CS for SB 1900

**By** the Committee on Governmental Oversight and Accountability; and Senator Boyd

585-03626A-21 20211900c1 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 the Florida Digital Service, is the lead entity for 14 15 the purpose of certain responsibilities; providing and revising requirements for the department, acting 16 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 s. 282.319, F.S.; creating the Florida 25 Cybersecurity Advisory Council within the Department of Management Services; providing the purpose of the 2.6 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

### Page 1 of 22

	585-03626A-21 20211900c1
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 the
36	council to meet at least quarterly for certain
37	purposes; requiring the council to work with certain
38	entities to identify certain local infrastructure
39	sectors and critical cyber infrastructure; requiring
40	the council to submit an annual report to the
41	Legislature; providing an effective date.
42	
43	Be It Enacted by the Legislature of the State of Florida:
44	
45	Section 1. Paragraph (i) of subsection (6) of section
46	20.055, Florida Statutes, is amended to read:
47	20.055 Agency inspectors general
48	(6) In carrying out the auditing duties and
49	responsibilities of this act, each inspector general shall
50	review and evaluate internal controls necessary to ensure the
51	fiscal accountability of the state agency. The inspector general
52	shall conduct financial, compliance, electronic data processing,
53	and performance audits of the agency and prepare audit reports
54	of his or her findings. The scope and assignment of the audits
55	shall be determined by the inspector general; however, the
56	agency head may at any time request the inspector general to
57	perform an audit of a special program, function, or
58	organizational unit. The performance of the audit shall be under

# Page 2 of 22

CS for SB 1900

585-03626A-21 20211900c1 59 the direction of the inspector general, except that if the 60 inspector general does not possess the qualifications specified 61 in subsection (4), the director of auditing shall perform the 62 functions listed in this subsection. 63 (i) The inspector general shall develop long-term and annual audit plans based on the findings of periodic risk 64 65 assessments. The plan, where appropriate, should include 66 postaudit samplings of payments and accounts. The plan shall show the individual audits to be conducted during each year and 67 68 related resources to be devoted to the respective audits. The 69 plan shall include a specific cybersecurity audit plan. The 70 Chief Financial Officer, to assist in fulfilling the 71 responsibilities for examining, auditing, and settling accounts, 72 claims, and demands pursuant to s. 17.03(1), and examining, 73 auditing, adjusting, and settling accounts pursuant to s. 17.04, 74 may use audits performed by the inspectors general and internal 75 auditors. For state agencies under the jurisdiction of the 76 Governor, the audit plans shall be submitted to the Chief 77 Inspector General. The plan shall be submitted to the agency 78 head for approval. A copy of the approved plan shall be 79 submitted to the Auditor General. 80 Section 2. Present subsections (8) through (21) of section 81 282.0041, Florida Statutes, are redesignated as subsections (9)

82 through (22), respectively, a new subsection (8) is added to 83 that section, and present subsection (22) of that section is 84 amended, to read:

- 85
- 86

87

(8) "Cybersecurity" means the protection afforded to an automated information system in order to attain the applicable

### Page 3 of 22

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

	585-03626A-21 20211900c1
88	objectives of preserving the confidentiality, integrity, and
89	availability of data, information, and information technology
90	resources.
91	(22) "Information technology security" means the protection
92	afforded to an automated information system in order to attain
93	the applicable objectives of preserving the integrity,
94	availability, and confidentiality of data, information, and
95	information technology resources.
96	Section 3. Paragraph (j) of subsection (1) of section
97	282.0051, Florida Statutes, is amended to read:
98	282.0051 Department of Management Services; Florida Digital
99	Service; powers, duties, and functions
100	(1) The Florida Digital Service has been created within the
101	department to propose innovative solutions that securely
102	modernize state government, including technology and information
103	services, to achieve value through digital transformation and
104	interoperability, and to fully support the cloud-first policy as
105	specified in s. 282.206. The department, through the Florida
106	Digital Service, shall have the following powers, duties, and
107	functions:
108	(j) Provide operational management and oversight of the
109	state data center established pursuant to s. 282.201, which
110	includes:
111	1. Implementing industry standards and best practices for
112	the state data center's facilities, operations, maintenance,
113	planning, and management processes.
114	2. Developing and implementing cost-recovery mechanisms
115	that recover the full direct and indirect cost of services
116	through charges to applicable customer entities. Such cost-

# Page 4 of 22

585-03626A-21

20211900c1

117 recovery mechanisms must comply with applicable state and 118 federal regulations concerning distribution and use of funds and 119 must ensure that, for any fiscal year, no service or customer 120 entity subsidizes another service or customer entity. The 121 Florida Digital Service may recommend other payment mechanisms to the Executive Office of the Governor, the President of the 122 123 Senate, and the Speaker of the House of Representatives. Such 124 mechanism may be implemented only if specifically authorized by 125 the Legislature.

