

HB 7023

2026

A bill to be entitled
An act relating to a review under the Open Government Sunset Review Act; amending s. 119.0725, F.S.; providing and revising definitions; providing an exemption from public records requirements for certain cybersecurity processes or practices, certain cybersecurity program reports, login credentials, and certain information associated with access to a public-facing portal held by an agency; revising an exemption from public records requirements for certain cybersecurity insurance information and certain cybersecurity-related information held by an agency; consolidating a public record exemption for certain agency-produced data processing software held by an agency; expanding an exemption from public meetings requirements for portions of a meeting that would reveal certain cybersecurity-related information held by an agency; providing for future legislative review and repeal of the exemptions; amending s. 15.16, F.S.; removing an exemption from public records requirements for certain secure login credentials held by the Department of State; amending s. 24.1051, F.S.; removing an exemption from public records requirements for certain cybersecurity-related information held by the Department of the Lottery; amending s. 101.5607,

HB 7023

2026

26 F.S.; conforming a provision to changes made by the
27 act; amending s. 106.0706, F.S.; removing an exemption
28 from public records requirements for certain user
29 identifications and passwords held by the Department
30 of State; amending s. 112.31446, F.S.; removing an
31 exemption from public records requirements for certain
32 secure login credentials held by the Commission on
33 Ethics; amending s. 119.07, F.S.; conforming a
34 provision to changes made by the act; amending s.
35 119.071, F.S.; removing an exemption from public
36 records requirements for certain agency-produced data
37 processing software; amending s. 119.0712, F.S.;
38 removing an exemption from public records requirements
39 for certain secure login credentials and certain
40 information associated with access to a public-facing
41 portal held by the Department of Highway Safety and
42 Motor Vehicles; amending s. 119.0713, F.S.; removing
43 an exemption from public records requirements for
44 certain cybersecurity-related information held by a
45 utility owned or operated by a unit of local
46 government; amending s. 119.0714, F.S.; conforming a
47 provision to changes made by the act; amending s.
48 282.318, F.S.; removing an exemption from public
49 records requirements for a comprehensive risk
50 assessment held by an agency; removing exemptions from

HB 7023

2026

51 public records requirements for certain cybersecurity-
52 related internal policies and procedures, certain
53 cybersecurity-related internal audits and evaluations
54 held by an agency, and certain cybersecurity-related
55 reports held by an agency; repealing s. 627.352, F.S.,
56 relating to security of data and information
57 technology in Citizens Property Insurance Corporation;
58 repealing s. 1004.055, F.S., relating to security of
59 data and information technology in state postsecondary
60 education institutions; providing a statement of
61 public necessity; providing an effective date.

62

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

64

65 **Section 1. Paragraphs (a), (c), (e), and (g) of subsection
66 (1), subsections (2) and (4), paragraph (b) of subsection (5),
67 and subsection (7) of section 119.0725, Florida Statutes, are
68 amended, and new paragraphs (g) and (i) are added to subsection
69 (1) of that section, to read:**

70 119.0725 Agency cybersecurity information; public records
71 exemption; public meetings exemption.—

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

73 (a) "Breach" means unauthorized access of data or
74 ~~information in electronic form containing personal information.~~
75 Good faith access of data or information ~~personal information~~ by

76 an employee or agent of an agency does not constitute a breach,
77 provided that the data or information is not used for a purpose
78 unrelated to the business or subject to further unauthorized
79 use.

80 (c) "Cybersecurity" means the protection afforded to
81 information technology or operational technology in order to
82 attain the applicable objectives of preserving the
83 confidentiality, integrity, and availability of those
84 technologies, data, and information has the same meaning as in
85 s. 282.0041.

86 (e) "Incident" means a violation or imminent threat of
87 violation, whether such violation is accidental or deliberate,
88 of an agency's cybersecurity, information technology resources,
89 or operational technology security, policies, or practices. As
90 used in this paragraph, the term "imminent threat of violation"
91 means a situation in which the agency has a factual basis for
92 believing that a specific incident is about to occur.

93 (g) "Login credentials" means information used to
94 authenticate a user's identity or otherwise authorize access
95 when logging into a computer, computer system, computer network,
96 electronic device, or an online user account accessible over the
97 Internet through a mobile device, a website, or any other
98 electronic means, or for authentication or password or account
99 recovery.

100 (h)-(g) "Operational technology" means the hardware and

101 software that cause or detect a change through the direct
102 monitoring or control of physical devices, systems, processes,
103 or events.

