

By the Committee on Appropriations

576-02891-22

20222518__

1 A bill to be entitled
2 An act relating to information technology; providing
3 for a type two transfer of the specified functions and
4 components of the Florida Digital Service to the
5 Executive Office of the Governor; providing for the
6 continuation of certain contracts and interagency
7 agreements; providing that all functions, records,
8 personnel, contracts, interagency agreements, and
9 equipment of the Department of Management Services
10 State Data Center are consolidated in the Northwest
11 Regional Data Center; transferring remaining funds
12 from the Working Capital Trust Fund to the Northwest
13 Regional Data Center for specified purposes; creating
14 s. 14.2017, F.S.; creating the Enterprise Florida
15 First Technology Center within the Executive Office of
16 the Governor; providing for the management of the
17 center by a director; prescribing qualifications of
18 the director and state chief data officer; providing
19 that the center is a separate budget entity;
20 prescribing duties of the center and the director;
21 amending s. 20.22, F.S.; removing the Florida Digital
22 Service from the divisions, programs, and services
23 within the Department of Management Services, to
24 conform to changes made by the act; amending s.
25 282.0041, F.S.; revising the definition of the term
26 "service-level agreement"; amending s. 282.0051, F.S.;
27 creating the Enterprise Florida First Technology
28 Center within the Executive Office of the Governor;
29 deleting references to the Florida Digital Service to

576-02891-22

20222518__

30 conform to changes made by the act; requiring the
31 center to consult with the Department of Management
32 Services to establish an information technology policy
33 for specified procurement activities; requiring the
34 Enterprise Florida First Technology Center to adopt
35 rules; conforming provisions to changes made by the
36 act; repealing s. 282.201, F.S., relating to the state
37 data center; amending s. 282.318, F.S.; designating
38 the Enterprise Florida First Technology Center as the
39 lead entity in state agency cybersecurity matters;
40 requiring the center to adopt certain rules; requiring
41 the center to designate an employee as the state chief
42 information security officer; conforming provisions to
43 changes made by the act; amending s. 282.319, F.S.;

44 housing the Florida Cybersecurity Advisory Council
45 within the Executive Office of the Governor, rather
46 than the Department of Management Services, to conform
47 to changes made by the act; providing that the
48 director of the Office of Policy and Budget, rather
49 than the Secretary of Management Services, is the
50 executive director of advisory council; conforming
51 provisions to changes made by the act; amending s.
52 287.0591, F.S.; requiring the Enterprise Florida First
53 Technology Center to participate in certain
54 solicitations for information technology commodities
55 and services; requiring the Department of Management
56 Services to consult with the Enterprise Florida First
57 Technology Center in prequalifying entities to provide
58 information technology services to the state; amending

576-02891-22

20222518__

59 s. 1004.649, F.S.; designating the Northwest Regional
60 Data Center as the state data center; specifying
61 required duties of the Northwest Regional Data Center;
62 specifying additional requirements for service-level
63 agreements with state agency customers; exempting
64 certain entities from using the data center;
65 prohibiting state agencies from engaging in certain
66 activities, unless otherwise authorized; modifying
67 provisions governing the transition of state agency
68 customers to a cloud-based data center; amending ss.
69 282.00515, 443.1113, and 943.0415, F.S.; conforming a
70 cross reference and provisions to changes made by the
71 act; providing an effective date.

72

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

74

75 Section 1. All powers; duties; functions; records; offices;
76 personnel; associated administrative support positions;
77 property; pending issues and existing contracts; administrative
78 authority; administrative rules in chapter 74, Florida
79 Administrative Code, in effect as of July 1, 2022; and
80 unexpended balances of appropriations and allocations from the
81 General Revenue Fund of the Department of Management Services
82 Florida Digital Service, with the exception of the State Data
83 Center, are transferred by a type two transfer pursuant to s.
84 20.06(2), Florida Statutes, to the Executive Office of the
85 Governor.

86 Section 2. Any contract or interagency agreement existing
87 before July 1, 2022, between the Department of Management

576-02891-22

20222518__

88 Services Florida Digital Service, or any entity or agent of the
89 agency, and any other agency, entity, or person shall continue
90 as a contract or agreement of the successor department or entity
91 responsible for the program, activity, or function relative to
92 the contract or agreement.