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

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

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

141 c. Providing rebates that may be credited against future142 billings to customer entities when revenues exceed costs.

d. Requiring customer entities to validate that sufficient
funds exist in the appropriate data processing appropriation
category or will be transferred into the appropriate data

#### Page 5 of 22

585-03626A-21 20211900c1 146 processing appropriation category before implementation of a 147 customer entity's request for a change in the type or level of service provided, if such change results in a net increase to 148 149 the customer entity's cost for that fiscal year. 150 e. By November 15 of each year, providing to the Office of Policy and Budget in the Executive Office of the Governor and to 151 152 the chairs of the legislative appropriations committees the 153 projected costs of providing data center services for the 154 following fiscal year. 155 f. Providing a plan for consideration by the Legislative 156 Budget Commission if the cost of a service is increased for a 157 reason other than a customer entity's request made pursuant to 158 sub-subparagraph d. Such a plan is required only if the service 159 cost increase results in a net increase to a customer entity for 160 that fiscal year. 161 q. Standardizing and consolidating procurement and 162 contracting practices. 163 4. In collaboration with the Department of Law Enforcement, 164 developing and implementing a process for detecting, reporting, 165 and responding to cybersecurity information technology security 166 incidents, breaches, and threats. 167 5. Adopting rules relating to the operation of the state 168 data center, including, but not limited to, budgeting and accounting procedures, cost-recovery methodologies, and 169 operating procedures. 170

171Section 4. Paragraph (g) of subsection (1) of section172282.201, Florida Statutes, is amended to read:

173 282.201 State data center.-The state data center is174 established within the department. The provision of data center

## Page 6 of 22

	585-03626A-21 20211900c1
175	services must comply with applicable state and federal laws,
176	regulations, and policies, including all applicable security,
177	privacy, and auditing requirements. The department shall appoint
178	a director of the state data center, preferably an individual
179	who has experience in leading data center facilities and has
180	expertise in cloud-computing management.
181	(1) STATE DATA CENTER DUTIES.—The state data center shall:
182	(g) In its procurement process, show preference for cloud-
183	computing solutions that minimize or do not require the
184	purchasing, financing, or leasing of state data center
185	infrastructure, and that meet the needs of customer agencies,
186	that reduce costs, and that meet or exceed the applicable state
187	and federal laws, regulations, and standards for cybersecurity
188	information technology security.
189	Section 5. Subsection (2) of section 282.206, Florida
190	Statutes, is amended to read:
191	282.206 Cloud-first policy in state agencies
192	(2) In its procurement process, each state agency shall
193	show a preference for cloud-computing solutions that either
194	minimize or do not require the use of state data center
195	infrastructure when cloud-computing solutions meet the needs of
196	the agency, reduce costs, and meet or exceed the applicable
197	state and federal laws, regulations, and standards for
198	cybersecurity information technology security.
199	Section 6. Section 282.318, Florida Statutes, is amended to
200	read:
201	282.318 Cybersecurity Security of data and information
202	technology
203	(1) This section may be cited as the <u>"State Cybersecurity</u>

# Page 7 of 22

585-03626A-21 20211900c1 204 Act." "Information Technology Security Act." 205 (2) As used in this section, the term "state agency" has 206 the same meaning as provided in s. 282.0041, except that the 207 term includes the Department of Legal Affairs, the Department of 208 Agriculture and Consumer Services, and the Department of 209 Financial Services. 210 (3) The department, acting through the Florida Digital 211 Service, is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity 212 risks and determining appropriate security measures. Such 213 214 standards and processes must be consistent with generally 215 accepted technology best practices, including the National Institute for Standards and Technology Cybersecurity Framework, 216 for cybersecurity. The department, acting through the Florida 217 Digital Service, shall adopt information technology security, to 218 219 include cybersecurity, and adopting rules that mitigate risks; 220 safequard state agency digital assets, an agency's data, 221 information, and information technology resources to ensure 222 availability, confidentiality, and integrity; and support a 223 security governance framework and to mitigate risks. The 224 department, acting through the Florida Digital Service, shall 225 also: 226 (a) Designate an employee of the Florida Digital Service as 227 the state chief information security officer. The state chief 228 information security officer must have experience and expertise 229 in security and risk management for communications and 230 information technology resources. The state chief information 231 security officer is responsible for the development, operation, 232 and oversight of cybersecurity for state technology systems. The

### Page 8 of 22

585-03626A-21 20211900c1 233 state chief information security officer shall be notified of 234 all confirmed or suspected incidents or threats of state agency 235 information technology resources and must report such incidents 236 or threats to the state chief information officer and the 237 Governor. 238 (b) Develop, and annually update by February 1, a statewide 239 cybersecurity information technology security strategic plan 240 that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive 241 protections against threats, tactical risk detection, threat 242 243 reporting, and response and recovery protocols for a cyber 244 incident the strategic issues of information technology security 245 policy, risk management, training, incident management, and 246 disaster recovery planning. 247 (c) Develop and publish for use by state agencies a 248 cybersecurity governance an information technology security 249 framework that, at a minimum, includes guidelines and processes 250 for: 251 1. Establishing asset management procedures to ensure that 252 an agency's information technology resources are identified and 253 managed consistent with their relative importance to the 254 agency's business objectives. 255 2. Using a standard risk assessment methodology that 256 includes the identification of an agency's priorities, 257 constraints, risk tolerances, and assumptions necessary to 258 support operational risk decisions. 259 3. Completing comprehensive risk assessments and 260 cybersecurity information technology security audits, which may 261 be completed by a private sector vendor, and submitting

## Page 9 of 22

CODING: Words stricken are deletions; words underlined are additions.

