

1 A bill to be entitled
2 An act relating to cybersecurity; providing a short
3 title; amending s. 110.205, F.S.; exempting certain
4 personnel from the career service; amending s.
5 282.0041, F.S.; providing and revising definitions;
6 amending s. 282.0051, F.S.; requiring the Florida
7 Digital Service to ensure that independent project
8 oversight is performed in a certain manner and to take
9 certain actions relating to the procurement of project
10 oversight as a service; requiring the Florida Digital
11 Service to provide certain reports by certain dates;
12 requiring the Florida Digital Service to establish an
13 operations committee for a certain purpose and
14 composed of certain members; requiring the Governor to
15 appoint a state chief information officer subject to
16 confirmation by the Senate; requiring the state chief
17 information officer to designate a state chief
18 technology officer; providing duties of the state
19 chief technology officer; amending s. 282.201, F.S.;
20 providing that the state data center shall be overseen
21 by and accountable to the Department of Management
22 Services in consultation with certain officers;
23 providing requirements for certain state data center
24 procurements; requiring the state chief information
25 officer to assume responsibility for a certain

26 | contract; requiring the Florida Digital Service to be
 27 | provided with full access to state data center
 28 | infrastructure, systems, applications, and other means
 29 | of hosting, supporting, and managing certain data;
 30 | requiring the state data center to submit a certain
 31 | report to the department and the Florida Digital
 32 | Service; amending s. 282.318, F.S.; requiring a state
 33 | agency to report ransomware and cybersecurity
 34 | incidents within a certain time period; requiring the
 35 | Florida Digital Service to notify the Governor and
 36 | Legislature of certain incidents; providing that
 37 | certain notification must be provided in a secure
 38 | environment; requiring the Florida Digital Service to
 39 | provide cybersecurity briefings to certain legislative
 40 | committees; authorizing the Florida Digital Service to
 41 | respond to certain cybersecurity incidents; requiring
 42 | a state agency head to designate a chief information
 43 | security officer for the agency; revising the purpose
 44 | of an agency's information security manager and the
 45 | date by which he or she must be designated; revising
 46 | the frequency of a comprehensive risk assessment;
 47 | authorizing the department to facilitate and providing
 48 | requirements for such assessment; authorizing certain
 49 | legislative committees to hold closed meetings to
 50 | receive certain briefings; requiring such committees

51 to maintain the confidential and exempt status of
 52 certain records; amending s. 282.3185, F.S.; requiring
 53 a local government to report ransomware and
 54 cybersecurity incidents within a certain time period;
 55 requiring the Florida Digital Service to notify the
 56 Governor and Legislature of certain incidents;
 57 providing that certain notification must be provided
 58 in a secure environment; amending s. 282.319, F.S.;
 59 revising the membership of the Florida Cybersecurity
 60 Advisory Council; creating s. 768.401, F.S.; providing
 61 that a county, municipality, or commercial entity that
 62 complies with certain requirements is not liable in
 63 connection with a cybersecurity incident; requiring
 64 certain entities to adopt certain revised frameworks
 65 or standards within a specified time period; providing
 66 that a private cause of action is not established;
 67 providing that certain failures are not evidence of
 68 negligence and do not constitute negligence per se;
 69 specifying that the defendant in certain actions has a
 70 certain burden of proof; providing an effective date.

71
 72 Be It Enacted by the Legislature of the State of Florida:

73
 74 Section 1. This act may be cited as the "Florida Cyber
 75 Protection Act."

76 Section 2. Paragraph (y) is added to subsection (2) of
 77 section 110.205, Florida Statutes, to read:

78 110.205 Career service; exemptions.—

79 (2) EXEMPT POSITIONS.—The exempt positions that are not
 80 covered by this part include the following:

81 (y) Personnel employed by or reporting to the state chief
 82 information security officer, the state chief data officer, a
 83 chief information security officer, and an agency information
 84 security manager.

85 Section 3. Subsections (3) through (5), (6) through (19),
 86 and (20) through (38) of section 282.0041, Florida Statutes, are
 87 renumbered as subsections (4) through (6), (8) through (21), and
 88 (24) through (42), respectively, present subsection (19) is
 89 amended, and new subsections (3), (7), (22), and (23) are added
 90 to that section, to read:

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

92 (3) "As a service" means the contracting with or
 93 outsourcing to a third-party of a defined role or function as a
 94 means of delivery.

95 (7) "Cloud provider" has the same meaning as provided in
 96 Special Publication 800-145 issued by the National Institute of
 97 Standards and Technology.

98 (21)~~(19)~~ "Incident" means a violation or an imminent
 99 threat of violation, whether such violation is accidental or
 100 deliberate, of information technology resources, security,

101 policies, or practices, or which may jeopardize the
102 confidentiality, integrity, or availability of an information
103 technology system or the information the system processes,
104 stores, or transmits. An imminent threat of violation refers to
105 a situation in which a state agency, county, or municipality has
106 a factual basis for believing that a specific incident is about
107 to occur.

108 (22) "Independent" means, for an entity providing
109 independent verification and validation, having no technical,
110 managerial, or financial interest in the relevant technology
111 project; no relationship to the relevant agency; and no
112 responsibility for or participation in any aspect of the
113 project, which includes project oversight by the Florida Digital
114 Service.

115 (23) "Independent verification and validation" means
116 third-party support services that provide a completely
117 independent and impartial assessment of the progress and work
118 products of a technology project from concept to business case
119 and throughout the project lifecycle.

120 Section 4. Section 282.0051, Florida Statutes, is amended
121 to read:

122 282.0051 Department of Management Services; Florida
123 Digital Service; powers, duties, and functions.—

124 (1) The Florida Digital Service is ~~has been~~ created within
125 the department to propose innovative solutions that securely

126 modernize state government, including technology and information
127 services, to achieve value through digital transformation and
128 interoperability, and to fully support the cloud-first policy as
129 specified in s. 282.206. The department, through the Florida
130 Digital Service, shall have the following powers, duties, and
131 functions:

132 (a) Develop and publish information technology policy for
133 the management of the state's information technology resources.

134 (b) Develop an enterprise architecture that:

135 1. Acknowledges the unique needs of the entities within
136 the enterprise in the development and publication of standards
137 and terminologies to facilitate digital interoperability;

138 2. Supports the cloud-first policy as specified in s.
139 282.206; and

140 3. Addresses how information technology infrastructure may
141 be modernized to achieve cloud-first objectives.

142 (c) Establish project management and oversight standards
143 with which state agencies must comply when implementing
144 information technology projects. The department, acting through
145 the Florida Digital Service, shall provide training
146 opportunities to state agencies to assist in the adoption of the
147 project management and oversight standards. To support data-
148 driven decisionmaking, the standards must include, but are not
149 limited to:

150 1. Performance measurements and metrics that objectively

151 reflect the status of an information technology project based on
152 a defined and documented project scope, cost, and schedule.