104 (i) "Public-facing portal" means a web portal or computer
105 application accessible by the public over the Internet, whether
106 through a mobile device, website, or other electronic means.

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

110 ~~(a) Coverage limits and deductible or self-insurance~~
111 ~~amounts of insurance or other risk mitigation coverages acquired~~
112 ~~for the protection of information technology systems,~~
113 ~~operational technology systems, or data of an agency.~~

114 (a) (b) Information relating to critical infrastructure.

115 (b) (e) Cybersecurity incident information reported
116 pursuant to s. 282.318 or s. 282.3185.

117 (c) (d) Network schematics, hardware and software
118 configurations, or encryption information, or any information
119 that identifies detection, investigation, or response practices
120 related to for suspected or confirmed cybersecurity incidents,
121 including suspected or confirmed breaches, if the disclosure of
122 such information could would facilitate unauthorized access to
123 or unauthorized modification, disclosure, or destruction of
124 data, information, or existing or proposed information
125 technology or operational technology.

126 (d) Information relating to processes or practices
127 designed to protect data, information, or existing or proposed
128 information technology or operational technology if the
129 disclosure of such information could facilitate unauthorized
130 access to or unauthorized modification, disclosure, or
131 destruction of such data, information, or technology.

132 (e) Portions of risk assessments, evaluations, audits, and
133 other reports of an agency's cybersecurity program if the
134 disclosure of such information could facilitate unauthorized
135 access to or unauthorized modification, disclosure, or
136 destruction of data, information, or existing or proposed
137 information technology or operational technology.

138 (f) Login credentials.

139 (g) Internet protocol addresses, geolocation data, and
140 other information that describes the location, computer,
141 computer system, or computer network from which a user accesses
142 a public-facing portal, and the dates and times that a user
143 accesses a public-facing portal.

144 (h) Agency-produced data processing software that is
145 sensitive.

146 (i) Insurance and self-insurance coverage limits and
147 deductibles, as well as any other risk mitigation coverages,
148 acquired for the protection of information technology,
149 operational technology, or data of an agency.‡

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

151 2. ~~Information technology resources, which include an~~
152 ~~agency's existing or proposed information technology systems.~~

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

156 (5)

157 (b) Such confidential and exempt information may be
158 disclosed by an agency in the furtherance of its official duties
159 and responsibilities or to another agency or governmental entity
160 in the furtherance of the agency's or governmental entity's
161 official its statutory duties and responsibilities.

162 (7) This section is subject to the Open Government Sunset
163 Review Act in accordance with s. 119.15 and shall stand repealed
164 on October 2, 2031 ~~October 2, 2026~~, unless reviewed and saved
165 from repeal through reenactment by the Legislature.

166 **Section 2. Paragraph (c) of subsection (3) of section**
167 **15.16, Florida Statutes, is amended to read:**

168 15.16 Reproduction of records; admissibility in evidence;
169 electronic receipt and transmission of records; certification;
170 acknowledgment.—

171 (3)

172 (c)1. E-mail addresses collected by the Department of
173 State pursuant to this subsection are exempt from s. 119.07(1)
174 and s. 24(a), Art. I of the State Constitution. This exemption
175 applies to e-mail addresses held by the Department of State

176 before, on, or after the effective date of the exemption.

177 ~~2. Secure login credentials held by the Department of~~
178 ~~State for the purpose of allowing a person to electronically~~
179 ~~file records under this subsection are exempt from s. 119.07(1)~~
180 ~~and s. 24(a), Art. I of the State Constitution. This exemption~~
181 ~~applies to secure login credentials held by the Department of~~
182 ~~State before, on, or after the effective date of the exemption.~~
183 For purposes of this subparagraph, the term "secure login
184 ~~credentials" means information held by the department for~~
185 ~~purposes of authenticating a user logging into a user account on~~
186 ~~a computer, a computer system, a computer network, or an~~
187 ~~electronic device; an online user account accessible over the~~
188 ~~Internet, whether through a mobile device, a website, or any~~
189 ~~other electronic means; or information used for authentication~~
190 ~~or password recovery.~~

191 2.3. This paragraph is subject to the Open Government
192 Sunset Review Act in accordance with s. 119.15 and shall stand
193 repealed on October 2, 2028, unless reviewed and saved from
194 repeal through reenactment by the Legislature.

