



410182

576-03929-21

Proposed Committee Substitute by the Committee on Appropriations
(Appropriations Subcommittee on Agriculture, Environment, and
General Government)

A bill to be entitled

An act relating to cybersecurity; amending s. 20.055,
F.S.; requiring certain audit plans of an inspector
general to include certain information; amending s.
282.0041, F.S.; revising and providing definitions;
amending ss. 282.0051, 282.201, and 282.206, F.S.;
revising provisions to replace references to
information technology security with cybersecurity;
amending s. 282.318, F.S.; revising provisions to
replace references to information technology security
and computer security with references to
cybersecurity; revising a short title; providing that
the Department of Management Services, acting through
the Florida Digital Service, is the lead entity for
the purpose of certain responsibilities; providing and
revising requirements for the department, acting
through the Florida Digital Service; providing that
the state chief information security officer is
responsible for state technology systems and shall be
notified of certain incidents and threats; revising
requirements for state agency heads; requiring the
department, through the Florida Digital Service, to
track the implementation by state agencies of certain
plans; creating s. 282.319, F.S.; creating the Florida
Cybersecurity Advisory Council within the Department
of Management Services; providing the purpose of the



410182

576-03929-21

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, nonvoting executive director
33 of the council; providing that members shall serve
34 without compensation but are entitled to reimbursement
35 for per diem and travel expenses; requiring council
36 members to maintain the confidential or exempt status
37 of information received; prohibiting council members
38 from using information not otherwise public for their
39 own personal gain; requiring council members to sign
40 an agreement acknowledging certain provisions;
41 requiring the council to meet at least quarterly for
42 certain purposes; requiring the council to work with
43 certain entities to identify certain local
44 infrastructure sectors and critical cyber
45 infrastructure; requiring the council to submit an
46 annual report to the Legislature; providing an
47 effective date.

48

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

50

51 Section 1. Paragraph (i) of subsection (6) of section
52 20.055, Florida Statutes, is amended to read:

53 20.055 Agency inspectors general.—

54 (6) In carrying out the auditing duties and
55 responsibilities of this act, each inspector general shall



410182

576-03929-21

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

69 (i) The inspector general shall develop long-term and
70 annual audit plans based on the findings of periodic risk
71 assessments. The plan, where appropriate, should include
72 postaudit samplings of payments and accounts. The plan shall
73 show the individual audits to be conducted during each year and
74 related resources to be devoted to the respective audits. The
75 plan shall include a specific cybersecurity audit plan. The
76 Chief Financial Officer, to assist in fulfilling the
77 responsibilities for examining, auditing, and settling accounts,
78 claims, and demands pursuant to s. 17.03(1), and examining,
79 auditing, adjusting, and settling accounts pursuant to s. 17.04,
80 may use audits performed by the inspectors general and internal
81 auditors. For state agencies under the jurisdiction of the
82 Governor, the audit plans shall be submitted to the Chief
83 Inspector General. The plan shall be submitted to the agency
84 head for approval. A copy of the approved plan shall be



410182

576-03929-21

85 submitted to the Auditor General.

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

91 282.0041 Definitions.—As used in this chapter, the term:

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

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

102 Section 3. Paragraph (j) of subsection (1) of section
103 282.0051, Florida Statutes, is amended to read:

104 282.0051 Department of Management Services; Florida Digital
105 Service; powers, duties, and functions.—

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



410182

576-03929-21

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

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

120 2. Developing and implementing cost-recovery mechanisms
121 that recover the full direct and indirect cost of services
122 through charges to applicable customer entities. Such cost-
123 recovery mechanisms must comply with applicable state and
124 federal regulations concerning distribution and use of funds and
125 must ensure that, for any fiscal year, no service or customer
126 entity subsidizes another service or customer entity. The
127 Florida Digital Service may recommend other payment mechanisms
128 to the Executive Office of the Governor, the President of the
129 Senate, and the Speaker of the House of Representatives. Such
130 mechanism may be implemented only if specifically authorized by
131 the Legislature.

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

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



410182

576-03929-21

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

147 c. Providing rebates that may be credited against future
148 billings to customer entities when revenues exceed costs.

