
397 119.0714, Florida Statutes, is amended to read:

398 119.0714 Court files; court records; official records.—

399 (1) COURT FILES.—Nothing in this chapter shall be construed
400 to exempt from s. 119.07(1) a public record that was made a part
401 of a court file and that is not specifically closed by order of
402 court, except:

403 (b) Data processing software as provided in s.
404 119.0725(2) (h) s. 119.071(1)(f).

405 Section 12. Paragraphs (d), (e), and (g) of subsection (4)
406 and subsections (5) through (9) of section 282.318, Florida

585-02050-26

20267024

407 Statutes, are amended to read:

408 282.318 Cybersecurity.—

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

410 (d) Conduct, and update every 3 years, a comprehensive risk
411 assessment, which may be completed by a private sector vendor,
412 to determine the security threats to the data, information, and
413 information technology resources, including mobile devices and
414 print environments, of the agency. The risk assessment must
415 comply with the risk assessment methodology developed by the
416 department ~~and is confidential and exempt from s. 119.07(1),~~
417 ~~except that such information shall be available to the Auditor~~
418 ~~General, the Florida Digital Service within the department, the~~
419 ~~Cybercrime Office of the Department of Law Enforcement, and, for~~
420 ~~state agencies under the jurisdiction of the Governor, the Chief~~
421 ~~Inspector General.~~ If a private sector vendor is used to
422 complete a comprehensive risk assessment, it must attest to the
423 validity of the risk assessment findings.

424 (e) Develop, and periodically update, written internal
425 policies and procedures, which include procedures for reporting
426 cybersecurity incidents and breaches to the Cybercrime Office of
427 the Department of Law Enforcement and the Florida Digital
428 Service within the department. Such policies and procedures must
429 be consistent with the rules, guidelines, and processes
430 established by the department to ensure the security of the
431 data, information, and information technology resources of the
432 agency. ~~The internal policies and procedures that, if disclosed,~~
433 ~~could facilitate the unauthorized modification, disclosure, or~~
434 ~~destruction of data or information technology resources are~~
435 ~~confidential information and exempt from s. 119.07(1), except~~

585-02050-26

20267024

436 that such information shall be available to the Auditor General,
437 the Cybercrime Office of the Department of Law Enforcement, the
438 Florida Digital Service within the department, and, for state
439 agencies under the jurisdiction of the Governor, the Chief
440 Inspector General.

441 (g) Ensure that periodic internal audits and evaluations of
442 the agency's cybersecurity program for the data, information,
443 and information technology resources of the agency are
444 conducted. ~~The results of such audits and evaluations are~~
445 ~~confidential information and exempt from s. 119.07(1), except~~
446 that such information shall be available to the Auditor General,
447 the Cybercrime Office of the Department of Law Enforcement, the
448 Florida Digital Service within the department, and, for agencies
449 under the jurisdiction of the Governor, the Chief Inspector
450 General.

451 (5) The portions of risk assessments, evaluations, external
452 audits, and other reports of a state agency's cybersecurity
453 program for the data, information, and information technology
454 resources of the state agency which are held by a state agency
455 are confidential and exempt from s. 119.07(1) and s. 24(a), Art.
456 I of the State Constitution if the disclosure of such portions
457 of records would facilitate unauthorized access to or the
458 unauthorized modification, disclosure, or destruction of:

459 (a) Data or information, whether physical or virtual; or
460 (b) Information technology resources, which include:
461 1. Information relating to the security of the agency's
462 technologies, processes, and practices designed to protect
463 networks, computers, data processing software, and data from
464 attack, damage, or unauthorized access; or

585-02050-26

20267024

465 2. Security information, whether physical or virtual, which
466 relates to the agency's existing or proposed information
467 technology systems.

468

469 For purposes of this subsection, "external audit" means an audit
470 that is conducted by an entity other than the state agency that
471 is the subject of the audit.

472 (6) Those portions of a public meeting as specified in s.
473 286.011 which would reveal records which are confidential and
474 exempt under subsection (5) are exempt from s. 286.011 and s.
475 24(b), Art. I of the State Constitution. No exempt portion of an
476 exempt meeting may be off the record. All exempt portions of
477 such meeting shall be recorded and transcribed. Such recordings
478 and transcripts are confidential and exempt from disclosure
479 under s. 119.07(1) and s. 24(a), Art. I of the State
480 Constitution unless a court of competent jurisdiction, after an
481 in camera review, determines that the meeting was not restricted
482 to the discussion of data and information made confidential and
483 exempt by this section. In the event of such a judicial
484 determination, only that portion of the recording and transcript
485 which reveals nonexempt data and information may be disclosed to
486 a third party.

