

1                   A bill to be entitled  
2           An act relating to cybersecurity; amending s. 20.055,  
3           F.S.; requiring certain audit plans of an inspector  
4           general to include certain information; amending s.  
5           282.0041, F.S.; revising and providing definitions;  
6           amending ss. 282.0051, 282.201, and 282.206, F.S.;  
7           revising provisions to replace references to  
8           information technology security with cybersecurity;  
9           amending s. 282.318, F.S.; revising provisions to  
10          replace references to information technology security  
11          and computer security with references to  
12          cybersecurity; revising a short title; providing that  
13          the Department of Management Services, acting through  
14          the Florida Digital Service, is the lead entity for  
15          the purpose of certain responsibilities; providing and  
16          revising requirements for the department, acting  
17          through the Florida Digital Service; providing that  
18          the state chief information security officer is  
19          responsible for state technology systems and shall be  
20          notified of certain incidents and threats; revising  
21          requirements for state agency heads; requiring the  
22          department, through the Florida Digital Service, to  
23          track the implementation by state agencies of certain  
24          plans; creating 282.319, F.S.; creating the Florida  
25          Cybersecurity Advisory Council within the Department

26 of Management Services; providing the purpose of the  
27 council; requiring the council to provide certain  
28 assistance to the Florida Digital Service; providing  
29 for the membership of the council; providing for terms  
30 of council members; providing that the Secretary of  
31 Management Services, or his or her designee, shall  
32 serve as the ex officio executive director of the  
33 council; providing that members shall serve without  
34 compensation but are entitled to reimbursement for per  
35 diem and travel expenses; requiring council members to  
36 maintain the confidential or exempt status of  
37 information received; prohibiting council members from  
38 using certain information for their own personal gain;  
39 requiring council members to sign an agreement  
40 acknowledging certain provisions; requiring the  
41 council to meet at least quarterly for certain  
42 purposes; requiring the council to work with certain  
43 entities to identify certain local infrastructure  
44 sectors and critical cyber infrastructure; requiring  
45 the council to submit an annual report to the  
46 Legislature; providing an effective date.

47  
48 Be It Enacted by the Legislature of the State of Florida:

49  
50 Section 1. Paragraph (i) of subsection (6) of section

51 20.055, Florida Statutes, is amended to read:

52 20.055 Agency inspectors general.—

53 (6) In carrying out the auditing duties and  
54 responsibilities of this act, each inspector general shall  
55 review and evaluate internal controls necessary to ensure the  
56 fiscal accountability of the state agency. The inspector general  
57 shall conduct financial, compliance, electronic data processing,  
58 and performance audits of the agency and prepare audit reports  
59 of his or her findings. The scope and assignment of the audits  
60 shall be determined by the inspector general; however, the  
61 agency head may at any time request the inspector general to  
62 perform an audit of a special program, function, or  
63 organizational unit. The performance of the audit shall be under  
64 the direction of the inspector general, except that if the  
65 inspector general does not possess the qualifications specified  
66 in subsection (4), the director of auditing shall perform the  
67 functions listed in this subsection.

68 (i) The inspector general shall develop long-term and  
69 annual audit plans based on the findings of periodic risk  
70 assessments. The plan, where appropriate, should include  
71 postaudit samplings of payments and accounts. The plan shall  
72 show the individual audits to be conducted during each year and  
73 related resources to be devoted to the respective audits. The  
74 plan shall include a specific cybersecurity audit plan. The  
75 Chief Financial Officer, to assist in fulfilling the

76 | responsibilities for examining, auditing, and settling accounts,  
 77 | claims, and demands pursuant to s. 17.03(1), and examining,  
 78 | auditing, adjusting, and settling accounts pursuant to s. 17.04,  
 79 | may use audits performed by the inspectors general and internal  
 80 | auditors. For state agencies under the jurisdiction of the  
 81 | Governor, the audit plans shall be submitted to the Chief  
 82 | Inspector General. The plan shall be submitted to the agency  
 83 | head for approval. A copy of the approved plan shall be  
 84 | submitted to the Auditor General.

85 | Section 2. Subsections (8) through (21) of section  
 86 | 282.0041, Florida Statutes, are renumbered as subsections (9)  
 87 | through (22), respectively, present subsection (22) is amended,  
 88 | and a new subsection (8) is added to that section, to read:

89 | 282.0041 Definitions.—As used in this chapter, the term:

90 | (8) "Cybersecurity" means the protection afforded to an  
 91 | automated information system in order to attain the applicable  
 92 | objectives of preserving the confidentiality, integrity, and  
 93 | availability of data, information, and information technology  
 94 | resources.