149 d. Requiring customer entities to validate that sufficient
150 funds exist in the appropriate data processing appropriation
151 category or will be transferred into the appropriate data
152 processing appropriation category before implementation of a
153 customer entity's request for a change in the type or level of
154 service provided, if such change results in a net increase to
155 the customer entity's cost for that fiscal year.

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

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

167 g. Standardizing and consolidating procurement and
168 contracting practices.

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



410182

576-03929-21

172 incidents, breaches, and threats.

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

177 Section 4. Paragraph (g) of subsection (1) of section
178 282.201, Florida Statutes, is amended to read:

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

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

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

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

197 282.206 Cloud-first policy in state agencies.—

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



410182

576-03929-21

201 infrastructure when cloud-computing solutions meet the needs of
202 the agency, reduce costs, and meet or exceed the applicable
203 state and federal laws, regulations, and standards for
204 cybersecurity information technology security.

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

207 282.318 Cybersecurity Security of data and information
208 technology.-

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

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

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



410182

576-03929-21

230 department, acting through the Florida Digital Service, shall
231 also:

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

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

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

257 1. Establishing asset management procedures to ensure that
258 an agency's information technology resources are identified and



410182

576-03929-21

259 managed consistent with their relative importance to the
260 agency's business objectives.

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

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

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

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

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

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

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

287 9. Establishing a cybersecurity ~~an information technology~~



410182

576-03929-21

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

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

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

300 12. Establishing the managerial, operational, and technical
301 safeguards for protecting state government data and information
302 technology resources that align with the state agency risk
303 management strategy and that protect the confidentiality,
304 integrity, and availability of information and 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



410182

576-03929-21

317 cybersecurity information technology security plans of state
318 executive branch agencies.

319 (g) Provide cybersecurity training to all state agency
320 technology professionals which 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 administer
338 the cybersecurity information technology security program of the
339 state agency. This designation must be provided annually in
340 writing to the department by January 1. A state agency's
341 information security manager, for purposes of these information
342 security duties, shall report directly to the agency head.

343 (b) In consultation with the department, through the
344 Florida Digital Service, and the Cybercrime Office of the
345 Department of Law Enforcement, establish an agency cybersecurity



410182

576-03929-21

346 ~~computer security incident~~ response team to respond to a
347 cybersecurity ~~an information technology security~~ incident. The
348 agency cybersecurity ~~computer security incident~~ response team
349 shall convene upon notification of a cybersecurity ~~an~~
350 ~~information technology security~~ incident and must immediately
351 report all confirmed or suspected incidents to the state chief
352 information security officer, or his or her designee, and comply
353 with all applicable guidelines and processes established
354 pursuant to paragraph (3) (c).

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

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

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



410182

576-03929-21

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

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

393 (e) Develop, and periodically update, written internal
394 policies and procedures, which include procedures for reporting
395 cybersecurity information technology security incidents and
396 breaches to the Cybercrime Office of the Department of Law
397 Enforcement and the Florida Digital Service within the
398 department. Such policies and procedures must be consistent with
399 the rules, guidelines, and processes established by the
400 department to ensure the security of the data, information, and
401 information technology resources of the agency. The internal
402 policies and procedures that, if disclosed, could facilitate the
403 unauthorized modification, disclosure, or destruction of data or



410182

576-03929-21

404 information technology resources are confidential information
405 and exempt from s. 119.07(1), except that such information shall
406 be available to the Auditor General, the Cybercrime Office of
407 the Department of Law Enforcement, the Florida Digital Service
408 within the department, and, for state agencies under the
409 jurisdiction of the Governor, the Chief Inspector General.

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

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

428 (h) Ensure that the ~~information technology security and~~
429 cybersecurity requirements in both the written specifications
430 for the solicitation, contracts, and service-level agreement of
431 information technology and information technology resources and
432 services meet or exceed the applicable state and federal laws,



410182

576-03929-21

433 regulations, and standards for ~~information technology security~~
434 ~~and cybersecurity~~, including the National Institute of Standards
435 ~~and Technology Cybersecurity Framework~~. Service-level agreements
436 must identify service provider and state agency responsibilities
437 for privacy and security, protection of government data,
438 personnel background screening, and security deliverables with
439 associated frequencies.