CS for SB 1900

CS for SB 1900

585-03626A-21 20211900c1 262 completed assessments and audits to the department. 263 4. Identifying protection procedures to manage the protection of an agency's information, data, and information 264 265 technology resources. 266 5. Establishing procedures for accessing information and 267 data to ensure the confidentiality, integrity, and availability 268 of such information and data. 269 6. Detecting threats through proactive monitoring of 270 events, continuous security monitoring, and defined detection 271 processes. 272 7. Establishing agency cybersecurity computer security 273 incident response teams and describing their responsibilities 274 for responding to cybersecurity information technology security 275 incidents, including breaches of personal information containing confidential or exempt data. 276 277 8. Recovering information and data in response to a 278 cybersecurity an information technology security incident. The 279 recovery may include recommended improvements to the agency 280 processes, policies, or guidelines. 281 9. Establishing a cybersecurity an information technology 282 security incident reporting process that includes procedures and 283 tiered reporting timeframes for notifying the department and the 284 Department of Law Enforcement of cybersecurity information technology security incidents. The tiered reporting timeframes 285 286 shall be based upon the level of severity of the cybersecurity 2.87 information technology security incidents being reported. 288 10. Incorporating information obtained through detection

289 and response activities into the agency's <u>cybersecurity</u> 290 information technology security incident response plans.

### Page 10 of 22

585-03626A-21 20211900c1 291 11. Developing agency strategic and operational 292 cybersecurity information technology security plans required 293 pursuant to this section. 294 12. Establishing the managerial, operational, and technical 295 safeguards for protecting state government data and information 296 technology resources that align with the state agency risk 297 management strategy and that protect the confidentiality, 298 integrity, and availability of information and data. 299 13. Establishing procedures for procuring information 300 technology commodities and services that require the commodity 301 or service to meet the National Institute of Standards and 302 Technology Cybersecurity Framework. (d) Assist state agencies in complying with this section. 303 304 (e) In collaboration with the Cybercrime Office of the 305 Department of Law Enforcement, annually provide training for 306 state agency information security managers and computer security 307 incident response team members that contains training on 308 cybersecurity information technology security, including 309 cybersecurity, threats, trends, and best practices. 310 (f) Annually review the strategic and operational 311 cybersecurity information technology security plans of state 312 executive branch agencies. 313 (g) Provide cybersecurity training to all state agency 314 technology professionals which develops, assesses, and documents 315 competencies by role and skill level. The training may be provided in collaboration with the Cybercrime Office of the 316 317 Department of Law Enforcement, a private sector entity, or an 318 institution of the state university system. 319 (h) Operate and maintain a Cybersecurity Operations Center

### Page 11 of 22

	585-03626A-21 20211900c1
320	led by the state chief information security officer, which must
321	be primarily virtual and staffed with tactical detection and
322	incident response personnel. The Cybersecurity Operations Center
323	shall serve as a clearinghouse for threat information and
324	coordinate with the Department of Law Enforcement to support
325	state agencies and their response to any confirmed or suspected
326	cybersecurity incident.
327	(i) Lead an Emergency Support Function, ESF CYBER, under
328	the state comprehensive emergency management plan as described
329	in s. 252.35.
330	(4) Each state agency head shall, at a minimum:
331	(a) Designate an information security manager to administer
332	the <u>cybersecurity</u> <del>information technology security</del> program of the
333	state agency. This designation must be provided annually in
334	writing to the department by January 1. A state agency's
335	information security manager, for purposes of these information
336	security duties, shall report directly to the agency head.
337	(b) In consultation with the department, through the
338	Florida Digital Service, and the Cybercrime Office of the
339	Department of Law Enforcement, establish an agency cybersecurity
340	<del>computer security incident</del> response team to respond to <u>a</u>
341	cybersecurity an information technology security incident. The
342	agency <u>cybersecurity</u> <del>computer security incident</del> response team
343	shall convene upon notification of <u>a cybersecurity</u> <del>an</del>
344	information technology security incident and must immediately
345	report all confirmed or suspected incidents to the state chief
346	information security officer, or his or her designee, and comply
347	with all applicable guidelines and processes established
348	pursuant to paragraph (3)(c).

# Page 12 of 22

585-03626A-21 20211900c1 349 (c) Submit to the department annually by July 31, the state 350 agency's strategic and operational cybersecurity information 351 technology security plans developed pursuant to rules and 352 guidelines established by the department, through the Florida 353 Digital Service. 354 1. The state agency strategic cybersecurity information 355 technology security plan must cover a 3-year period and, at a minimum, define security goals, intermediate objectives, and 356 357 projected agency costs for the strategic issues of agency 358 information security policy, risk management, security training, 359 security incident response, and disaster recovery. The plan must 360 be based on the statewide cybersecurity information technology 361 security strategic plan created by the department and include 362 performance metrics that can be objectively measured to reflect the status of the state agency's progress in meeting security 363 364 goals and objectives identified in the agency's strategic 365 information security plan.

2. The state agency operational <u>cybersecurity</u> information technology security plan must include a progress report that objectively measures progress made towards the prior operational <u>cybersecurity</u> information technology security plan and a project plan that includes activities, timelines, and deliverables for security objectives that the state agency will implement during the current fiscal year.

(d) Conduct, and update every 3 years, a comprehensive risk assessment, which may be completed by a private sector vendor, to determine the security threats to the data, information, and information technology resources, including mobile devices and print environments, of the agency. The risk assessment must

#### Page 13 of 22

585-03626A-21 20211900c1 378 comply with the risk assessment methodology developed by the 379 department and is confidential and exempt from s. 119.07(1), 380 except that such information shall be available to the Auditor 381 General, the Florida Digital Service within the department, the 382 Cybercrime Office of the Department of Law Enforcement, and, for 383 state agencies under the jurisdiction of the Governor, the Chief 384 Inspector General. If a private sector vendor is used to complete a comprehensive risk assessment, it must attest to the 385 386 validity of the risk assessment findings.