153 2. Methodologies for calculating acceptable variances in
154 the projected versus actual scope, schedule, or cost of an
155 information technology project.

156 3. Reporting requirements, including requirements designed
157 to alert all defined stakeholders that an information technology
158 project has exceeded acceptable variances defined and documented
159 in a project plan.

160 4. Content, format, and frequency of project updates.

161 5. Technical standards to ensure an information technology
162 project complies with the enterprise architecture.

163 (d) Ensure that independent ~~Perform~~ project oversight on
164 all state agency information technology projects that have total
165 project costs of \$10 million or more and that are funded in the
166 General Appropriations Act or any other law is performed and in
167 compliance with applicable state and federal law.

168 1. The department may not be considered independent for
169 purposes of project oversight under this paragraph on a project
170 for which the department has provided or may be asked to provide
171 any operational or technical support, including, but not limited
172 to, providing advice or conducting any review.

173 2. The department shall establish an appropriate contract
174 vehicle to facilitate procurement of project oversight as a
175 service by the enterprise and ensure that the contract vehicle

176 includes offerings that incorporate the ability to comply with
177 applicable state and federal law, including any independent
178 verification and validation requirements. An entity that
179 provides project oversight as a service must provide a project
180 oversight report to the department.

181 3. An agency may request the department to procure project
182 oversight as a service for a project that is subject to this
183 paragraph. Such procurement by the department does not violate
184 the requirement that the project oversight must be independent.

185 4. The department, acting through the Florida Digital
186 Service, shall at least quarterly review received project
187 oversight reports and, upon acceptance of the contents of such
188 reports, provide the reports to the Executive Office of the
189 Governor, the President of the Senate, and the Speaker of the
190 House of Representatives.

191 5. The department, acting through the Florida Digital
192 Service, shall report at least quarterly to the Executive Office
193 of the Governor, the President of the Senate, and the Speaker of
194 the House of Representatives on any information technology
195 project that the department identifies as high-risk due to the
196 project exceeding acceptable variance ranges defined and
197 documented in a project plan. The report must include a risk
198 assessment, including fiscal risks, associated with proceeding
199 to the next stage of the project, and a recommendation for
200 corrective actions required, including suspension or termination

201 of the project.

202 (e) Identify opportunities for standardization and
203 consolidation of information technology services that support
204 interoperability and the cloud-first policy, as specified in s.
205 282.206, and business functions and operations, including
206 administrative functions such as purchasing, accounting and
207 reporting, cash management, and personnel, and that are common
208 across state agencies. The department, acting through the
209 Florida Digital Service, shall biennially on January 15 ± of
210 each even-numbered year provide recommendations for
211 standardization and consolidation to the Executive Office of the
212 Governor, the President of the Senate, and the Speaker of the
213 House of Representatives.

214 (f) Establish best practices for the procurement of
215 information technology products and cloud-computing services in
216 order to reduce costs, increase the quality of data center
217 services, or improve government services.

218 (g) Develop standards for information technology reports
219 and updates, including, but not limited to, operational work
220 plans, project spend plans, and project status reports, for use
221 by state agencies.

222 (h) Upon request, assist state agencies in the development
223 of information technology-related legislative budget requests.

224 (i) Conduct annual assessments of state agencies to
225 determine compliance with all information technology standards

226 and guidelines developed and published by the department and
227 provide results of the assessments to the Executive Office of
228 the Governor, the President of the Senate, and the Speaker of
229 the House of Representatives.

230 (j) Conduct a market analysis not less frequently than
231 every 3 years beginning in 2021 to determine whether the
232 information technology resources within the enterprise are
233 utilized in the most cost-effective and cost-efficient manner,
234 while recognizing that the replacement of certain legacy
235 information technology systems within the enterprise may be cost
236 prohibitive or cost inefficient due to the remaining useful life
237 of those resources; whether the enterprise is complying with the
238 cloud-first policy specified in s. 282.206; and whether the
239 enterprise is utilizing best practices with respect to
240 information technology, information services, and the
241 acquisition of emerging technologies and information services.
242 Each market analysis shall be used to prepare a strategic plan
243 for continued and future information technology and information
244 services for the enterprise, including, but not limited to,
245 proposed acquisition of new services or technologies and
246 approaches to the implementation of any new services or
247 technologies. Copies of each market analysis and accompanying
248 strategic plan must be submitted to the Executive Office of the
249 Governor, the President of the Senate, and the Speaker of the
250 House of Representatives not later than December 31 of each year

251 that a market analysis is conducted.

252 (k) Recommend other information technology services that
253 should be designed, delivered, and managed as enterprise
254 information technology services. Recommendations must include
255 the identification of existing information technology resources
256 associated with the services, if existing services must be
257 transferred as a result of being delivered and managed as
258 enterprise information technology services.

259 (l) In consultation with state agencies, propose a
260 methodology and approach for identifying and collecting both
261 current and planned information technology expenditure data at
262 the state agency level.

263 (m)1. Notwithstanding any other law, provide project
264 oversight on any information technology project of the
265 Department of Financial Services, the Department of Legal
266 Affairs, and the Department of Agriculture and Consumer Services
267 which has a total project cost of \$20 million or more. Such
268 information technology projects must also comply with the
269 applicable information technology architecture, project
270 management and oversight, and reporting standards established by
271 the department, acting through the Florida Digital Service.

272 2. When performing the project oversight function
273 specified in subparagraph 1., report by the 15th day after the
274 end of each quarter ~~at least quarterly~~ to the Executive Office
275 of the Governor, the President of the Senate, and the Speaker of

276 the House of Representatives on any information technology
277 project that the department, acting through the Florida Digital
278 Service, identifies as high-risk due to the project exceeding
279 acceptable variance ranges defined and documented in the project
280 plan. The report shall include a risk assessment, including
281 fiscal risks, associated with proceeding to the next stage of
282 the project and a recommendation for corrective actions
283 required, including suspension or termination of the project.

284 (n) If an information technology project implemented by a
285 state agency must be connected to or otherwise accommodated by
286 an information technology system administered by the Department
287 of Financial Services, the Department of Legal Affairs, or the
288 Department of Agriculture and Consumer Services, consult with
289 these departments regarding the risks and other effects of such
290 projects on their information technology systems and work
291 cooperatively with these departments regarding the connections,
292 interfaces, timing, or accommodations required to implement such
293 projects.

294 (o) If adherence to standards or policies adopted by or
295 established pursuant to this section causes conflict with
296 federal regulations or requirements imposed on an entity within
297 the enterprise and results in adverse action against an entity
298 or federal funding, work with the entity to provide alternative
299 standards, policies, or requirements that do not conflict with
300 the federal regulation or requirement. The department, acting

301 through the Florida Digital Service, shall annually by January
302 15 report such alternative standards to the Executive Office of
303 the Governor, the President of the Senate, and the Speaker of
304 the House of Representatives.