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

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

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

461 2. For ~~cybersecurity information technology security~~



410182

576-03929-21

462 breaches, state agencies shall provide notice in accordance with
463 s. 501.171.

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

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

475 (b) Information technology resources, which includes:

476 1. Information relating to the security of the agency's
477 technologies, processes, and practices designed to protect
478 networks, computers, data processing software, and data from
479 attack, damage, or unauthorized access; or

480 2. Security information, whether physical or virtual, which
481 relates to the agency's existing or proposed information
482 technology systems.

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



410182

576-03929-21

491 modification, disclosure, or destruction of:

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

493 (b) Information technology resources, which include:

494 1. Information relating to the security of the agency's
495 technologies, processes, and practices designed to protect
496 networks, computers, data processing software, and data from
497 attack, damage, or unauthorized access; or

498 2. Security information, whether physical or virtual, which
499 relates to the agency's existing or proposed information
500 technology systems.

501

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

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



410182

576-03929-21

520 (8) The portions of records made confidential and exempt in
521 subsections (5), (6), and (7) shall be available to the Auditor
522 General, the Cybercrime Office of the Department of Law
523 Enforcement, the Florida Digital Service within the department,
524 and, for agencies under the jurisdiction of the Governor, the
525 Chief Inspector General. Such portions of records may be made
526 available to a local government, another state agency, or a
527 federal agency for cybersecurity ~~information technology security~~
528 purposes or in furtherance of the state agency's official
529 duties.

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

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

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

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

542 282.319 Florida Cybersecurity Advisory Council.-

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

548 (2) The purpose of the council is to assist state agencies



410182

576-03929-21

549 in protecting their information technology resources from cyber
550 threats and incidents.

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

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

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

559 (b) The state chief information officer.

560 (c) The state chief information security officer.

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

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

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

569 (g) The Chief Inspector General.

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

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

573 (j) Three representatives from critical infrastructure
574 sectors, one of which must be from a water treatment facility,
575 appointed by the Governor.

576 (k) Four representatives of the private sector with senior
577 level experience in cybersecurity or software engineering from



410182

576-03929-21

578 within the finance, energy, health care, and transportation
579 sectors, appointed by the Governor.

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

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

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

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

596 (8) Members of the council shall maintain the confidential
597 or exempt status of information received in the performance of
598 their duties and responsibilities as members of the council. In
599 accordance with s. 112.313, a current or former member of the
600 council may not disclose or use information not available to the
601 general public and gained by reason of their official position,
602 except for information relating exclusively to governmental
603 practices, for their personal gain or benefit or for the
604 personal gain or benefit of any other person or business entity.
605 Members shall sign an agreement acknowledging the provisions of
606 this subsection.



410182

576-03929-21

- 607 (9) The council shall meet at least quarterly to:
608 (a) Review existing state agency cybersecurity policies.
609 (b) Assess ongoing risks to state agency information
610 technology.
611 (c) Recommend a reporting and information sharing system to
612 notify state agencies of new risks.
613 (d) Recommend data breach simulation exercises.
614 (e) Assist the Florida Digital Service in developing
615 cybersecurity best practice recommendations for state agencies
616 which include recommendations regarding:
617 1. Continuous risk monitoring.
618 2. Password management.
619 3. Protecting data in legacy and new systems.
620 (f) Examine inconsistencies between state and federal law
621 regarding cybersecurity.
622 (10) The council shall work with the National Institute of
623 Standards and Technology and other federal agencies, private
624 sector businesses, and private cybersecurity experts:
625 (a) For critical infrastructure not covered by federal law,
626 to identify which local infrastructure sectors are at the
627 greatest risk of cyber attacks and need the most enhanced
628 cybersecurity measures.
629 (b) To use federal guidance to identify categories of
630 critical infrastructure as critical cyber infrastructure if
631 cyber damage or unauthorized cyber access to the infrastructure
632 could reasonably result in catastrophic consequences.
633 (11) Beginning June 30, 2022, and each June 30 thereafter,
634 the council shall submit to the President of the Senate and the
635 Speaker of the House of Representatives any legislative



410182

576-03929-21

636 recommendations considered necessary by the council to address
637 cybersecurity.

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