387 (e) Develop, and periodically update, written internal 388 policies and procedures, which include procedures for reporting 389 cybersecurity information technology security incidents and 390 breaches to the Cybercrime Office of the Department of Law 391 Enforcement and the Florida Digital Service within the 392 department. Such policies and procedures must be consistent with 393 the rules, quidelines, and processes established by the 394 department to ensure the security of the data, information, and 395 information technology resources of the agency. The internal 396 policies and procedures that, if disclosed, could facilitate the 397 unauthorized modification, disclosure, or destruction of data or 398 information technology resources are confidential information 399 and exempt from s. 119.07(1), except that such information shall 400 be available to the Auditor General, the Cybercrime Office of 401 the Department of Law Enforcement, the Florida Digital Service 402 within the department, and, for state agencies under the 403 jurisdiction of the Governor, the Chief Inspector General.

404 (f) Implement managerial, operational, and technical
405 safeguards and risk assessment remediation plans recommended by
406 the department to address identified risks to the data,

#### Page 14 of 22

585-03626A-21 20211900c1 407 information, and information technology resources of the agency. 408 The department, through the Florida Digital Service, shall track 409 implementation by state agencies upon development of such 410 remediation plans in coordination with agency inspectors 411 general. (q) Ensure that periodic internal audits and evaluations of 412 413 the agency's cybersecurity information technology security program for the data, information, and information technology 414 resources of the agency are conducted. The results of such 415 audits and evaluations are confidential information and exempt 416

from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service within the department, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

422 (h) Ensure that the information technology security and 423 cybersecurity requirements in both the written specifications 424 for the solicitation, contracts, and service-level agreement of 425 information technology and information technology resources and 426 services meet or exceed the applicable state and federal laws, 427 regulations, and standards for information technology security 428 and cybersecurity, including the National Institute of Standards 429 and Technology Cybersecurity Framework. Service-level agreements 430 must identify service provider and state agency responsibilities for privacy and security, protection of government data, 431 432 personnel background screening, and security deliverables with 433 associated frequencies.

434 (i) Provide information technology security and
435 cybersecurity awareness training to all state agency employees

### Page 15 of 22

585-03626A-21 20211900c1 436 in the first 30 days after commencing employment concerning 437 cybersecurity information technology security risks and the 438 responsibility of employees to comply with policies, standards, 439 quidelines, and operating procedures adopted by the state agency 440 to reduce those risks. The training may be provided in 441 collaboration with the Cybercrime Office of the Department of 442 Law Enforcement, a private sector entity, or an institution of 443 the state university system. 444 (j) Develop a process for detecting, reporting, and 445 responding to threats, breaches, or cybersecurity information 446 technology security incidents which is consistent with the 447 security rules, guidelines, and processes established by the 448 department through the Florida Digital Service. 449 1. All cybersecurity information technology security 450 incidents and breaches must be reported to the Florida Digital 451 Service within the department and the Cybercrime Office of the 452 Department of Law Enforcement and must comply with the 453 notification procedures and reporting timeframes established 454 pursuant to paragraph (3)(c). 455 2. For cybersecurity information technology security 456 breaches, state agencies shall provide notice in accordance with 457 s. 501.171. 458 (5) Portions of records held by a state agency which contain network schematics, hardware and software 459 460 configurations, or encryption, or which identify detection, 461 investigation, or response practices for suspected or confirmed 462 cybersecurity information technology security incidents, 463 including suspected or confirmed breaches, are confidential and 464 exempt from s. 119.07(1) and s. 24(a), Art. I of the State

## Page 16 of 22

585-03626A-21 20211900c1 465 Constitution, if the disclosure of such records would facilitate 466 unauthorized access to or the unauthorized modification, 467 disclosure, or destruction of: 468 (a) Data or information, whether physical or virtual; or 469 (b) Information technology resources, which includes: 470 1. Information relating to the security of the agency's 471 technologies, processes, and practices designed to protect 472 networks, computers, data processing software, and data from attack, damage, or unauthorized access; or 473 474 2. Security information, whether physical or virtual, which 475 relates to the agency's existing or proposed information 476 technology systems. (6) The portions of risk assessments, evaluations, external 477 478 audits, and other reports of a state agency's cybersecurity 479 information technology security program for the data, 480 information, and information technology resources of the state 481 agency which are held by a state agency are confidential and 482 exempt from s. 119.07(1) and s. 24(a), Art. I of the State 483 Constitution if the disclosure of such portions of records would 484 facilitate unauthorized access to or the unauthorized 485 modification, disclosure, or destruction of: 486 (a) Data or information, whether physical or virtual; or

487

(b) Information technology resources, which include:

488 1. Information relating to the security of the agency's technologies, processes, and practices designed to protect 489 490 networks, computers, data processing software, and data from 491 attack, damage, or unauthorized access; or

492 2. Security information, whether physical or virtual, which 493 relates to the agency's existing or proposed information