195 **Section 3. Paragraph (a) of subsection (1) of section**
196 **24.1051, Florida Statutes, is amended to read:**

197 24.1051 Exemptions from inspection or copying of public
198 records.—

199 (1) (a) The following information held by the department is
200 confidential and exempt from s. 119.07(1) and s. 24(a), Art. I

HB 7023

2026

201 of the State Constitution:

202 1. Information that, if released, could harm the security
203 or integrity of the department, including:

204 ~~a. Information relating to the security of the department's technologies, processes, and practices designed to protect networks, computers, data processing software, data, and data systems from attack, damage, or unauthorized access. This sub-subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2027, unless reviewed and saved from repeal through reenactment by the Legislature.~~

212 ~~a.b.~~ Security information or information that would reveal security measures of the department, whether physical or virtual.

215 ~~b.e.~~ Information about lottery games, promotions, tickets, and ticket stock, including information concerning the description, design, production, printing, packaging, shipping, delivery, storage, and validation of such games, promotions, tickets, and stock.

220 ~~c.d.~~ Information concerning terminals, machines, and devices that issue tickets.

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

225 3. Personal identifying information obtained by the

HB 7023

2026

226 department when processing background investigations of current
227 or potential retailers or vendors.

228 4. Financial information about an entity which is not
229 publicly available and is provided to the department in
230 connection with its review of the financial responsibility of
231 the entity pursuant to s. 24.111 or s. 24.112, provided that the
232 entity marks such information as confidential. However,
233 financial information related to any contract or agreement, or
234 an addendum thereto, with the department, including the amount
235 of money paid, any payment structure or plan, expenditures,
236 incentives, bonuses, fees, and penalties, shall be public
237 record.

238 **Section 4. Paragraph (d) of subsection (1) of section
239 101.5607, Florida Statutes, is amended to read:**

240 101.5607 Department of State to maintain voting system
241 information; prepare software.—

242 (1)

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

245 **Section 5. Section 106.0706, Florida Statutes, is amended
246 to read:**

247 106.0706 Electronic filing of campaign finance reports;
248 public records exemption.—

249 ~~(1) All user identifications and passwords held by the
250 Department of State pursuant to s. 106.0705 are confidential and~~

HB 7023

2026

251 exempt from s. 119.07(1) and s. 24(a), Art. I of the State
252 ~~Constitution.~~

253 ~~(1)-(2)-(a)~~ Information entered in the electronic filing
254 system for purposes of generating a report pursuant to s.
255 106.0705 is exempt from s. 119.07(1) and s. 24(a), Art. I of the
256 State Constitution.

257 ~~(2)-(b)~~ Information entered in the electronic filing system
258 is no longer exempt once the report is generated and filed with
259 the Division of Elections.

260 **Section 6. Subsection (6) of section 112.31446, Florida
261 Statutes, is amended to read:**

262 112.31446 Electronic filing system for financial
263 disclosure.—

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

268 ~~(b)~~ Information entered in the electronic filing system
269 for purposes of financial disclosure is exempt from s. 119.07(1)
270 and s. 24(a), Art. I of the State Constitution. Information
271 entered in the electronic filing system is no longer exempt once
272 the disclosure of financial interests or statement of financial
273 interests is submitted to the commission or, in the case of a
274 candidate, filed with a qualifying officer, whichever occurs
275 first.

HB 7023

2026

276 **Section 7. Paragraph (g) of subsection (1) of section**
277 **119.07, Florida Statutes, is amended to read:**

278 119.07 Inspection and copying of records; photographing
279 public records; fees; exemptions.—

280 (1)

281 (g) In any civil action in which an exemption to this
282 section is asserted, if the exemption is alleged to exist under
283 or by virtue of s. 119.071(1) (d) ~~or (f)~~, (2) (d), (e), or (f), or
284 (4) (c) or s. 119.0725(2) (h), the public record or part thereof
285 in question shall be submitted to the court for an inspection in
286 camera. If an exemption is alleged to exist under or by virtue
287 of s. 119.071(2) (c), an inspection in camera is discretionary
288 with the court. If the court finds that the asserted exemption
289 is not applicable, it shall order the public record or part
290 thereof in question to be immediately produced for inspection or
291 copying as requested by the person seeking such access.

292 **Section 8. Paragraph (f) of subsection (1) of section**
293 **119.071, Florida Statutes, is amended to read:**

294 119.071 General exemptions from inspection or copying of
295 public records.—

296 (1) AGENCY ADMINISTRATION.—

297 ~~(f) Agency-produced data processing software that is~~
298 ~~sensitive is exempt from s. 119.07(1) and s. 24(a), Art. I of~~
299 ~~the State Constitution. The designation of agency-produced~~
300 ~~software as sensitive does not prohibit an agency head from~~

301 sharing or exchanging such software with another public agency.