95 | ~~(22) "Information technology security" means the~~  
 96 | ~~protection afforded to an automated information system in order~~  
 97 | ~~to attain the applicable objectives of preserving the integrity,~~  
 98 | ~~availability, and confidentiality of data, information, and~~  
 99 | ~~information technology resources.~~

100 | Section 3. Paragraph (j) of subsection (1) of section

101 282.0051, Florida Statutes, is amended to read:

102 282.0051 Department of Management Services; Florida  
103 Digital Service; powers, duties, and functions.—

104 (1) The Florida Digital Service has been created within  
105 the department to propose innovative solutions that securely  
106 modernize state government, including technology and information  
107 services, to achieve value through digital transformation and  
108 interoperability, and to fully support the cloud-first policy as  
109 specified in s. 282.206. The department, through the Florida  
110 Digital Service, shall have the following powers, duties, and  
111 functions:

112 (j) Provide operational management and oversight of the  
113 state data center established pursuant to s. 282.201, which  
114 includes:

115 1. Implementing industry standards and best practices for  
116 the state data center's facilities, operations, maintenance,  
117 planning, and management processes.

118 2. Developing and implementing cost-recovery mechanisms  
119 that recover the full direct and indirect cost of services  
120 through charges to applicable customer entities. Such cost-  
121 recovery mechanisms must comply with applicable state and  
122 federal regulations concerning distribution and use of funds and  
123 must ensure that, for any fiscal year, no service or customer  
124 entity subsidizes another service or customer entity. The  
125 Florida Digital Service may recommend other payment mechanisms

126 | to the Executive Office of the Governor, the President of the  
127 | Senate, and the Speaker of the House of Representatives. Such  
128 | mechanism may be implemented only if specifically authorized by  
129 | the Legislature.

130 |       3. Developing and implementing appropriate operating  
131 | guidelines and procedures necessary for the state data center to  
132 | perform its duties pursuant to s. 282.201. The guidelines and  
133 | procedures must comply with applicable state and federal laws,  
134 | regulations, and policies and conform to generally accepted  
135 | governmental accounting and auditing standards. The guidelines  
136 | and procedures must include, but need not be limited to:

137 |       a. Implementing a consolidated administrative support  
138 | structure responsible for providing financial management,  
139 | procurement, transactions involving real or personal property,  
140 | human resources, and operational support.

141 |       b. Implementing an annual reconciliation process to ensure  
142 | that each customer entity is paying for the full direct and  
143 | indirect cost of each service as determined by the customer  
144 | entity's use of each service.

145 |       c. Providing rebates that may be credited against future  
146 | billings to customer entities when revenues exceed costs.

147 |       d. Requiring customer entities to validate that sufficient  
148 | funds exist in the appropriate data processing appropriation  
149 | category or will be transferred into the appropriate data  
150 | processing appropriation category before implementation of a

151 customer entity's request for a change in the type or level of  
152 service provided, if such change results in a net increase to  
153 the customer entity's cost for that fiscal year.

154 e. By November 15 of each year, providing to the Office of  
155 Policy and Budget in the Executive Office of the Governor and to  
156 the chairs of the legislative appropriations committees the  
157 projected costs of providing data center services for the  
158 following fiscal year.

159 f. Providing a plan for consideration by the Legislative  
160 Budget Commission if the cost of a service is increased for a  
161 reason other than a customer entity's request made pursuant to  
162 sub-subparagraph d. Such a plan is required only if the service  
163 cost increase results in a net increase to a customer entity for  
164 that fiscal year.

165 g. Standardizing and consolidating procurement and  
166 contracting practices.

167 4. In collaboration with the Department of Law  
168 Enforcement, developing and implementing a process for  
169 detecting, reporting, and responding to cybersecurity  
170 ~~information technology security~~ incidents, breaches, and  
171 threats.

172 5. Adopting rules relating to the operation of the state  
173 data center, including, but not limited to, budgeting and  
174 accounting procedures, cost-recovery methodologies, and  
175 operating procedures.