### Page 17 of 22

585-03626A-21

CS for SB 1900

20211900c1

494	technology systems.
495	
496	For purposes of this subsection, "external audit" means an audit
497	that is conducted by an entity other than the state agency that
498	is the subject of the audit.
499	(7) Those portions of a public meeting as specified in s.
500	286.011 which would reveal records which are confidential and
501	exempt under subsection (5) or subsection (6) are exempt from s.
502	286.011 and s. 24(b), Art. I of the State Constitution. No
503	exempt portion of an exempt meeting may be off the record. All
504	exempt portions of such meeting shall be recorded and
505	transcribed. Such recordings and transcripts are confidential
506	and exempt from disclosure under s. 119.07(1) and s. 24(a), Art.
507	I of the State Constitution unless a court of competent
508	jurisdiction, after an in camera review, determines that the
509	meeting was not restricted to the discussion of data and
510	information made confidential and exempt by this section. In the
511	event of such a judicial determination, only that portion of the
512	recording and transcript which reveals nonexempt data and
513	information may be disclosed to a third party.
514	(8) The portions of records made confidential and exempt in
515	subsections (5), (6), and (7) shall be available to the Auditor

5 (5), (6), and (/)516 General, the Cybercrime Office of the Department of Law 517 Enforcement, the Florida Digital Service within the department, 518 and, for agencies under the jurisdiction of the Governor, the 519 Chief Inspector General. Such portions of records may be made 520 available to a local government, another state agency, or a 521 federal agency for cybersecurity information technology security 522 purposes or in furtherance of the state agency's official

### Page 18 of 22

CS for SB 1900

	585-03626A-21 20211900c1
523	duties.
524	(9) The exemptions contained in subsections (5), (6), and
525	(7) apply to records held by a state agency before, on, or after
526	the effective date of this exemption.
527	(10) Subsections (5), (6), and (7) are subject to the Open
528	Government Sunset Review Act in accordance with s. 119.15 and
529	shall stand repealed on October 2, 2025, unless reviewed and
530	saved from repeal through reenactment by the Legislature.
531	(11) The department shall adopt rules relating to
532	cybersecurity information technology security and to administer
533	this section.
534	Section 7. Section 282.319, Florida Statutes, is created to
535	read:
536	282.319 Florida Cybersecurity Advisory Council.—
537	(1) The Florida Cybersecurity Advisory Council, an advisory
538	council as defined in s. 20.03(7), is created within the
539	department. Except as otherwise provided in this section, the
540	advisory council shall operate in a manner consistent with s.
541	20.052.
542	(2) The purpose of the council is to assist state agencies
543	in protecting their information technology resources from cyber
544	threats and incidents.
545	(3) The council shall assist the Florida Digital Service in
546	implementing best cybersecurity practices, taking into
547	consideration the final recommendations of the Florida
548	Cybersecurity Task Force created under chapter 2019-118, Laws of
549	Florida.
550	(4) The council shall be comprised of the following
551	members:

# Page 19 of 22

	585-03626A-21 20211900c1
552	(a) The Lieutenant Governor or his or her designee.
553	(b) The state chief information officer.
554	(c) The state chief information security officer.
555	(d) The director of the Division of Emergency Management or
556	his or her designee.
557	(e) A representative of the computer crime center of the
558	Department of Law Enforcement, appointed by the executive
559	director of the department.
560	(f) A representative of the Florida Fusion Center of the
561	Department of Law Enforcement, appointed by the executive
562	director of the department.
563	(g) The Chief Inspector General.
564	(h) A representative from the Public Service Commission.
565	(i) Up to two representatives from institutions of higher
566	education located in this state, appointed by the Governor.
567	(j) Three representatives from critical infrastructure
568	sectors, one of which must be from a water treatment facility,
569	appointed by the Governor.
570	(k) Four representatives of the private sector with senior
571	level experience in cybersecurity or software engineering from
572	within the finance, energy, health care, and transportation
573	sectors, appointed by the Governor.
574	(1) Two representatives with expertise on emerging
575	technology, with one appointed by the President of the Senate
576	and one appointed by the Speaker of the House of
577	Representatives.
578	(5) Members shall serve for a term of 4 years; however, for
579	the purpose of providing staggered terms, the initial
580	appointments of members made by the Governor shall be for a term