302 **Section 9. Paragraph (f) of subsection (2) of section**
303 **119.0712, Florida Statutes, is amended to read:**

304 119.0712 Executive branch agency-specific exemptions from
305 inspection or copying of public records.—

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

307 (f) 1. ~~Secure login credentials held by the Department of~~
308 ~~Highway Safety and Motor Vehicles are exempt from s. 119.07(1)~~
309 ~~and s. 24(a), Art. I of the State Constitution. This exemption~~
310 ~~applies to secure login credentials held by the department~~
311 ~~before, on, or after the effective date of the exemption. For~~
312 ~~purposes of this subparagraph, the term "secure login~~
313 ~~credentials" means information held by the department for~~
314 ~~purposes of authenticating a user logging into a user account on~~
315 ~~a computer, a computer system, a computer network, or an~~
316 ~~electronic device; an online user account accessible over the~~
317 ~~Internet, whether through a mobile device, a website, or any~~
318 ~~other electronic means; or information used for authentication~~
319 ~~or password recovery.~~

320 2. ~~Internet protocol addresses, geolocation data, and~~
321 ~~other information held by the Department of Highway Safety and~~
322 ~~Motor Vehicles which describes the location, computer, computer~~
323 ~~system, or computer network from which a user accesses a public~~
324 ~~facing portal, and the dates and times that a user accesses a~~
325 ~~public-facing portal, are exempt from s. 119.07(1) and s. 24(a),~~

326 ~~Art. I of the State Constitution. This exemption applies to such~~
327 ~~information held by the department before, on, or after the~~
328 ~~effective date of the exemption. For purposes of this~~
329 ~~subparagraph, the term "public-facing portal" means a web portal~~
330 ~~or computer application accessible by the public over the~~
331 ~~Internet, whether through a mobile device, website, or other~~
332 ~~electronic means, which is established for administering chapter~~
333 ~~319, chapter 320, chapter 322, chapter 328, or any other~~
334 ~~provision of law conferring duties upon the department.~~

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

339 **Section 10. Subsection (5) of section 119.0713, Florida**
340 **Statutes, is amended to read:**

341 119.0713 Local government agency exemptions from
342 inspection or copying of public records.—

343 (5) ~~(a) Customer meter-derived data and billing information~~
344 ~~in increments less than one billing cycle~~ ~~The following~~
345 ~~information held by a utility owned or operated by a unit of~~
346 ~~local government is exempt from s. 119.07(1) and s. 24(a), Art.~~
347 ~~I of the State Constitution.~~ ~~÷~~

348 1. ~~Information related to the security of the technology,~~
349 ~~processes, or practices of a utility owned or operated by a unit~~
350 ~~of local government that are designed to protect the utility's~~

351 networks, computers, programs, and data from attack, damage, or
352 unauthorized access, which information, if disclosed, would
353 facilitate the alteration, disclosure, or destruction of such
354 data or information technology resources.

355 2. Information related to the security of existing or
356 proposed information technology systems or industrial control
357 technology systems of a utility owned or operated by a unit of
358 local government, which, if disclosed, would facilitate
359 unauthorized access to, and alteration or destruction of, such
360 systems in a manner that would adversely impact the safe and
361 reliable operation of the systems and the utility.

362 3. Customer meter derived data and billing information in
363 increments less than one billing cycle.

364 (b) This exemption applies to such information held by a
365 utility owned or operated by a unit of local government before,
366 on, or after the effective date of this exemption.

367 (e) This subsection is Subparagraphs (a)1. and 2. are
368 subject to the Open Government Sunset Review Act in accordance
369 with s. 119.15 and shall stand repealed on October 2, 2027,
370 unless reviewed and saved from repeal through reenactment by the
371 Legislature.

372 **Section 11. Paragraph (b) of subsection (1) of section
373 119.0714, Florida Statutes, is amended to read:**

374 119.0714 Court files; court records; official records.—

375 (1) COURT FILES.—Nothing in this chapter shall be

376 construed to exempt from s. 119.07(1) a public record that was
377 made a part of a court file and that is not specifically closed
378 by order of court, except:

379 (b) Data processing software as provided in s.
380 119.0725(2)(h) s. 119.071(1)(f).