93 Section 3. All functions, records, personnel, contracts,
94 interagency agreements, and equipment in the current Department
95 of Management Services State Data Center are consolidated in the
96 Northwest Regional Data Center. The unexpended balance of funds
97 remaining in the Working Capital Trust Fund on June 30, 2022, is
98 transferred to the Northwest Regional Data Center to be used to
99 satisfy customer refunds or excess assessments for fiscal year
100 2021-2022.

101 Section 4. Section 14.2017, Florida Statutes, is created to
102 read:

103 14.2017 Enterprise Florida First Technology Center.-

104 (1) The Enterprise Florida First Technology Center is
105 established within the Executive Office of the Governor, headed
106 for all purposes by a director who holds the title of state
107 chief information officer. The Enterprise Florida First
108 Technology Center shall be a separate budget entity and shall
109 prepare and submit a budget request in accordance with chapter
110 216. The center shall be responsible for all professional,
111 technical, and administrative support functions necessary to
112 carry out its responsibilities under chapter 282. The director
113 of the center shall be appointed by and serves at the pleasure
114 of the Governor and must be a proven, effective administrator
115 who has at least 10 years of executive-level experience in the
116 public or private sector, preferably with experience in the

576-02891-22

20222518__

117 development of information technology strategic planning and the
118 development and implementation of fiscal and substantive
119 information technology policy and standards.

120 (2) The state chief information officer shall designate a
121 state chief data officer. The chief data officer must be a
122 proven and effective administrator who must have significant and
123 substantive experience in data management, data governance,
124 interoperability, and security.

125 (3) The state chief information officer shall facilitate
126 meetings with all state agency chief information officers for
127 the purpose of communication regarding standards, rules,
128 projects, and significant events related to information
129 technology. These meetings must be held at least quarterly.

130 Section 5. Paragraph (b) of subsection (2) of section
131 20.22, Florida Statutes, is amended to read:

132 20.22 Department of Management Services.—There is created a
133 Department of Management Services.

134 (2) The following divisions, programs, and services within
135 the Department of Management Services are established:

136 ~~(b) The Florida Digital Service.~~

137 Section 6. Subsection (30) of section 282.0041, Florida
138 Statutes, is amended to read:

139 282.0041 Definitions.—As used in this chapter, the term:

140 (30) "Service-level agreement" means a written contract
141 between the Department of Management Services or a provider of
142 data center services and a customer entity which specifies the
143 scope of services provided, service level, the duration of the
144 agreement, the responsible parties, and service costs. A
145 service-level agreement is not a rule pursuant to chapter 120.

576-02891-22

20222518__

146 Section 7. Section 282.0051, Florida Statutes, is amended
147 to read:

148 282.0051 Executive Office of the Governor ~~Department of~~
149 ~~Management Services~~; Enterprise Florida First Technology Center
150 ~~Florida Digital Service~~; powers, duties, and functions.—

151 (1) The Enterprise Florida First Technology Center ~~Florida~~
152 ~~Digital Service~~ has been created within the Executive Office of
153 the Governor ~~department~~ to propose innovative solutions that
154 securely modernize state government, including technology and
155 information services, to achieve value through digital
156 transformation and interoperability, and to fully support the
157 cloud-first policy as specified in s. 282.206. The Executive
158 Office of the Governor ~~department~~, through the Enterprise
159 Florida First Technology Center ~~Florida Digital Service~~, shall
160 have the following powers, duties, and functions:

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

163 (b) Develop an enterprise architecture that:

164 1. Acknowledges the unique needs of the entities within the
165 enterprise in the development and publication of standards and
166 terminologies to facilitate digital interoperability;

167 2. Supports the cloud-first policy as specified in s.
168 282.206; and

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

171 (c) Establish project management and oversight standards
172 with which state agencies must comply when implementing
173 information technology projects. The center ~~department~~, ~~acting~~
174 ~~through the Florida Digital Service~~, shall provide training

576-02891-22

20222518__

175 opportunities to state agencies to assist in the adoption of the
176 project management and oversight standards. To support data-
177 driven decisionmaking, the standards must include, but are not
178 limited to:

179 1. Performance measurements and metrics that objectively
180 reflect the status of an information technology project based on
181 a defined and documented project scope, cost, and schedule.

182 2. Methodologies for calculating acceptable variances in
183 the projected versus actual scope, schedule, or cost of an
184 information technology project.