176 Section 4. Paragraph (g) of subsection (1) of section  
177 282.201, Florida Statutes, is amended to read:

178 282.201 State data center.—The state data center is  
179 established within the department. The provision of data center  
180 services must comply with applicable state and federal laws,  
181 regulations, and policies, including all applicable security,  
182 privacy, and auditing requirements. The department shall appoint  
183 a director of the state data center, preferably an individual  
184 who has experience in leading data center facilities and has  
185 expertise in cloud-computing management.

186 (1) STATE DATA CENTER DUTIES.—The state data center shall:

187 (g) In its procurement process, show preference for cloud-  
188 computing solutions that minimize or do not require the  
189 purchasing, financing, or leasing of state data center  
190 infrastructure, and that meet the needs of customer agencies,  
191 that reduce costs, and that meet or exceed the applicable state  
192 and federal laws, regulations, and standards for cybersecurity  
193 ~~information technology security~~.

194 Section 5. Subsection (2) of section 282.206, Florida  
195 Statutes, is amended to read:

196 282.206 Cloud-first policy in state agencies.—

197 (2) In its procurement process, each state agency shall  
198 show a preference for cloud-computing solutions that either  
199 minimize or do not require the use of state data center  
200 infrastructure when cloud-computing solutions meet the needs of



201 the agency, reduce costs, and meet or exceed the applicable  
202 state and federal laws, regulations, and standards for  
203 cybersecurity ~~information technology security~~.

204 Section 6. Section 282.318, Florida Statutes, is amended  
205 to read:

206 282.318 Cybersecurity ~~Security of data and information~~  
207 ~~technology~~.

208 (1) This section may be cited as the "State Cybersecurity  
209 Act." ~~"Information Technology Security Act."~~

210 (2) As used in this section, the term "state agency" has  
211 the same meaning as provided in s. 282.0041, except that the  
212 term includes the Department of Legal Affairs, the Department of  
213 Agriculture and Consumer Services, and the Department of  
214 Financial Services.

215 (3) The department, acting through the Florida Digital  
216 Service, is the lead entity responsible for establishing  
217 standards and processes for assessing state agency cybersecurity  
218 risks and determining appropriate security measures. Such  
219 standards and processes must be consistent with generally  
220 accepted technology best practices, including the National  
221 Institute for Standards and Technology Cybersecurity Framework,  
222 for cybersecurity. The department, acting through the Florida  
223 Digital Service, shall adopt ~~information technology security, to~~  
224 ~~include cybersecurity, and adopting~~ rules that mitigate risks;  
225 safeguard state agency digital assets, an agency's data,

226 information, and information technology resources to ensure  
227 availability, confidentiality, and integrity; and support a  
228 security governance framework ~~and to mitigate risks~~. The  
229 department, acting through the Florida Digital Service, shall  
230 also:

231 (a) Designate an employee of the Florida Digital Service  
232 as the state chief information security officer. The state chief  
233 information security officer must have experience and expertise  
234 in security and risk management for communications and  
235 information technology resources. The state chief information  
236 security officer is responsible for the development, operation,  
237 and oversight of cybersecurity for state technology systems. The  
238 state chief information security officer shall be notified of  
239 all confirmed or suspected incidents or threats of state agency  
240 information technology resources and must report such incidents  
241 or threats to the state chief information officer and the  
242 Governor.

243 (b) Develop, and annually update by February 1, a  
244 statewide cybersecurity information technology security  
245 strategic plan that includes security goals and objectives for  
246 cybersecurity, including the identification and mitigation of  
247 risk, proactive protections against threats, tactical risk  
248 detection, threat reporting, and response and recovery protocols  
249 for a cyber incident ~~the strategic issues of information~~  
250 ~~technology security policy, risk management, training, incident~~

251 ~~management, and disaster recovery planning.~~

252 (c) Develop and publish for use by state agencies a  
253 cybersecurity governance ~~an information technology security~~  
254 framework that, at a minimum, includes guidelines and processes  
255 for:

256 1. Establishing asset management procedures to ensure that  
257 an agency's information technology resources are identified and  
258 managed consistent with their relative importance to the  
259 agency's business objectives.

260 2. Using a standard risk assessment methodology that  
261 includes the identification of an agency's priorities,  
262 constraints, risk tolerances, and assumptions necessary to  
263 support operational risk decisions.