381 **Section 12. Subsection (10) of section 282.318, Florida**
382 **Statutes, is renumbered as subsection (5), and paragraphs (d),**
383 **(e), and (g) of subsection (4) and present subsections (5)**
384 **through (9) of that section are amended, to read:**

385 282.318 Cybersecurity.—

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

387 (d) Conduct, and update every 3 years, a comprehensive
388 risk assessment, which may be completed by a private sector
389 vendor, to determine the security threats to the data,
390 information, and information technology resources, including
391 mobile devices and print environments, of the agency. The risk
392 assessment must comply with the risk assessment methodology
393 developed by the department ~~and is confidential and exempt from~~
394 ~~s. 119.07(1), except that such information shall be available to~~
395 ~~the Auditor General, the Florida Digital Service within the~~
396 ~~department, the Cybercrime Office of the Department of Law~~
397 ~~Enforcement, and, for state agencies under the jurisdiction of~~
398 ~~the Governor, the Chief Inspector General.~~ If a private sector
399 vendor is used to complete a comprehensive risk assessment, it
400 must attest to the validity of the risk assessment findings.

401 (e) Develop, and periodically update, written internal
402 policies and procedures, which include procedures for reporting
403 cybersecurity incidents and breaches to the Cybercrime Office of
404 the Department of Law Enforcement and the Florida Digital
405 Service within the department. Such policies and procedures must
406 be consistent with the rules, guidelines, and processes
407 established by the department to ensure the security of the
408 data, information, and information technology resources of the
409 agency. ~~The internal policies and procedures that, if disclosed,~~
410 ~~could facilitate the unauthorized modification, disclosure, or~~
411 ~~destruction of data or information technology resources are~~
412 ~~confidential information and exempt from s. 119.07(1), except~~
413 ~~that such information shall be available to the Auditor General,~~
414 ~~the Cybercrime Office of the Department of Law Enforcement, the~~
415 ~~Florida Digital Service within the department, and, for state~~
416 ~~agencies under the jurisdiction of the Governor, the Chief~~
417 ~~Inspector General.~~

418 (g) Ensure that periodic internal audits and evaluations
419 of the agency's cybersecurity program for the data, information,
420 and information technology resources of the agency are
421 conducted. ~~The results of such audits and evaluations are~~
422 ~~confidential information and exempt from s. 119.07(1), except~~
423 ~~that such information shall be available to the Auditor General,~~
424 ~~the Cybercrime Office of the Department of Law Enforcement, the~~
425 ~~Florida Digital Service within the department, and, for agencies~~

426 under the jurisdiction of the Governor, the Chief Inspector
427 General.

428 (5) The portions of risk assessments, evaluations,
429 external audits, and other reports of a state agency's
430 cybersecurity program for the data, information, and information
431 technology resources of the state agency which are held by a
432 state agency are confidential and exempt from s. 119.07(1) and
433 s. 24(a), Art. I of the State Constitution if the disclosure of
434 such portions of records would facilitate unauthorized access to
435 or the unauthorized modification, disclosure, or destruction of:

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

437 (b) Information technology resources, which include:

438 1. Information relating to the security of the agency's
439 technologies, processes, and practices designed to protect
440 networks, computers, data processing software, and data from
441 attack, damage, or unauthorized access; or

442 2. Security information, whether physical or virtual,
443 which relates to the agency's existing or proposed information
444 technology systems.

445

446 For purposes of this subsection, "external audit" means an audit
447 that is conducted by an entity other than the state agency that
448 is the subject of the audit.

449 (6) Those portions of a public meeting as specified in s.
450 286.011 which would reveal records which are confidential and

451 exempt under subsection (5) are exempt from s. 286.011 and s.
452 24(b), Art. I of the State Constitution. No exempt portion of an
453 exempt meeting may be off the record. All exempt portions of
454 such meeting shall be recorded and transcribed. Such recordings
455 and transcripts are confidential and exempt from disclosure
456 under s. 119.07(1) and s. 24(a), Art. I of the State
457 Constitution unless a court of competent jurisdiction, after an
458 in camera review, determines that the meeting was not restricted
459 to the discussion of data and information made confidential and
460 exempt by this section. In the event of such a judicial
461 determination, only that portion of the recording and transcript
462 which reveals nonexempt data and information may be disclosed to
463 a third party.

464 (7) The portions of records made confidential and exempt
465 in subsections (5) and (6) shall be available to the Auditor
466 General, the Cybercrime Office of the Department of Law
467 Enforcement, the Florida Digital Service within the department,
468 and, for agencies under the jurisdiction of the Governor, the
469 Chief Inspector General. Such portions of records may be made
470 available to a local government, another state agency, or a
471 federal agency for cybersecurity purposes or in furtherance of
472 the state agency's official duties.