305 (p)1. Establish an information technology policy for all
306 information technology-related state contracts, including state
307 term contracts for information technology commodities,
308 consultant services, and staff augmentation services. The
309 information technology policy must include:

310 a. Identification of the information technology product
311 and service categories to be included in state term contracts.

312 b. Requirements to be included in solicitations for state
313 term contracts.

314 c. Evaluation criteria for the award of information
315 technology-related state term contracts.

316 d. The term of each information technology-related state
317 term contract.

318 e. The maximum number of vendors authorized on each state
319 term contract.

320 f. At a minimum, a requirement that any contract for
321 information technology commodities or services meet the National
322 Institute of Standards and Technology Cybersecurity Framework.

323 g. For an information technology project wherein project
324 oversight is required pursuant to paragraph (d) or paragraph
325 (m), a requirement that independent verification and validation

326 | be employed throughout the project life cycle with the primary
327 | objective of independent verification and validation being to
328 | provide an objective assessment of products and processes
329 | throughout the project life cycle. An entity providing
330 | independent verification and validation may not have technical,
331 | managerial, or financial interest in the project and may not
332 | have responsibility for, or participate in, any other aspect of
333 | the project.

334 | 2. Evaluate vendor responses for information technology-
335 | related state term contract solicitations and invitations to
336 | negotiate.

337 | 3. Answer vendor questions on information technology-
338 | related state term contract solicitations.

339 | 4. Ensure that the information technology policy
340 | established pursuant to subparagraph 1. is included in all
341 | solicitations and contracts that are administratively executed
342 | by the department.

343 | (q) Recommend potential methods for standardizing data
344 | across state agencies which will promote interoperability and
345 | reduce the collection of duplicative data.

346 | (r) Recommend open data technical standards and
347 | terminologies for use by the enterprise.

348 | (s) Ensure that enterprise information technology
349 | solutions are capable of utilizing an electronic credential and
350 | comply with the enterprise architecture standards.

351 (t) Establish an operations committee that shall meet as
352 necessary for the purpose of developing collaborative efforts
353 between agencies and other governmental entities relating to
354 cybersecurity issues, including the coordination of preparedness
355 and response efforts relating to cybersecurity incidents and
356 issues relating to the interoperability of agency projects. The
357 Secretary of Management Services shall serve as the executive
358 director of the committee. The committee shall be composed of
359 the following members:

360 1. The state chief information officer, or his or her
361 designee.

362 2. The Attorney General, or his or her designee.

363 3. The Secretary of State, or his or her designee.

364 4. The executive director of the Department of Law
365 Enforcement, or his or her designee.

366 5. The Secretary of Transportation, or his or her
367 designee.

368 6. The director of the Division of Emergency Management,
369 or his or her designee.

370 7. The Secretary of Health Care Administration, or his or
371 her designee.

372 8. The Commissioner of Education, or his or her designee.

373 9. The executive director of the Department of Highway
374 Safety and Motor Vehicles, or his or her designee.

375 10. The chair of the Public Service Commission, or his or

376 her designee.

377 11. The director of the Florida State Guard, or his or her
 378 designee.

379 12. The Adjutant General of the Florida National Guard, or
 380 his or her designee.

381 13. Any other agency head appointed by the Governor.

382 (2)(a) The Governor shall appoint ~~Secretary of Management~~
 383 ~~Services shall designate~~ a state chief information officer,
 384 subject to confirmation by the Senate, who shall administer the
 385 Florida Digital Service. The state chief information officer,
 386 before ~~prior to~~ appointment, must have at least 5 years of
 387 experience in the development of information system strategic
 388 planning and development or information technology policy, and,
 389 preferably, have leadership-level experience in the design,
 390 development, and deployment of interoperable software and data
 391 solutions.

392 (b) The state chief information officer, ~~in consultation~~
 393 ~~with the Secretary of Management Services,~~ shall designate a
 394 state chief data officer. The chief data officer must be a
 395 proven and effective administrator who must have significant and
 396 substantive experience in data management, data governance,
 397 interoperability, and security.

398 (c) The state chief information officer shall designate a
 399 state chief technology officer who shall be responsible for:

400 1. Exploring technology solutions to meet the enterprise

- 401 need;
 402 2. The deployments of adopted enterprise solutions;
 403 3. Compliance with the cloud-first policy specified in s.
 404 282.206;
 405 4. Recommending best practices to increase the likelihood
 406 of technology project success;
 407 5. Developing strategic partnerships with the private
 408 sector; and
 409 6. Directly supporting enterprise cybersecurity and data
 410 interoperability initiatives.

411
 412 The state chief technology officer may acquire cloud migration
 413 as a service to comply with this section as it pertains to the
 414 implementation across the enterprise of the cloud-first policy.

415 (3) The department, acting through the Florida Digital
 416 Service and from funds appropriated to the Florida Digital
 417 Service, shall:

418 (a) ~~Create, not later than December 1, 2022,~~ and maintain
 419 a comprehensive indexed data catalog in collaboration with the
 420 enterprise that lists the data elements housed within the
 421 enterprise and the legacy system or application in which these
 422 data elements are located. The data catalog must, at a minimum,
 423 specifically identify all data that is restricted from public
 424 disclosure based on federal or state laws and regulations and
 425 require that all such information be protected in accordance

426 with s. 282.318.

427 (b) Develop and publish, ~~not later than December 1, 2022,~~
428 in collaboration with the enterprise, a data dictionary for each
429 agency that reflects the nomenclature in the comprehensive
430 indexed data catalog.

431 (c) Adopt, by rule, standards that support the creation
432 and deployment of an application programming interface to
433 facilitate integration throughout the enterprise.

434 (d) Adopt, by rule, standards necessary to facilitate a
435 secure ecosystem of data interoperability that is compliant with
436 the enterprise architecture.

437 (e) Adopt, by rule, standards that facilitate the
438 deployment of applications or solutions to the existing
439 enterprise system in a controlled and phased approach.

440 (f) After submission of documented use cases developed in
441 conjunction with the affected agencies, assist the affected
442 agencies with the deployment, contingent upon a specific
443 appropriation therefor, of new interoperable applications and
444 solutions:

445 1. For the Department of Health, the Agency for Health
446 Care Administration, the Agency for Persons with Disabilities,
447 the Department of Education, the Department of Elderly Affairs,
448 and the Department of Children and Families.

449 2. To support military members, veterans, and their
450 families.

451 (4) For information technology projects that have a total
452 project costs ~~cost~~ of \$10 million or more:

453 (a) State agencies must provide the Florida Digital
454 Service with written notice of any planned procurement of an
455 information technology project.