# Page 20 of 22

581       of 2 years. A vacancy shall be filled for the remainder of the         582       unexpired term in the same manner as the initial appointment.         583       All members of the council are eligible for reappointment.         584       (6) The Secretary of Management Services, or his or her         585       designee, shall serve as the ex officio, nonvoting executive         586       director of the council.         587       (7) Members of the council shall serve without compensation         588       but are entitled to receive reimbursement for per diem and         589       (8) The council shall meet at least quarterly to:         591       (8) The council shall meet at least quarterly to:         592       (b) Assess ongoing risks to state agency information         593       technology.         594       (c) Recommend a reporting and information sharing system to         595       notify state agencies of new risks.         596       (d) Recommend at breach simulation exercises.         597       (e) Assist the Florida Digital Service in developing         598       which include recommendations regarding:         600       1. Continuous risk monitoring.         611       2. Password management.         622       3. Protecting data in legacy and new systems.         631	I	585-03626A-21 20211900c1
All members of the council are eligible for reappointment.         (6) The Secretary of Management Services, or his or her         designee, shall serve as the ex officio, nonvoting executive         director of the council.         (7) Members of the council shall serve without compensation         but are entitled to receive reimbursement for per diem and         travel expenses pursuant to s. 112.061.         (8) The council shall meet at least quarterly to:         (a) Review existing state agency cybersecurity policies.         (b) Assess ongoing risks to state agency information         technology.         (c) Recommend a reporting and information sharing system to         notify state agencies of new risks.         (d) Recommend data breach simulation exercises.         (e) Assist the Florida Digital Service in developing         cybersecurity best practice recommendations for state agencies         which include recommendations regarding:         1. Continuous risk monitoring.         2. Password management.         3. Protecting data in legacy and new systems.         (f) Examine inconsistencies between state and federal law         regarding cybersecurity.         (9) The council shall work with the National Institute of         Standards and Technology and other federal agencies, private         sector businesses, and private cybersecurity experts:	581	of 2 years. A vacancy shall be filled for the remainder of the
60The Secretary of Management Services, or his or herdesignee, shall serve as the ex officio, nonvoting executivedirector of the council.61626364656566677071717273747475757576777777777878797979707070717172737474757575757576767777787979707070707070707070 <td>582</td> <td>unexpired term in the same manner as the initial appointment.</td>	582	unexpired term in the same manner as the initial appointment.
designee, shall serve as the ex officio, nonvoting executive         director of the council.         (7) Members of the council shall serve without compensation         but are entitled to receive reimbursement for per diem and         travel expenses pursuant to s. 112.061.         (8) The council shall meet at least quarterly to:         (a) Review existing state agency cybersecurity policies.         (b) Assess ongoing risks to state agency information         technology.         (c) Recommend a reporting and information sharing system to         notify state agencies of new risks.         (d) Recommend data breach simulation exercises.         (e) Assist the Florida Digital Service in developing         cybersecurity best practice recommendations for state agencies         which include recommendations regarding:         (1) Continuous risk monitoring.         (1) Examine inconsistencies between state and federal law         regarding cybersecurity.         (9) The council shall work with the National Institute of         Standards and Technology and other federal agencies, private         sector businesses, and private cybersecurity experts:         (a) For critical infrastructure not covered by federal law,	583	All members of the council are eligible for reappointment.
386       director of the council.         687       (7) Members of the council shall serve without compensation         588       but are entitled to receive reimbursement for per diem and         589       travel expenses pursuant to s. 112.061.         590       (8) The council shall meet at least quarterly to:         591       (a) Review existing state agency cybersecurity policies.         592       (b) Assess ongoing risks to state agency information         593       technology.         594       (c) Recommend a reporting and information sharing system to         595       notify state agencies of new risks.         596       (d) Recommend data breach simulation exercises.         597       (e) Assist the Florida Digital Service in developing         598       cybersecurity best practice recommendations for state agencies         599       which include recommendations regarding:         600       1. Continuous risk monitoring.         601       2. Password management.         602       3. Protecting data in legacy and new systems.         603       (f) Examine inconsistencies between state and federal law         604       regarding cybersecurity.         605       (9) The council shall work with the National Institute of         606       Standards and Technology and other fe	584	(6) The Secretary of Management Services, or his or her
587(7) Members of the council shall serve without compensation588but are entitled to receive reimbursement for per diem and589travel expenses pursuant to s. 112.061.590(8) The council shall meet at least quarterly to:591(a) Review existing state agency cybersecurity policies.592(b) Assess ongoing risks to state agency information593technology.594(c) Recommend a reporting and information sharing system to595notify state agencies of new risks.596(d) Recommend data breach simulation exercises.597(e) Assist the Florida Digital Service in developing598cybersecurity best practice recommendations for state agencies599which include recommendations regarding:6001. Continuous risk monitoring.6012. Password management.6023. Protecting data in legacy and new systems.603(f) Examine inconsistencies between state and federal law604regarding cybersecurity.605(9) The council shall work with the National Institute of606Standards and Technology and other federal agencies, private607(a) For critical infrastructure not covered by federal law,	585	designee, shall serve as the ex officio, nonvoting executive