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

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

480 **Section 13.** Section 627.352, Florida Statutes, is
481 repealed.

482 **Section 14.** Section 1004.055, Florida Statutes, is
483 repealed.

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

488 (a) Network schematics, hardware and software
489 configurations, encryption information, or any information that
490 identifies detection, investigation, or response practices
491 relating to cybersecurity incidents, including breaches, if the
492 disclosure of such information could facilitate unauthorized
493 access to or unauthorized modification, disclosure, or
494 destruction of data, information, or existing or proposed
495 information technology or operational technology.

496 (b) Information relating to processes or practices
497 designed to protect data, information, or existing or proposed
498 information technology or operational technology if the
499 disclosure of such information could facilitate unauthorized
500 access to or unauthorized modification, disclosure, or

501 destruction of such data, information, or technology.

502 (c) Portions of risk assessments, evaluations, audits, and
503 other reports of an agency's cybersecurity program if the
504 disclosure of such information could facilitate unauthorized
505 access to or unauthorized modification, disclosure, or
506 destruction of data, information, or existing or proposed
507 information technology or operational technology.

508 (d) Login credentials.

509 (e) Internet protocol addresses, geolocation data, and
510 other information that describes the location, computer,
511 computer system, or computer network from which a user accesses
512 a public-facing portal, and the dates and times that a user
513 accesses a public-facing portal.

514 (f) Agency-produced data processing software that is
515 sensitive.

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

520
521 Release of such information could place an agency at greater
522 risk of breaches, cybersecurity incidents, and ransomware
523 attacks. Network schematics, hardware and software
524 configurations, encryption information, or any information that
525 identifies detection, investigation, or response practices for

526 cybersecurity incidents, including breaches reveal how an
527 agency's information technology and operational technology
528 systems are structured and defended. Disclosure of such
529 information could enable a malicious actor to map system
530 architecture, identify vulnerabilities, and bypass security
531 controls. Information describing processes or practices designed
532 to protect data, information, or existing or proposed
533 information technology or operational technology could similarly
534 be used to exploit weaknesses and predict defensive actions.
535 Portions of risk assessments, evaluations, audits, and other
536 reports of an agency's cybersecurity program routinely include
537 descriptions of vulnerabilities, testing results, and
538 recommendations. Disclosure of such information would
539 substantially increase the likelihood of a successful
540 cyberattack. Login credentials are a foundational security
541 control and disclosure of such information could allow malicious
542 actors to authenticate into government systems, impersonate
543 legitimate users, and access personal identifying and other
544 sensitive information. Internet protocol addresses, geolocation
545 data, and other information which describes the location,
546 computer, computer system, or computer network from which a user
547 accesses a public-facing portal, and the dates and times that a
548 user accesses a public-facing portal could be used to track
549 usage patterns, identify remote access points, or monitor portal
550 vulnerabilities. Sensitive agency-produced data processing

551 software can reveal the inner workings of security controls,
552 authentication mechanisms, or automated processes that malicious
553 actors can use to exploit weaknesses in security measures. If
554 information related to coverage limits and deductibles of
555 cybersecurity insurance were disclosed, it could give
556 cybercriminals an understanding of the monetary sum an agency
557 can afford or may be willing to pay as a result of a ransomware
558 attack at the expense of the taxpayer. Accordingly, the
559 Legislature finds that the disclosure of such sensitive
560 cybersecurity-related information would significantly impair the
561 administration of vital governmental programs.

562 (2) The Legislature also finds that it is a public
563 necessity that any portion of a meeting that would reveal the
564 confidential and exempt information by made exempt from s.
565 286.011, Florida Statutes, and s. 24(b), Article I of the State
566 Constitution, and that any recordings and transcripts of the
567 closed portion of a meeting be made confidential and exempt from
568 s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the
569 State Constitution. The failure to close that portion of a
570 meeting at which confidential and exempt information would be
571 revealed, and prevent the disclosure of the recordings and
572 transcripts of those portions of a meeting, would defeat the
573 purpose of the underlying public records exemption and could
574 result in the release of highly sensitive information related to
575 the cybersecurity of an agency system.

576 (3) For these reasons, the Legislature finds that these
577 public records and public meetings exemptions are of the utmost
578 importance and are a public necessity.

579 **Section 16.** This act shall take effect upon becoming a
580 law.