456 (b) The Florida Digital Service must participate in the
457 development of specifications and recommend modifications to any
458 planned procurement of an information technology project by
459 state agencies so that the procurement complies with the
460 enterprise architecture.

461 (c) The Florida Digital Service must participate in post-
462 award contract monitoring.

463 (5) The department, acting through the Florida Digital
464 Service, may not retrieve or disclose any data without a shared-
465 data agreement in place between the department and the
466 enterprise entity that has primary custodial responsibility of,
467 or data-sharing responsibility for, that data.

468 (6) The department, acting through the Florida Digital
469 Service, shall adopt rules to administer this section.

470 Section 5. Section 282.201, Florida Statutes, is amended
471 to read:

472 282.201 State data center.—The state data center is
473 established within the department and shall be overseen by and
474 accountable to the department in consultation with the state
475 chief information officer, the state chief data officer, the

476 state chief information security officer, and the state chief
477 technology officer. Any procurement or purchase of enterprise
478 architecture which is comparable to a project that would be
479 subject to requirements under s. 282.0051(4) if the total
480 project cost was \$10 million or more and which may be consumed
481 by an enterprise must be provided to the department and the
482 Florida Digital Service for review before publication. The
483 provision of data center services must comply with applicable
484 state and federal laws, regulations, and policies, including all
485 applicable security, privacy, and auditing requirements. The
486 Florida Digital Service ~~department~~ shall appoint a director of
487 the state data center who has experience in leading data center
488 facilities and has expertise in cloud-computing management.

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

490 (a) Offer, develop, and support the services and
491 applications defined in service-level agreements executed with
492 its customer entities.

493 (b) Maintain performance of the state data center by
494 ensuring proper data backup; data backup recovery; disaster
495 recovery; and appropriate security, power, cooling, fire
496 suppression, and capacity.

497 (c) Develop and implement business continuity and disaster
498 recovery plans, and annually conduct a live exercise of each
499 plan.

500 (d) Enter into a service-level agreement with each

501 customer entity to provide the required type and level of
 502 service or services. If a customer entity fails to execute an
 503 agreement within 60 days after commencement of a service, the
 504 state data center may cease service. A service-level agreement
 505 may not have a term exceeding 3 years and at a minimum must:

- 506 1. Identify the parties and their roles, duties, and
 507 responsibilities under the agreement.
- 508 2. State the duration of the contract term and specify the
 509 conditions for renewal.
- 510 3. Identify the scope of work.
- 511 4. Identify the products or services to be delivered with
 512 sufficient specificity to permit an external financial or
 513 performance audit.
- 514 5. Establish the services to be provided, the business
 515 standards that must be met for each service, the cost of each
 516 service by agency application, and the metrics and processes by
 517 which the business standards for each service are to be
 518 objectively measured and reported.
- 519 6. Provide a timely billing methodology to recover the
 520 costs of services provided to the customer entity pursuant to s.
 521 215.422.
- 522 7. Provide a procedure for modifying the service-level
 523 agreement based on changes in the type, level, and cost of a
 524 service.
- 525 8. Include a right-to-audit clause to ensure that the

526 parties to the agreement have access to records for audit
527 purposes during the term of the service-level agreement.

528 9. Provide that a service-level agreement may be
529 terminated by either party for cause only after giving the other
530 party and the department notice in writing of the cause for
531 termination and an opportunity for the other party to resolve
532 the identified cause within a reasonable period.

533 10. Provide for mediation of disputes by the Division of
534 Administrative Hearings pursuant to s. 120.573.

535 (e) For purposes of chapter 273, be the custodian of
536 resources and equipment located in and operated, supported, and
537 managed by the state data center.

538 (f) Assume administrative access rights to resources and
539 equipment, including servers, network components, and other
540 devices, consolidated into the state data center.

541 1. Upon consolidation, a state agency shall relinquish
542 administrative rights to consolidated resources and equipment.
543 State agencies required to comply with federal and state
544 criminal justice information security rules and policies shall
545 retain administrative access rights sufficient to comply with
546 the management control provisions of those rules and policies;
547 however, the state data center shall have the appropriate type
548 or level of rights to allow the center to comply with its duties
549 pursuant to this section. The Department of Law Enforcement
550 shall serve as the arbiter of disputes pertaining to the

551 appropriate type and level of administrative access rights
552 pertaining to the provision of management control in accordance
553 with the federal criminal justice information guidelines.

554 2. The state data center shall provide customer entities
555 with access to applications, servers, network components, and
556 other devices necessary for entities to perform business
557 activities and functions, and as defined and documented in a
558 service-level agreement.

559 (g) In its procurement process, show preference for cloud-
560 computing solutions that minimize or do not require the
561 purchasing, financing, or leasing of state data center
562 infrastructure, and that meet the needs of customer agencies,
563 that reduce costs, and that meet or exceed the applicable state
564 and federal laws, regulations, and standards for cybersecurity.

565 (h) Assist customer entities in transitioning from state
566 data center services to the Northwest Regional Data Center or
567 other third-party cloud-computing services procured by a
568 customer entity or by the Northwest Regional Data Center on
569 behalf of a customer entity.

570 (2) USE OF THE STATE DATA CENTER.—The following are exempt
571 from the use of the state data center: the Department of Law
572 Enforcement, the Department of the Lottery's Gaming System,
573 Systems Design and Development in the Office of Policy and
574 Budget, the regional traffic management centers as described in
575 s. 335.14(2) and the Office of Toll Operations of the Department

576 of Transportation, the State Board of Administration, state
 577 attorneys, public defenders, criminal conflict and civil
 578 regional counsel, capital collateral regional counsel, and the
 579 Florida Housing Finance Corporation.

580 (3) AGENCY LIMITATIONS.—Unless exempt from the use of the
 581 state data center pursuant to this section or authorized by the
 582 Legislature, a state agency may not:

583 (a) Create a new agency computing facility or data center,
 584 or expand the capability to support additional computer
 585 equipment in an existing agency computing facility or data
 586 center; or

587 (b) Terminate services with the state data center without
 588 giving written notice of intent to terminate services 180 days
 589 before such termination.

590 (4) DEPARTMENT RESPONSIBILITIES.—The department shall
 591 provide operational management and oversight of the state data
 592 center, which includes:

593 (a) Implementing industry standards and best practices for
 594 the state data center's facilities, operations, maintenance,
 595 planning, and management processes.

596 (b) Developing and implementing cost-recovery mechanisms
 597 that recover the full direct and indirect cost of services
 598 through charges to applicable customer entities. Such cost-
 599 recovery mechanisms must comply with applicable state and
 600 federal regulations concerning distribution and use of funds and

601 must ensure that, for any fiscal year, no service or customer
602 entity subsidizes another service or customer entity. The
603 department may recommend other payment mechanisms to the
604 Executive Office of the Governor, the President of the Senate,
605 and the Speaker of the House of Representatives. Such mechanisms
606 may be implemented only if specifically authorized by the
607 Legislature.