487 (7) The portions of records made confidential and exempt in
488 subsections (5) and (6) shall be available to the Auditor
489 General, the Cybercrime Office of the Department of Law
490 Enforcement, the Florida Digital Service within the department,
491 and, for agencies under the jurisdiction of the Governor, the
492 Chief Inspector General. Such portions of records may be made
493 available to a local government, another state agency, or a

585-02050-26

20267024

494 ~~federal agency for cybersecurity purposes or in furtherance of~~
495 ~~the state agency's official duties.~~

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

499 ~~(9) Subsections (5) and (6) are subject to the Open~~
500 ~~Government Sunset Review Act in accordance with s. 119.15 and~~
501 ~~shall stand repealed on October 2, 2026, unless reviewed and~~
502 ~~saved from repeal through reenactment by the Legislature.~~

503 Section 13. Section 627.352, Florida Statutes, is repealed.

504 Section 14. Section 1004.055, Florida Statutes, is
505 repealed.

506 Section 15. (1) The Legislature finds that it is a public
507 necessity that the following information held by an agency be
508 made confidential and exempt from s. 119.07(1), Florida
509 Statutes, and s. 24(a), Article I of the State Constitution:

510 (a) Network schematics, hardware and software
511 configurations, encryption information, or any information that
512 identifies detection, investigation, or response practices
513 relating to cybersecurity incidents, including breaches, if the
514 disclosure of such information could facilitate unauthorized
515 access to or unauthorized modification, disclosure, or
516 destruction of data, information, or existing or proposed
517 information technology or operational technology.

518 (b) Information relating to processes or practices designed
519 to protect data, information, or existing or proposed
520 information technology or operational technology if the
521 disclosure of such information could facilitate unauthorized
522 access to or unauthorized modification, disclosure, or

585-02050-26

20267024

523 destruction of such data, information, or technology.

524 (c) Portions of risk assessments, evaluations, audits, and
525 other reports of an agency's cybersecurity program if the
526 disclosure of such information could facilitate unauthorized
527 access to or unauthorized modification, disclosure, or
528 destruction of data, information, or existing or proposed
529 information technology or operational technology.

530 (d) Login credentials.

531 (e) Internet protocol addresses, geolocation data, and
532 other information that describes the location, computer,
533 computer system, or computer network from which a user accesses
534 a public-facing portal, and the dates and times that a user
535 accesses a public-facing portal.

536 (f) Agency-produced data processing software that is
537 sensitive.

538 (g) Insurance and self-insurance coverage limits and
539 deductibles, as well as any other risk mitigation coverages,
540 acquired for the protection of information technology,
541 operational technology, or data of an agency.

542 (2) The Legislature finds that release of the information
543 described in subsection (1) could place an agency at greater
544 risk of breaches, cybersecurity incidents, and ransomware
545 attacks. Network schematics, hardware and software
546 configurations, encryption information, or any information that
547 identifies detection, investigation, or response practices for
548 cybersecurity incidents, including breaches, reveals how an
549 agency's information technology and operational technology
550 systems are structured and defended. Disclosure of such
551 information could enable a malicious actor to map system

585-02050-26

20267024

552 architecture, identify vulnerabilities, and bypass security
553 controls. Information describing processes or practices designed
554 to protect data, information, or existing or proposed
555 information technology or operational technology could similarly
556 be used to exploit weaknesses and predict defensive actions.
557 Portions of risk assessments, evaluations, audits, and other
558 reports of an agency's cybersecurity program routinely include
559 descriptions of vulnerabilities, testing results, and
560 recommendations. Disclosure of such information would
561 substantially increase the likelihood of a successful
562 cyberattack. Login credentials are a foundational security
563 control, and disclosure of such information could allow
564 malicious actors to authenticate themselves in order to access
565 government systems, impersonate legitimate users, and access
566 personal identifying and other sensitive information. Internet
567 protocol addresses, geolocation data, and other information that
568 describes the location, computer, computer system, or computer
569 network from which a user accesses a public-facing portal, and
570 the dates and times that a user accesses a public-facing portal,
571 could be used to track usage patterns, identify remote access
572 points, or monitor portal vulnerabilities. Sensitive agency-
573 produced data processing software can reveal the inner workings
574 of security controls, authentication mechanisms, or automated
575 processes that malicious actors can use to exploit weaknesses in
576 security measures. If information related to coverage limits and
577 deductibles of cybersecurity insurance were disclosed, it could
578 give cybercriminals an understanding of the monetary sum an
579 agency can afford or may be willing to pay as a result of a
580 ransomware attack at the expense of taxpayers. Accordingly, the

585-02050-26

20267024

581 Legislature finds that the disclosure of such sensitive
582 cybersecurity-related information would significantly impair the
583 administration of vital governmental programs.

584 (3) The Legislature also finds that it is a public
585 necessity that any portion of a meeting which would reveal the
586 confidential and exempt information in subsection (1) be made
587 exempt from s. 286.011, Florida Statutes, and s. 24(b), Article
588 I of the State Constitution, and that any recordings and
589 transcripts of the closed portion of a meeting be made
590 confidential and exempt from s. 119.07(1), Florida Statutes, and
591 s. 24(a), Article I of the State Constitution. The failure to
592 close that portion of a meeting at which confidential and exempt
593 information would be revealed, and prevent the disclosure of the
594 recordings and transcripts of those portions of a meeting, would
595 defeat the purpose of the underlying public records exemption
596 and could result in the release of highly sensitive information
597 related to the cybersecurity of an agency system.

598 (4) For these reasons, the Legislature finds that these
599 public records and public meetings exemptions are of the utmost
600 importance and are a public necessity.

601 Section 16. This act shall take effect upon becoming a law.