but are entitled to receive reimbursement for per diem and         travel expenses pursuant to s. 112.061.         (8) The council shall meet at least quarterly to:         (a) Review existing state agency cybersecurity policies.         (b) Assess ongoing risks to state agency information         technology.         (c) Recommend a reporting and information sharing system to         notify state agencies of new risks.         (c) Recommend data breach simulation exercises.         (d) Recommend data breach simulation exercises.         (e) Assist the Florida Digital Service in developing         cybersecurity best practice recommendations for state agencies         which include recommendations regarding:         (1) Continuous risk monitoring.         (2) Assword management.         (3) Protecting data in legacy and new systems.         (f) Examine inconsistencies between state and federal law         regarding cybersecurity.         (f) The council shall work with the National Institute of         Standards and Technology and other federal agencies, private         sector businesses, and private cybersecurity experts:         (a) For critical infrastructure not covered by federal law,	586	director of the council.
Travel expenses pursuant to s. 112.061.589(8) The council shall meet at least quarterly to:591(a) Review existing state agency cybersecurity policies.592(b) Assess ongoing risks to state agency information593technology.594(c) Recommend a reporting and information sharing system to595notify state agencies of new risks.596(d) Recommend data breach simulation exercises.597(e) Assist the Florida Digital Service in developing598cybersecurity best practice recommendations for state agencies599which include recommendations regarding:6001. Continuous risk monitoring.6012. Password management.6023. Protecting data in legacy and new systems.603(f) Examine inconsistencies between state and federal law604regarding cybersecurity.605(9) The council shall work with the National Institute of606Standards and Technology and other federal agencies, private607(a) For critical infrastructure not covered by federal law,	587	(7) Members of the council shall serve without compensation
590       (8) The council shall meet at least quarterly to:         591       (a) Review existing state agency cybersecurity policies.         592       (b) Assess ongoing risks to state agency information         593       technology.         594       (c) Recommend a reporting and information sharing system to         595       notify state agencies of new risks.         596       (d) Recommend data breach simulation exercises.         597       (e) Assist the Florida Digital Service in developing         598       cybersecurity best practice recommendations for state agencies         599       which include recommendations regarding:         600       1. Continuous risk monitoring.         601       2. Password management.         602       3. Protecting data in legacy and new systems.         603       (f) Examine inconsistencies between state and federal law         604       regarding cybersecurity.         605       (9) The council shall work with the National Institute of         606       Standards and Technology and other federal agencies, private         607       sector businesses, and private cybersecurity experts:         608       (a) For critical infrastructure not covered by federal law,	588	but are entitled to receive reimbursement for per diem and
591       (a) Review existing state agency cybersecurity policies.         592       (b) Assess ongoing risks to state agency information         593       technology.         594       (c) Recommend a reporting and information sharing system to         595       notify state agencies of new risks.         596       (d) Recommend data breach simulation exercises.         597       (e) Assist the Florida Digital Service in developing         598       cybersecurity best practice recommendations for state agencies         599       which include recommendations regarding:         600       1. Continuous risk monitoring.         601       2. Password management.         602       3. Protecting data in legacy and new systems.         603       (f) Examine inconsistencies between state and federal law         604       regarding cybersecurity.         605       (9) The council shall work with the National Institute of         606       Standards and Technology and other federal agencies, private         607       sector businesses, and private cybersecurity experts:         608       (a) For critical infrastructure not covered by federal law,	589	travel expenses pursuant to s. 112.061.
(b) Assess ongoing risks to state agency information         593         (c) Recommend a reporting and information sharing system to         594       (c) Recommend a reporting and information sharing system to         595       notify state agencies of new risks.         596       (d) Recommend data breach simulation exercises.         597       (e) Assist the Florida Digital Service in developing         598       cybersecurity best practice recommendations for state agencies         599       which include recommendations regarding:         600       1. Continuous risk monitoring.         601       2. Password management.         602       3. Protecting data in legacy and new systems.         603       (f) Examine inconsistencies between state and federal law         604       regarding cybersecurity.         605       (9) The council shall work with the National Institute of         606       Standards and Technology and other federal agencies, private         607       sector businesses, and private cybersecurity experts:         608       (a) For critical infrastructure not covered by federal law,	590	(8) The council shall meet at least quarterly to:
593technology.594(c) Recommend a reporting and information sharing system to595notify state agencies of new risks.596(d) Recommend data breach simulation exercises.597(e) Assist the Florida Digital Service in developing598cybersecurity best practice recommendations for state agencies599which include recommendations regarding:6001. Continuous risk monitoring.6012. Password management.6023. Protecting data in legacy and new systems.603(f) Examine inconsistencies between state and federal law604regarding cybersecurity.605(9) The council shall work with the National Institute of606Standards and Technology and other federal agencies, private607(a) For critical infrastructure not covered by federal law,	591	(a) Review existing state agency cybersecurity policies.
1594(c) Recommend a reporting and information sharing system to595notify state agencies of new risks.596(d) Recommend data breach simulation exercises.597(e) Assist the Florida Digital Service in developing598cybersecurity best practice recommendations for state agencies599which include recommendations regarding:6001. Continuous risk monitoring.6012. Password management.6023. Protecting data in legacy and new systems.603(f) Examine inconsistencies between state and federal law604regarding cybersecurity.605(9) The council shall work with the National Institute of606Standards and Technology and other federal agencies, private607(a) For critical infrastructure not covered by federal law,	592	(b) Assess ongoing risks to state agency information
595notify state agencies of new risks.596(d) Recommend data breach simulation exercises.597(e) Assist the Florida Digital Service in developing598cybersecurity best practice recommendations for state agencies599which include recommendations regarding:6001. Continuous risk monitoring.6012. Password management.6023. Protecting data in legacy and new systems.603(f) Examine inconsistencies between state and federal law604regarding cybersecurity.605(9) The council shall work with the National Institute of606Standards and Technology and other federal agencies, private607(a) For critical infrastructure not covered by federal law,	593	technology.