608 (c) Developing and implementing appropriate operating
609 guidelines and procedures necessary for the state data center to
610 perform its duties pursuant to subsection (1). The guidelines
611 and procedures must comply with applicable state and federal
612 laws, regulations, and policies and conform to generally
613 accepted governmental accounting and auditing standards. The
614 guidelines and procedures must include, but need not be limited
615 to:

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

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

624 3. Providing rebates that may be credited against future
625 billings to customer entities when revenues exceed costs.

626 4. Requiring customer entities to validate that sufficient
 627 funds exist before implementation of a customer entity's request
 628 for a change in the type or level of service provided, if such
 629 change results in a net increase to the customer entity's cost
 630 for that fiscal year.

631 5. By November 15 of each year, providing to the Office of
 632 Policy and Budget in the Executive Office of the Governor and to
 633 the chairs of the legislative appropriations committees the
 634 projected costs of providing data center services for the
 635 following fiscal year.

636 6. Providing a plan for consideration by the Legislative
 637 Budget Commission if the cost of a service is increased for a
 638 reason other than a customer entity's request made pursuant to
 639 subparagraph 4. Such a plan is required only if the service cost
 640 increase results in a net increase to a customer entity for that
 641 fiscal year.

642 7. Standardizing and consolidating procurement and
 643 contracting practices.

644 (d) In collaboration with the Department of Law
 645 Enforcement and the Florida Digital Service, developing and
 646 implementing a process for detecting, reporting, and responding
 647 to cybersecurity incidents, breaches, and threats.

648 (e) Adopting rules relating to the operation of the state
 649 data center, including, but not limited to, budgeting and
 650 accounting procedures, cost-recovery methodologies, and

651 operating procedures.

652 (5) NORTHWEST REGIONAL DATA CENTER CONTRACT.—In order for
653 the department to carry out its duties and responsibilities
654 relating to the state data center, the state chief information
655 officer shall assume responsibility for the contract entered
656 into by the secretary of the department ~~shall contract by July~~
657 ~~1, 2022,~~ with the Northwest Regional Data Center pursuant to s.
658 287.057(11). The contract shall provide that the Northwest
659 Regional Data Center will manage the operations of the state
660 data center and provide data center services to state agencies.
661 Notwithstanding the terms of the contract, the Northwest
662 Regional Data Center must provide the Florida Digital Service
663 with access to information regarding the operations of the state
664 data center.

665 (a) The department shall provide contract oversight,
666 including, but not limited to, reviewing invoices provided by
667 the Northwest Regional Data Center for services provided to
668 state agency customers.

669 (b) The department shall approve or request updates to
670 invoices within 10 business days after receipt. If the
671 department does not respond to the Northwest Regional Data
672 Center, the invoice will be approved by default. The Northwest
673 Regional Data Center must submit approved invoices directly to
674 state agency customers.

675 (6) FLORIDA DIGITAL SERVICE ACCESS.—The state data center,

676 and any successor entity assuming the responsibilities of the
677 state data center including, but not limited to, the Northwest
678 Regional Data Center, shall provide the Florida Digital Service
679 with full access to any infrastructure, system, application, or
680 other means that hosts, supports, or manages data in the custody
681 of an enterprise. For any such infrastructure, system,
682 application, or other means, the state data center or a
683 successor entity shall fully integrate with the Cybersecurity
684 Operations Center.

685 (7) STATE DATA CENTER REPORT.—Subject to s. 119.0725, the
686 state data center and any successor entity must submit to the
687 department and the Florida Digital Service a quarterly report
688 that provides, relating to infrastructure servicing enterprise
689 customers and data, the number of:

690 (a) Technology assets which are within 1 year of end of
691 life as defined by the manufacturer.

692 (b) Technology assets which are beyond end of life as
693 defined by the manufacturer.

694 (c) Technology assets which are within 2 years of being
695 unsupported by the manufacturer.

696 (d) Technology assets which are currently unsupported by
697 the manufacturer.

698 (e) Workloads which are hosted by a commercial cloud
699 service provider as defined in the National Institute of
700 Standards and Technology publication 500-292.

701 (f) Workloads which are not hosted by a commercial entity
 702 which is a cloud service provider as defined in the National
 703 Institute of Standards and Technology publication 500-292.

704 (g) Service level disruptions and average duration of
 705 disruption.

706 Section 6. Subsection (10) of section 282.318, Florida
 707 Statutes, is renumbered as subsection (11), subsections (3) and
 708 (4) are amended, and a new subsection (10) is added to that
 709 section, to read:

710 282.318 Cybersecurity.—

711 (3) The department, acting through the Florida Digital
 712 Service, is the lead entity responsible for establishing
 713 standards and processes for assessing state agency cybersecurity
 714 risks and determining appropriate security measures. Such
 715 standards and processes must be consistent with generally
 716 accepted technology best practices, including the National
 717 Institute for Standards and Technology Cybersecurity Framework,
 718 for cybersecurity. The department, acting through the Florida
 719 Digital Service, shall adopt rules that mitigate risks;
 720 safeguard state agency digital assets, data, information, and
 721 information technology resources to ensure availability,
 722 confidentiality, and integrity; and support a security
 723 governance framework. The department, acting through the Florida
 724 Digital Service, shall also:

725 (a) Designate an employee of the Florida Digital Service

726 as the state chief information security officer. The state chief
727 information security officer must have experience and expertise
728 in security and risk management for communications and
729 information technology resources. The state chief information
730 security officer is responsible for the development, operation,
731 and oversight of cybersecurity for state technology systems. The
732 state chief information security officer shall be notified of
733 all confirmed or suspected incidents or threats of state agency
734 information technology resources and must report such incidents
735 or threats to the state chief information officer and the
736 Governor.

737 (b) Develop, and annually update by February 1, a
738 statewide cybersecurity strategic plan that includes security
739 goals and objectives for cybersecurity, including the
740 identification and mitigation of risk, proactive protections
741 against threats, tactical risk detection, threat reporting, and
742 response and recovery protocols for a cyber incident.

743 (c) Develop and publish for use by state agencies a
744 cybersecurity governance framework that, at a minimum, includes
745 guidelines and processes for:

746 1. Establishing asset management procedures to ensure that
747 an agency's information technology resources are identified and
748 managed consistent with their relative importance to the
749 agency's business objectives.

750 2. Using a standard risk assessment methodology that

751 includes the identification of an agency's priorities,
752 constraints, risk tolerances, and assumptions necessary to
753 support operational risk decisions.

754 3. Completing comprehensive risk assessments and
755 cybersecurity audits, which may be completed by a private sector
756 vendor, and submitting completed assessments and audits to the
757 department.