264 3. Completing comprehensive risk assessments and  
265 cybersecurity ~~information technology security~~ audits, which may  
266 be completed by a private sector vendor, and submitting  
267 completed assessments and audits to the department.

268 4. Identifying protection procedures to manage the  
269 protection of an agency's information, data, and information  
270 technology resources.

271 5. Establishing procedures for accessing information and  
272 data to ensure the confidentiality, integrity, and availability  
273 of such information and data.

274 6. Detecting threats through proactive monitoring of  
275 events, continuous security monitoring, and defined detection

276 processes.

277       7. Establishing agency cybersecurity ~~computer security~~  
278 incident response teams and describing their responsibilities  
279 for responding to cybersecurity ~~information technology security~~  
280 incidents, including breaches of personal information containing  
281 confidential or exempt data.

282       8. Recovering information and data in response to a  
283 cybersecurity ~~an information technology security~~ incident. The  
284 recovery may include recommended improvements to the agency  
285 processes, policies, or guidelines.

286       9. Establishing a cybersecurity ~~an information technology~~  
287 ~~security~~ incident reporting process that includes procedures and  
288 tiered reporting timeframes for notifying the department and the  
289 Department of Law Enforcement of cybersecurity ~~information~~  
290 ~~technology security~~ incidents. The tiered reporting timeframes  
291 shall be based upon the level of severity of the cybersecurity  
292 ~~information technology security~~ incidents being reported.

293       10. Incorporating information obtained through detection  
294 and response activities into the agency's cybersecurity  
295 ~~information technology security~~ incident response plans.

296       11. Developing agency strategic and operational  
297 cybersecurity ~~information technology security~~ plans required  
298 pursuant to this section.

299       12. Establishing the managerial, operational, and  
300 technical safeguards for protecting state government data and

301 information technology resources that align with the state  
302 agency risk management strategy and that protect the  
303 confidentiality, integrity, and availability of information and  
304 data.

305 13. Establishing procedures for procuring information  
306 technology commodities and services that require the commodity  
307 or service to meet the National Institute of Standards and  
308 Technology Cybersecurity Framework.

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

310 (e) In collaboration with the Cybercrime Office of the  
311 Department of Law Enforcement, annually provide training for  
312 state agency information security managers and computer security  
313 incident response team members that contains training on  
314 cybersecurity information technology security, including  
315 cybersecurity, threats, trends, and best practices.

316 (f) Annually review the strategic and operational  
317 cybersecurity information technology security plans of state  
318 executive branch agencies.

319 (g) Provide cybersecurity training to all state agency  
320 technology professionals that develops, assesses, and documents  
321 competencies by role and skill level. The training may be  
322 provided in collaboration with the Cybercrime Office of the  
323 Department of Law Enforcement, a private sector entity, or an  
324 institution of the state university system.

325 (h) Operate and maintain a Cybersecurity Operations Center

326 | led by the state chief information security officer, which must  
327 | be primarily virtual and staffed with tactical detection and  
328 | incident response personnel. The Cybersecurity Operations Center  
329 | shall serve as a clearinghouse for threat information and  
330 | coordinate with the Department of Law Enforcement to support  
331 | state agencies and their response to any confirmed or suspected  
332 | cybersecurity incident.

333 |       (i) Lead an Emergency Support Function, ESF CYBER, under  
334 | the state comprehensive emergency management plan as described  
335 | in s. 252.35.

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

337 |       (a) Designate an information security manager to  
338 | administer the cybersecurity ~~information technology security~~  
339 | program of the state agency. This designation must be provided  
340 | annually in writing to the department by January 1. A state  
341 | agency's information security manager, for purposes of these  
342 | information security duties, shall report directly to the agency  
343 | head.

344 |       (b) In consultation with the department, through the  
345 | Florida Digital Service, and the Cybercrime Office of the  
346 | Department of Law Enforcement, establish an agency cybersecurity  
347 | ~~computer security incident~~ response team to respond to a  
348 | cybersecurity ~~an information technology security~~ incident. The  
349 | agency cybersecurity ~~computer security incident~~ response team  
350 | shall convene upon notification of a cybersecurity ~~an~~

351 ~~information technology security~~ incident and must immediately  
352 report all confirmed or suspected incidents to the state chief  
353 information security officer, or his or her designee, and comply  
354 with all applicable guidelines and processes established  
355 pursuant to paragraph (3) (c).