596(d) Recommend data breach simulation exercises.597(e) Assist the Florida Digital Service in developing598cybersecurity best practice recommendations for state agencies599which include recommendations regarding:6001. Continuous risk monitoring.6012. Password management.6023. Protecting data in legacy and new systems.603(f) Examine inconsistencies between state and federal law604regarding cybersecurity.605(9) The council shall work with the National Institute of606Standards and Technology and other federal agencies, private607(a) For critical infrastructure not covered by federal law,	594	(c) Recommend a reporting and information sharing system to
<ul> <li>(e) Assist the Florida Digital Service in developing</li> <li>cybersecurity best practice recommendations for state agencies</li> <li>which include recommendations regarding:</li> <li>1. Continuous risk monitoring.</li> <li>2. Password management.</li> <li>3. Protecting data in legacy and new systems.</li> <li>(f) Examine inconsistencies between state and federal law</li> <li>regarding cybersecurity.</li> <li>(9) The council shall work with the National Institute of</li> <li>Standards and Technology and other federal agencies, private</li> <li>sector businesses, and private cybersecurity experts:</li> <li>(a) For critical infrastructure not covered by federal law,</li> </ul>	595	notify state agencies of new risks.
598       cybersecurity best practice recommendations for state agencies         599       which include recommendations regarding:         600       1. Continuous risk monitoring.         601       2. Password management.         602       3. Protecting data in legacy and new systems.         603       (f) Examine inconsistencies between state and federal law         604       regarding cybersecurity.         605       (9) The council shall work with the National Institute of         606       Standards and Technology and other federal agencies, private         607       sector businesses, and private cybersecurity experts:         608       (a) For critical infrastructure not covered by federal law,	596	(d) Recommend data breach simulation exercises.
599which include recommendations regarding:6001. Continuous risk monitoring.6012. Password management.6023. Protecting data in legacy and new systems.603(f) Examine inconsistencies between state and federal law604regarding cybersecurity.605(9) The council shall work with the National Institute of606Standards and Technology and other federal agencies, private607sector businesses, and private cybersecurity experts:608(a) For critical infrastructure not covered by federal law,	597	(e) Assist the Florida Digital Service in developing
<ul> <li>600 <u>1. Continuous risk monitoring.</u></li> <li>601 <u>2. Password management.</u></li> <li>602 <u>3. Protecting data in legacy and new systems.</u></li> <li>603 (f) Examine inconsistencies between state and federal law</li> <li>604 regarding cybersecurity.</li> <li>605 (9) The council shall work with the National Institute of</li> <li>606 Standards and Technology and other federal agencies, private</li> <li>607 sector businesses, and private cybersecurity experts:</li> <li>608 (a) For critical infrastructure not covered by federal law,</li> </ul>	598	cybersecurity best practice recommendations for state agencies
<ul> <li>601</li> <li><u>2. Password management.</u></li> <li>602</li> <li><u>3. Protecting data in legacy and new systems.</u></li> <li>603 <ul> <li>(f) Examine inconsistencies between state and federal law</li> </ul> </li> <li>604 <ul> <li>regarding cybersecurity.</li> </ul> </li> <li>605 <ul> <li>(9) The council shall work with the National Institute of</li> </ul> </li> <li>606 <ul> <li>Standards and Technology and other federal agencies, private</li> </ul> </li> <li>607 <ul> <li>sector businesses, and private cybersecurity experts:</li> <li>(a) For critical infrastructure not covered by federal law,</li> </ul> </li> </ul>	599	which include recommendations regarding:
<ul> <li>602 <u>3. Protecting data in legacy and new systems.</u></li> <li>603 (f) Examine inconsistencies between state and federal law</li> <li>604 regarding cybersecurity.</li> <li>605 (9) The council shall work with the National Institute of</li> <li>606 Standards and Technology and other federal agencies, private</li> <li>607 sector businesses, and private cybersecurity experts:</li> <li>608 (a) For critical infrastructure not covered by federal law,</li> </ul>	600	1. Continuous risk monitoring.
603 (f) Examine inconsistencies between state and federal law 604 regarding cybersecurity. 605 (9) The council shall work with the National Institute of 606 Standards and Technology and other federal agencies, private 607 sector businesses, and private cybersecurity experts: 608 (a) For critical infrastructure not covered by federal law,	601	2. Password management.
<pre>604 regarding cybersecurity. 605 (9) The council shall work with the National Institute of 606 Standards and Technology and other federal agencies, private 607 sector businesses, and private cybersecurity experts: 608 (a) For critical infrastructure not covered by federal law,</pre>	602	3. Protecting data in legacy and new systems.
605(9) The council shall work with the National Institute of606Standards and Technology and other federal agencies, private607sector businesses, and private cybersecurity experts:608(a) For critical infrastructure not covered by federal law,	603	(f) Examine inconsistencies between state and federal law
606 <u>Standards and Technology and other federal agencies, private</u> 607 <u>sector businesses, and private cybersecurity experts:</u> 608 <u>(a) For critical infrastructure not covered by federal law,</u>	604	regarding cybersecurity.
607 <u>sector businesses, and private cybersecurity experts:</u> 608 <u>(a) For critical infrastructure not covered by federal law,</u>	605	(9) The council shall work with the National Institute of
608 (a) For critical infrastructure not covered by federal law,	606	Standards and Technology and other federal agencies, private
	607	sector businesses, and private cybersecurity experts:
609 to identify which local infrastructure sectors are at the	608	(a) For critical infrastructure not covered by federal law,
	609	to identify which local infrastructure sectors are at the

# Page 21 of 22

	585-03626A-21 20211900c1
610	greatest risk of cyber attacks and need the most enhanced
611	cybersecurity measures.
612	(b) To use federal guidance to identify categories of
613	critical infrastructure as critical cyber infrastructure if
614	cyber damage or unauthorized cyber access to the infrastructure
615	could reasonably result in catastrophic consequences.
616	(10) Beginning June 30, 2022, and each June 30 thereafter,
617	the council shall submit to the President of the Senate and the
618	Speaker of the House of Representatives any legislative
619	recommendations considered necessary by the council to address
620	cybersecurity.
621	Section 8. This act shall take effect July 1, 2021.

# Page 22 of 22