758 4. Identifying protection procedures to manage the
759 protection of an agency's information, data, and information
760 technology resources.

761 5. Establishing procedures for accessing information and
762 data to ensure the confidentiality, integrity, and availability
763 of such information and data.

764 6. Detecting threats through proactive monitoring of
765 events, continuous security monitoring, and defined detection
766 processes.

767 7. Establishing agency cybersecurity incident response
768 teams and describing their responsibilities for responding to
769 cybersecurity incidents, including breaches of personal
770 information containing confidential or exempt data.

771 8. Recovering information and data in response to a
772 cybersecurity incident. The recovery may include recommended
773 improvements to the agency processes, policies, or guidelines.

774 9. Establishing a cybersecurity incident reporting process
775 that includes procedures for notifying the department and the

776 Department of Law Enforcement of cybersecurity incidents.

777 a. The level of severity of the cybersecurity incident is

778 defined by the National Cyber Incident Response Plan of the

779 United States Department of Homeland Security as follows:

780 (I) Level 5 is an emergency-level incident within the

781 specified jurisdiction that poses an imminent threat to the

782 provision of wide-scale critical infrastructure services;

783 national, state, or local government security; or the lives of

784 the country's, state's, or local government's residents.

785 (II) Level 4 is a severe-level incident that is likely to

786 result in a significant impact in the affected jurisdiction to

787 public health or safety; national, state, or local security;

788 economic security; or civil liberties.

789 (III) Level 3 is a high-level incident that is likely to

790 result in a demonstrable impact in the affected jurisdiction to

791 public health or safety; national, state, or local security;

792 economic security; civil liberties; or public confidence.

793 (IV) Level 2 is a medium-level incident that may impact

794 public health or safety; national, state, or local security;

795 economic security; civil liberties; or public confidence.

796 (V) Level 1 is a low-level incident that is unlikely to

797 impact public health or safety; national, state, or local

798 security; economic security; civil liberties; or public

799 confidence.

800 b. The cybersecurity incident reporting process must

801 specify the information that must be reported by a state agency
 802 following a cybersecurity incident or ransomware incident,
 803 which, at a minimum, must include the following:

804 (I) A summary of the facts surrounding the cybersecurity
 805 incident or ransomware incident.

806 (II) The date on which the state agency most recently
 807 backed up its data; the physical location of the backup, if the
 808 backup was affected; and if the backup was created using cloud
 809 computing.

810 (III) The types of data compromised by the cybersecurity
 811 incident or ransomware incident.

812 (IV) The estimated fiscal impact of the cybersecurity
 813 incident or ransomware incident.

814 (V) In the case of a ransomware incident, the details of
 815 the ransom demanded.

816 c.(I) A state agency shall report all ransomware incidents
 817 and ~~any cybersecurity incidents~~ incident determined by the state
 818 ~~agency to be of severity level 3, 4, or 5~~ to the Florida Digital
 819 Service, the Cybersecurity Operations Center, and the Cybercrime
 820 Office of the Department of Law Enforcement as soon as possible
 821 but no later than 4 ~~48~~ hours after discovery of the
 822 cybersecurity incident and no later than 2 ~~12~~ hours after
 823 discovery of the ransomware incident. The report must contain
 824 the information required in sub-subparagraph b. The Florida
 825 Digital Service shall notify the Governor, the President of the

826 Senate, and the Speaker of the House of Representatives of any
 827 incident discovered by a state agency but not timely reported
 828 under this sub-sub-subparagraph.

829 (II) The Cybersecurity Operations Center shall notify the
 830 President of the Senate and the Speaker of the House of
 831 Representatives of any severity level 3, 4, or 5 incident as
 832 soon as possible but no later than 12 hours after receiving a
 833 state agency's incident report. The notification must include a
 834 high-level description of the incident and the likely effects
 835 and must be provided in a secure environment.

836 ~~d. A state agency shall report a cybersecurity incident~~
 837 ~~determined by the state agency to be of severity level 1 or 2 to~~
 838 ~~the Cybersecurity Operations Center and the Cybercrime Office of~~
 839 ~~the Department of Law Enforcement as soon as possible. The~~
 840 ~~report must contain the information required in sub-subparagraph~~
 841 ~~b.~~

842 ~~e.~~ The Cybersecurity Operations Center shall provide a
 843 consolidated incident report by the 15th day after the end of
 844 each quarter ~~on a quarterly basis~~ to the President of the
 845 Senate, the Speaker of the House of Representatives, and the
 846 Florida Cybersecurity Advisory Council. The report provided to
 847 the Florida Cybersecurity Advisory Council may not contain the
 848 name of any agency, network information, or system identifying
 849 information but must contain sufficient relevant information to
 850 allow the Florida Cybersecurity Advisory Council to fulfill its

851 responsibilities as required in s. 282.319(9).

852 10. Incorporating information obtained through detection
853 and response activities into the agency's cybersecurity incident
854 response plans.

855 11. Developing agency strategic and operational
856 cybersecurity plans required pursuant to this section.

857 12. Establishing the managerial, operational, and
858 technical safeguards for protecting state government data and
859 information technology resources that align with the state
860 agency risk management strategy and that protect the
861 confidentiality, integrity, and availability of information and
862 data.

863 13. Establishing procedures for procuring information
864 technology commodities and services that require the commodity
865 or service to meet the National Institute of Standards and
866 Technology Cybersecurity Framework.

867 14. Submitting after-action reports following a
868 cybersecurity incident or ransomware incident. Such guidelines
869 and processes for submitting after-action reports must be
870 developed and published by December 1, 2022.

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

872 (e) In collaboration with the Cybercrime Office of the
873 Department of Law Enforcement, annually provide training for
874 state agency information security managers and computer security
875 incident response team members that contains training on

876 cybersecurity, including cybersecurity threats, trends, and best
877 practices.

878 (f) Annually review the strategic and operational
879 cybersecurity plans of state agencies.

880 (g) Annually provide cybersecurity training to all state
881 agency technology professionals and employees with access to
882 highly sensitive information which develops, assesses, and
883 documents competencies by role and skill level. The
884 cybersecurity training curriculum must include training on the
885 identification of each cybersecurity incident severity level
886 referenced in sub-subparagraph (c)9.a. The training may be
887 provided in collaboration with the Cybercrime Office of the
888 Department of Law Enforcement, a private sector entity, or an
889 institution of the State University System.

890 (h) Operate and maintain a Cybersecurity Operations Center
891 led by the state chief information security officer, which must
892 be primarily virtual and staffed with tactical detection and
893 incident response personnel. The Cybersecurity Operations Center
894 shall serve as a clearinghouse for threat information and
895 coordinate with the Department of Law Enforcement to support
896 state agencies and their response to any confirmed or suspected
897 cybersecurity incident.