356 (c) Submit to the department annually by July 31, the  
357 state agency's strategic and operational cybersecurity  
358 ~~information technology security~~ plans developed pursuant to  
359 rules and guidelines established by the department, through the  
360 Florida Digital Service.

361 1. The state agency strategic cybersecurity ~~information~~  
362 ~~technology security~~ plan must cover a 3-year period and, at a  
363 minimum, define security goals, intermediate objectives, and  
364 projected agency costs for the strategic issues of agency  
365 information security policy, risk management, security training,  
366 security incident response, and disaster recovery. The plan must  
367 be based on the statewide cybersecurity ~~information technology~~  
368 ~~security~~ strategic plan created by the department and include  
369 performance metrics that can be objectively measured to reflect  
370 the status of the state agency's progress in meeting security  
371 goals and objectives identified in the agency's strategic  
372 information security plan.

373 2. The state agency operational cybersecurity ~~information~~  
374 ~~technology security~~ plan must include a progress report that  
375 objectively measures progress made towards the prior operational

376 cybersecurity ~~information technology security~~ plan and a project  
377 plan that includes activities, timelines, and deliverables for  
378 security objectives that the state agency will implement during  
379 the current fiscal year.

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

394 (e) Develop, and periodically update, written internal  
395 policies and procedures, which include procedures for reporting  
396 cybersecurity ~~information technology security~~ incidents and  
397 breaches to the Cybercrime Office of the Department of Law  
398 Enforcement and the Florida Digital Service within the  
399 department. Such policies and procedures must be consistent with  
400 the rules, guidelines, and processes established by the



401 department to ensure the security of the data, information, and  
402 information technology resources of the agency. The internal  
403 policies and procedures that, if disclosed, could facilitate the  
404 unauthorized modification, disclosure, or destruction of data or  
405 information technology resources are confidential information  
406 and exempt from s. 119.07(1), except that such information shall  
407 be available to the Auditor General, the Cybercrime Office of  
408 the Department of Law Enforcement, the Florida Digital Service  
409 within the department, and, for state agencies under the  
410 jurisdiction of the Governor, the Chief Inspector General.

411 (f) Implement managerial, operational, and technical  
412 safeguards and risk assessment remediation plans recommended by  
413 the department to address identified risks to the data,  
414 information, and information technology resources of the agency.  
415 The department, through the Florida Digital Service, shall track  
416 implementation by state agencies upon development of such  
417 remediation plans in coordination with agency inspectors  
418 general.

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

426 Department of Law Enforcement, the Florida Digital Service  
427 within the department, and, for agencies under the jurisdiction  
428 of the Governor, the Chief Inspector General.

429 (h) Ensure that the ~~information technology security and~~  
430 cybersecurity requirements in both the written specifications  
431 for the solicitation, contracts, and service-level agreement of  
432 information technology and information technology resources and  
433 services meet or exceed the applicable state and federal laws,  
434 regulations, and standards for ~~information technology security~~  
435 ~~and cybersecurity,~~ including the National Institute of Standards  
436 and Technology Cybersecurity Framework. Service-level agreements  
437 must identify service provider and state agency responsibilities  
438 for privacy and security, protection of government data,  
439 personnel background screening, and security deliverables with  
440 associated frequencies.

441 (i) Provide ~~information technology security and~~  
442 cybersecurity awareness training to all state agency employees  
443 in the first 30 days after commencing employment concerning  
444 cybersecurity ~~information technology security~~ risks and the  
445 responsibility of employees to comply with policies, standards,  
446 guidelines, and operating procedures adopted by the state agency  
447 to reduce those risks. The training may be provided in  
448 collaboration with the Cybercrime Office of the Department of  
449 Law Enforcement, a private sector entity, or an institution of  
450 the state university system.

451 (j) Develop a process for detecting, reporting, and  
452 responding to threats, breaches, or cybersecurity information  
453 ~~technology security~~ incidents which is consistent with the  
454 security rules, guidelines, and processes established by the  
455 department through the Florida Digital Service.

456 1. All cybersecurity information ~~technology security~~  
457 incidents and breaches must be reported to the Florida Digital  
458 Service within the department and the Cybercrime Office of the  
459 Department of Law Enforcement and must comply with the  
460 notification procedures and reporting timeframes established  
461 pursuant to paragraph (3) (c).

462 2. For cybersecurity information ~~technology security~~  
463 breaches, state agencies shall provide notice in accordance with  
464 s. 501.171.