898 (i) Lead an Emergency Support Function, ESF CYBER and
899 DIGITAL, under the state comprehensive emergency management plan
900 as described in s. 252.35.

901 (j) Provide cybersecurity briefings to the members of any
902 legislative committee or subcommittee responsible for policy
903 matters relating to cybersecurity.

904 (k) Have the authority to respond to any state agency
905 cybersecurity incident.

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

907 (a) Designate a chief information security officer to
908 integrate the agency's technical and operational cybersecurity
909 efforts with the Cybersecurity Operations Center. This
910 designation must be provided annually in writing to the Florida
911 Digital Service by January 1. An agency's chief information
912 security officer shall report to the agency's chief information
913 officer. An agency may request the department to procure a chief
914 information security officer as a service to fulfill the
915 agency's duties under this paragraph.

916 (b)-(a) Designate an information security manager to ensure
917 compliance with cybersecurity governance, manage risk, and
918 ensure compliance with the state's incident response plan
919 ~~administer the cybersecurity program of the state agency.~~ This
920 designation must be provided annually in writing to the
921 department by January 15 ~~1~~. A state agency's information
922 security manager, for purposes of these information security
923 duties, shall report directly to the agency head.

924 (c)-(b) In consultation with the department, through the
925 Florida Digital Service, and the Cybercrime Office of the

926 Department of Law Enforcement, and incorporating the resources
927 of the Florida State Guard as appropriate, establish an agency
928 cybersecurity response team to respond to a cybersecurity
929 incident. The agency cybersecurity response team shall convene
930 upon notification of a cybersecurity incident and must
931 immediately report all confirmed or suspected incidents to the
932 state chief information security officer, or his or her
933 designee, and comply with all applicable guidelines and
934 processes established pursuant to paragraph (3) (c).

935 (d)-(e) Submit to the department annually by July 31, the
936 state agency's strategic and operational cybersecurity plans
937 developed pursuant to rules and guidelines established by the
938 department, through the Florida Digital Service.

939 1. The state agency strategic cybersecurity plan must
940 cover a 3-year period and, at a minimum, define security goals,
941 intermediate objectives, and projected agency costs for the
942 strategic issues of agency information security policy, risk
943 management, security training, security incident response, and
944 disaster recovery. The plan must be based on the statewide
945 cybersecurity strategic plan created by the department and
946 include performance metrics that can be objectively measured to
947 reflect the status of the state agency's progress in meeting
948 security goals and objectives identified in the agency's
949 strategic information security plan.

950 2. The state agency operational cybersecurity plan must

951 include a progress report that objectively measures progress
952 made towards the prior operational cybersecurity plan and a
953 project plan that includes activities, timelines, and
954 deliverables for security objectives that the state agency will
955 implement during the current fiscal year.

956 (e)~~(d)~~ Conduct, and update annually by April 30 ~~every 3~~
957 ~~years~~, a comprehensive risk assessment, which may be facilitated
958 by the department or completed by a private sector vendor, to
959 determine the security threats to the data, information, and
960 information technology resources, including mobile devices and
961 print environments, of the agency. The risk assessment must
962 comply with the risk assessment criteria, methodology, and scope
963 developed by the state chief information security officer. The
964 risk assessment findings must be signed by the agency head or
965 the agency head's designee and the Florida Digital Service. The
966 risk assessment methodology developed by the department and is
967 confidential and exempt from s. 119.07(1), except that such
968 information shall be available to the Auditor General, the
969 Florida Digital Service within the department, the Cybercrime
970 Office of the Department of Law Enforcement, and, for state
971 agencies under the jurisdiction of the Governor, the Chief
972 Inspector General. If a private sector vendor is used to
973 complete a comprehensive risk assessment, it must attest to the
974 validity of the risk assessment findings.

975 (f)~~(e)~~ Develop, and periodically update, written internal

976 policies and procedures, which include procedures for reporting
977 cybersecurity incidents and breaches to the Cybercrime Office of
978 the Department of Law Enforcement and the Florida Digital
979 Service within the department. Such policies and procedures must
980 be consistent with the rules, guidelines, and processes
981 established by the department to ensure the security of the
982 data, information, and information technology resources of the
983 agency. The internal policies and procedures that, if disclosed,
984 could facilitate the unauthorized modification, disclosure, or
985 destruction of data or information technology resources are
986 confidential information and exempt from s. 119.07(1), except
987 that such information shall be available to the Auditor General,
988 the Cybercrime Office of the Department of Law Enforcement, the
989 Florida Digital Service within the department, and, for state
990 agencies under the jurisdiction of the Governor, the Chief
991 Inspector General.

992 (g)~~(f)~~ Implement managerial, operational, and technical
993 safeguards and risk assessment remediation plans recommended by
994 the department to address identified risks to the data,
995 information, and information technology resources of the agency.
996 The department, through the Florida Digital Service, shall track
997 implementation by state agencies upon development of such
998 remediation plans in coordination with agency inspectors
999 general.

1000 (h)~~(g)~~ Ensure that periodic internal audits and

1001 evaluations of the agency's cybersecurity program for the data,
 1002 information, and information technology resources of the agency
 1003 are conducted. The results of such audits and evaluations are
 1004 confidential information and exempt from s. 119.07(1), except
 1005 that such information shall be available to the Auditor General,
 1006 the Cybercrime Office of the Department of Law Enforcement, the
 1007 Florida Digital Service within the department, and, for agencies
 1008 under the jurisdiction of the Governor, the Chief Inspector
 1009 General.

1010 (i)~~(h)~~ Ensure that the cybersecurity requirements in the
 1011 written specifications for the solicitation, contracts, and
 1012 service-level agreement of information technology and
 1013 information technology resources and services meet or exceed the
 1014 applicable state and federal laws, regulations, and standards
 1015 for cybersecurity, including the National Institute of Standards
 1016 and Technology Cybersecurity Framework. Service-level agreements
 1017 must identify service provider and state agency responsibilities
 1018 for privacy and security, protection of government data,
 1019 personnel background screening, and security deliverables with
 1020 associated frequencies.

1021 (j)~~(i)~~ Provide cybersecurity awareness training to all
 1022 state agency employees within 30 days after commencing
 1023 employment, and annually thereafter, concerning cybersecurity
 1024 risks and the responsibility of employees to comply with
 1025 policies, standards, guidelines, and operating procedures

1026 adopted by the state agency to reduce those risks. The training
1027 may be provided in collaboration with the Cybercrime Office of
1028 the Department of Law Enforcement, a private sector entity, or
1029 an institution of the State University System.

1030 ~~(k)-(j)~~ Develop a process for detecting, reporting, and
1031 responding to threats, breaches, or cybersecurity incidents
1032 which is consistent with the security rules, guidelines, and
1033 processes established by the department through the Florida
1034 Digital Service.