465 (5) Portions of records held by a state agency which  
466 contain network schematics, hardware and software  
467 configurations, or encryption, or which identify detection,  
468 investigation, or response practices for suspected or confirmed  
469 cybersecurity information ~~technology security~~ incidents,  
470 including suspected or confirmed breaches, are confidential and  
471 exempt from s. 119.07(1) and s. 24(a), Art. I of the State  
472 Constitution, if the disclosure of such records would facilitate  
473 unauthorized access to or the unauthorized modification,  
474 disclosure, or destruction of:

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

476 (b) Information technology resources, which includes:  
 477 1. Information relating to the security of the agency's  
 478 technologies, processes, and practices designed to protect  
 479 networks, computers, data processing software, and data from  
 480 attack, damage, or unauthorized access; or  
 481 2. Security information, whether physical or virtual,  
 482 which relates to the agency's existing or proposed information  
 483 technology systems.

484 (6) The portions of risk assessments, evaluations,  
 485 external audits, and other reports of a state agency's  
 486 cybersecurity ~~information technology security~~ program for the  
 487 data, information, and information technology resources of the  
 488 state agency which are held by a state agency are confidential  
 489 and exempt from s. 119.07(1) and s. 24(a), Art. I of the State  
 490 Constitution if the disclosure of such portions of records would  
 491 facilitate unauthorized access to or the unauthorized  
 492 modification, disclosure, or destruction of:

493 (a) Data or information, whether physical or virtual; or  
 494 (b) Information technology resources, which include:  
 495 1. Information relating to the security of the agency's  
 496 technologies, processes, and practices designed to protect  
 497 networks, computers, data processing software, and data from  
 498 attack, damage, or unauthorized access; or  
 499 2. Security information, whether physical or virtual,  
 500 which relates to the agency's existing or proposed information

501 | technology systems.

502 |

503 | For purposes of this subsection, "external audit" means an audit  
504 | that is conducted by an entity other than the state agency that  
505 | is the subject of the audit.

506 |         (7) Those portions of a public meeting as specified in s.  
507 | 286.011 which would reveal records which are confidential and  
508 | exempt under subsection (5) or subsection (6) are exempt from s.  
509 | 286.011 and s. 24(b), Art. I of the State Constitution. No  
510 | exempt portion of an exempt meeting may be off the record. All  
511 | exempt portions of such meeting shall be recorded and  
512 | transcribed. Such recordings and transcripts are confidential  
513 | and exempt from disclosure under s. 119.07(1) and s. 24(a), Art.  
514 | I of the State Constitution unless a court of competent  
515 | jurisdiction, after an in camera review, determines that the  
516 | meeting was not restricted to the discussion of data and  
517 | information made confidential and exempt by this section. In the  
518 | event of such a judicial determination, only that portion of the  
519 | recording and transcript which reveals nonexempt data and  
520 | information may be disclosed to a third party.

521 |         (8) The portions of records made confidential and exempt  
522 | in subsections (5), (6), and (7) shall be available to the  
523 | Auditor General, the Cybercrime Office of the Department of Law  
524 | Enforcement, the Florida Digital Service within the department,  
525 | and, for agencies under the jurisdiction of the Governor, the

526 Chief Inspector General. Such portions of records may be made  
527 available to a local government, another state agency, or a  
528 federal agency for cybersecurity ~~information technology security~~  
529 purposes or in furtherance of the state agency's official  
530 duties.

531 (9) The exemptions contained in subsections (5), (6), and  
532 (7) apply to records held by a state agency before, on, or after  
533 the effective date of this exemption.

534 (10) Subsections (5), (6), and (7) are subject to the Open  
535 Government Sunset Review Act in accordance with s. 119.15 and  
536 shall stand repealed on October 2, 2025, unless reviewed and  
537 saved from repeal through reenactment by the Legislature.

538 (11) The department shall adopt rules relating to  
539 cybersecurity ~~information technology security~~ and to administer  
540 this section.

541 Section 7. Section 282.319, Florida Statutes, is created  
542 to read:

543 282.319 Florida Cybersecurity Advisory Council.-

544 (1) The Florida Cybersecurity Advisory Council, an  
545 advisory council as defined in s. 20.03(7), is created within  
546 the department. Except as otherwise provided in this section,  
547 the advisory council shall operate in a manner consistent with  
548 s. 20.052.

549 (2) The purpose of the council is to assist state agencies  
550 in protecting their information technology resources from cyber

551 threats and incidents.

552 (3) The council shall assist the Florida Digital Service  
553 in implementing best cybersecurity practices, taking into  
554 consideration the final recommendations of the Florida  
555 Cybersecurity Task Force created under chapter 2019-118, Laws of  
556 Florida.

557 (4) The council shall be comprised of the following  
558 members:

559 (a) The Lieutenant Governor or his or her designee.

560 (b) The state chief information officer.

561 (c) The state chief information security officer.

562 (d) The director of the Division of Emergency Management  
563 or his or her designee.

564 (e) A representative of the computer crime center of the  
565 Department of Law Enforcement, appointed by the executive  
566 director of the Department of Law Enforcement.

567 (f) A representative of the Florida Fusion Center of the  
568 Department of Law Enforcement, appointed by the executive  
569 director of the Department of Law Enforcement.

570 (g) The Chief Inspector General.

571 (h) A representative from the Public Service Commission.

572 (i) Up to two representatives from institutions of higher  
573 education located in this state, appointed by the Governor.

574 (j) Three representatives from critical infrastructure  
575 sectors, one of which must be from a water treatment facility,

576 appointed by the Governor.

577 (k) Four representatives of the private sector with senior  
578 level experience in cybersecurity or software engineering from  
579 within the finance, energy, health care, and transportation  
580 sectors, appointed by the Governor.

581 (l) Two representatives with expertise on emerging  
582 technology, with one appointed by the President of the Senate  
583 and one appointed by the Speaker of the House of  
584 Representatives.

585 (5) Members shall serve for a term of 4 years; however,  
586 for the purpose of providing staggered terms, the initial  
587 appointments of members made by the Governor shall be for a term  
588 of 2 years. A vacancy shall be filled for the remainder of the  
589 unexpired term in the same manner as the initial appointment.  
590 All members of the council are eligible for reappointment.

591 (6) The Secretary of Management Services, or his or her  
592 designee, shall serve as the ex officio, nonvoting executive  
593 director of the council.

594 (7) Members of the council shall serve without  
595 compensation but are entitled to receive reimbursement for per  
596 diem and travel expenses pursuant to s. 112.061.

597 (8) Members of the council shall maintain the confidential  
598 or exempt status of information received in the performance of  
599 their duties and responsibilities as members of the council. In  
600 accordance with s. 112.313, a current or former member of the



601 council may not disclose or use information not available to the  
 602 general public and gained by reason of their official position,  
 603 except for information relating exclusively to governmental  
 604 practices, for their personal gain or benefit or for the  
 605 personal gain or benefit of any other person or business entity.  
 606 Members shall sign an agreement acknowledging the provisions of  
 607 this subsection.

608 (9) The council shall meet at least quarterly to:  
 609 (a) Review existing state agency cybersecurity policies.  
 610 (b) Assess ongoing risks to state agency information  
 611 technology.

612 (c) Recommend a reporting and information sharing system  
 613 to notify state agencies of new risks.

614 (d) Recommend data breach simulation exercises.

615 (e) Assist the Florida Digital Service in developing  
 616 cybersecurity best practice recommendations for state agencies  
 617 that include recommendations regarding:

618 1. Continuous risk monitoring.

619 2. Password management.

620 3. Protecting data in legacy and new systems.

621 (f) Examine inconsistencies between state and federal law  
 622 regarding cybersecurity.

623 (10) The council shall work with the National Institute of  
 624 Standards and Technology and other federal agencies, private  
 625 sector businesses, and private cybersecurity experts:

626        (a) For critical infrastructure not covered by federal  
627 law, to identify which local infrastructure sectors are at the  
628 greatest risk of cyber attacks and need the most enhanced  
629 cybersecurity measures.

630        (b) To use federal guidance to identify categories of  
631 critical infrastructure as critical cyber infrastructure if  
632 cyber damage or unauthorized cyber access to the infrastructure  
633 could reasonably result in catastrophic consequences.

634        (11) Beginning June 30, 2022, and each June 30 thereafter,  
635 the council shall submit to the President of the Senate and the  
636 Speaker of the House of Representatives any legislative  
637 recommendations considered necessary by the council to address  
638 cybersecurity.

639        Section 8. This act shall take effect July 1, 2021.