1035 1. All cybersecurity incidents and ransomware incidents
1036 must be reported by state agencies. Such reports must comply
1037 with the notification procedures and reporting timeframes
1038 established pursuant to paragraph (3) (c).

1039 2. For cybersecurity breaches, state agencies shall
1040 provide notice in accordance with s. 501.171.

1041 ~~(l)-(k)~~ Submit to the Florida Digital Service, within 1
1042 week after the remediation of a cybersecurity incident or
1043 ransomware incident, an after-action report that summarizes the
1044 incident, the incident's resolution, and any insights gained as
1045 a result of the incident.

1046 (10) Any legislative committee or subcommittee responsible
1047 for policy matters relating to cybersecurity may hold meetings
1048 closed by the respective legislative body under the rules of
1049 such legislative body at which such committee or subcommittee is
1050 briefed on records made confidential and exempt under

1051 subsections (5) and (6). The committee or subcommittee must
 1052 maintain the confidential and exempt status of such records.

1053 Section 7. Paragraph (d) of subsection (5) of section
 1054 282.3185, Florida Statutes, is redesignated as paragraph (c),
 1055 and paragraph (b) and present paragraph (c) of that subsection
 1056 are amended to read:

1057 282.3185 Local government cybersecurity.—

1058 (5) INCIDENT NOTIFICATION.—

1059 (b)1. A local government shall report all ransomware
 1060 incidents and ~~any~~ cybersecurity incidents ~~incident determined by~~
 1061 ~~the local government to be of severity level 3, 4, or 5 as~~
 1062 provided in s. 282.318(3)(c) to the Florida Digital Service, the
 1063 Cybersecurity Operations Center, the Cybercrime Office of the
 1064 Department of Law Enforcement, and the sheriff who has
 1065 jurisdiction over the local government as soon as possible but
 1066 no later than 4 ~~48~~ hours after discovery of the cybersecurity
 1067 incident and no later than 2 ~~12~~ hours after discovery of the
 1068 ransomware incident. The report must contain the information
 1069 required in paragraph (a). The Florida Digital Service shall
 1070 notify the Governor, the President of the Senate, and the
 1071 Speaker of the House of Representatives of any incident
 1072 discovered by a local government but not timely reported under
 1073 this subparagraph.

1074 2. The Cybersecurity Operations Center shall notify the
 1075 President of the Senate and the Speaker of the House of

1076 Representatives of any severity level 3, 4, or 5 incident as
 1077 soon as possible but no later than 12 hours after receiving a
 1078 local government's incident report. The notification must
 1079 include a high-level description of the incident and the likely
 1080 effects and must be provided in a secure environment.

1081 ~~(c) A local government may report a cybersecurity incident~~
 1082 ~~determined by the local government to be of severity level 1 or~~
 1083 ~~2 as provided in s. 282.318(3)(c) to the Cybersecurity~~
 1084 ~~Operations Center, the Cybercrime Office of the Department of~~
 1085 ~~Law Enforcement, and the sheriff who has jurisdiction over the~~
 1086 ~~local government. The report shall contain the information~~
 1087 ~~required in paragraph (a).~~

1088 Section 8. Paragraph (j) of subsection (4) of section
 1089 282.319, Florida Statutes, is amended to read:

1090 282.319 Florida Cybersecurity Advisory Council.—

1091 (4) The council shall be comprised of the following
 1092 members:

1093 (j) Three representatives from critical infrastructure
 1094 sectors, ~~one of whom must be from a water treatment facility,~~
 1095 appointed by the Governor.

1096 Section 9. Section 768.401, Florida Statutes, is created
 1097 to read:

1098 768.401 Limitation on liability for cybersecurity
 1099 incidents.—

1100 (1) A county or municipality that substantially complies

1101 with s. 282.3185 is not liable in connection with a
1102 cybersecurity incident.

1103 (2) A sole proprietorship, partnership, corporation,
1104 trust, estate, cooperative, association, or other commercial
1105 entity that acquires, maintains, stores, or uses personal
1106 information is not liable in connection with a cybersecurity
1107 incident if the entity substantially complies with s. 501.171,
1108 if applicable, and has:

1109 (a) Adopted a cybersecurity program that substantially
1110 aligns with the current version of any of the following
1111 standards:

1112 1. The National Institute of Standards and Technology
1113 (NIST) Framework for Improving Critical Infrastructure
1114 Cybersecurity.

1115 2. NIST special publication 800-171.

1116 3. NIST special publications 800-53 and 800-53A.

1117 4. The Federal Risk and Authorization Management Program
1118 security assessment framework.

1119 5. CIS Critical Security Controls.

1120 6. The International Organization for
1121 Standardization/International Electrotechnical Commission 27000-
1122 series family of standards; or

1123 (b) If regulated by the state or Federal Government, or
1124 both, or if otherwise subject to the requirements of any of the
1125 following laws and regulations, substantially complied its

1126 cybersecurity program to the current version of the following,
1127 as applicable:

1128 1. The security requirements of the Health Insurance
1129 Portability and Accountability Act of 1996, 45 C.F.R. part 164
1130 subpart C.

1131 2. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L.
1132 No. 106-102, as amended.

1133 3. The Federal Information Security Modernization Act of
1134 2014, Pub. L. No. 113-283.

1135 4. The Health Information Technology for Economic and
1136 Clinical Health Act, 45 C.F.R. part 162.

1137 (3) The scale and scope of compliance with a standard,
1138 law, or regulation under paragraph (2) (a) or paragraph (2) (b) by
1139 a covered entity, as applicable, is appropriate if it is based
1140 on all of the following factors:

1141 (a) The size and complexity of the covered entity;

1142 (b) The nature and scope of the activities of the covered
1143 entity; and

1144 (c) The sensitivity of the information to be protected.

1145 (4) Any commercial entity covered by subsection (2) that
1146 substantially complies with a combination of industry-recognized
1147 cybersecurity frameworks or standards, including the payment
1148 card industry data security standard, to gain the presumption
1149 against liability pursuant to subsection (2) must, upon the
1150 revision of two or more of the frameworks or standards with

CS/HB 1511

2023

1151 which the entity complies, adopt the revised frameworks or
1152 standards within 1 year after the latest publication date stated
1153 in the revisions.

1154 (5) This section does not establish a private cause of
1155 action. Failure of a county, municipality, or commercial entity
1156 to substantially implement a cybersecurity program that is in
1157 compliance with this section is not evidence of negligence and
1158 does not constitute negligence per se.

1159 (6) In an action in connection with a cybersecurity
1160 incident, if the defendant is an entity covered by subsection
1161 (1) or subsection (2), the defendant has the burden of proof to
1162 establish substantial compliance.

1163 Section 10. This act shall take effect July 1, 2023.