185 3. Reporting requirements, including requirements designed
186 to alert all defined stakeholders that an information technology
187 project has exceeded acceptable variances defined and documented
188 in a project plan.

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

190 5. Technical standards to ensure an information technology
191 project complies with the enterprise architecture.

192 (d) Perform project oversight on all state agency
193 information technology projects that have total project costs of
194 \$10 million or more and that are funded in the General
195 Appropriations Act or any other law. The center ~~department,~~
196 ~~acting through the Florida Digital Service,~~ shall report at
197 least quarterly to ~~the Executive Office of the Governor,~~ the
198 President of the Senate, and the Speaker of the House of
199 Representatives on any information technology project that the
200 center ~~department~~ identifies as high-risk due to the project
201 exceeding acceptable variance ranges defined and documented in a
202 project plan. The report must include a risk assessment,
203 including fiscal risks, associated with proceeding to the next

576-02891-22

20222518__

204 stage of the project, and a recommendation for corrective
205 actions required, including suspension or termination of the
206 project.

207 (e) Identify opportunities for standardization and
208 consolidation of information technology services that support
209 interoperability and the cloud-first policy, as specified in s.
210 282.206, and business functions and operations, including
211 administrative functions such as purchasing, accounting and
212 reporting, cash management, and personnel, and that are common
213 across state agencies. The center department, ~~acting through the~~
214 ~~Florida Digital Service~~, shall biennially on January 1 of each
215 even-numbered year provide recommendations for standardization
216 and consolidation to ~~the Executive Office of the Governor~~, the
217 President of the Senate, and the Speaker of the House of
218 Representatives.

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

223 (g) Develop standards for information technology reports
224 and updates, including, but not limited to, operational work
225 plans, project spend plans, and project status reports, for use
226 by state agencies.

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

229 (i) Conduct annual assessments of state agencies to
230 determine compliance with all information technology standards
231 and guidelines developed and published by the center department
232 and provide results of the assessments to ~~the Executive Office~~

576-02891-22

20222518__

233 ~~of the Governor,~~ the President of the Senate, and the Speaker of
234 the House of Representatives.

235 (j) ~~Provide operational management and oversight of the~~
236 ~~state data center established pursuant to s. 282.201, which~~
237 ~~includes:~~

238 1. ~~Implementing industry standards and best practices for~~
239 ~~the state data center's facilities, operations, maintenance,~~
240 ~~planning, and management processes.~~

241 2. ~~Developing and implementing cost recovery mechanisms~~
242 ~~that recover the full direct and indirect cost of services~~
243 ~~through charges to applicable customer entities. Such cost~~
244 ~~recovery mechanisms must comply with applicable state and~~
245 ~~federal regulations concerning distribution and use of funds and~~
246 ~~must ensure that, for any fiscal year, no service or customer~~
247 ~~entity subsidizes another service or customer entity. The~~
248 ~~Florida Digital Service may recommend other payment mechanisms~~
249 ~~to the Executive Office of the Governor, the President of the~~
250 ~~Senate, and the Speaker of the House of Representatives. Such~~
251 ~~mechanism may be implemented only if specifically authorized by~~
252 ~~the Legislature.~~

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

260 a. ~~Implementing a consolidated administrative support~~
261 ~~structure responsible for providing financial management,~~

576-02891-22

20222518__

262 ~~procurement, transactions involving real or personal property,~~
263 ~~human resources, and operational support.~~

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

268 ~~e. Providing rebates that may be credited against future~~
269 ~~billings to customer entities when revenues exceed costs.~~

270 ~~d. Requiring customer entities to validate that sufficient~~
271 ~~funds exist in the appropriate data processing appropriation~~
272 ~~category or will be transferred into the appropriate data~~
273 ~~processing appropriation category before implementation of a~~
274 ~~customer entity's request for a change in the type or level of~~
275 ~~service provided, if such change results in a net increase to~~
276 ~~the customer entity's cost for that fiscal year.~~

277 ~~e. By November 15 of each year, providing to the Office of~~
278 ~~Policy and Budget in the Executive Office of the Governor and to~~
279 ~~the chairs of the legislative appropriations committees the~~
280 ~~projected costs of providing data center services for the~~
281 ~~following fiscal year.~~

282 ~~f. Providing a plan for consideration by the Legislative~~
283 ~~Budget Commission if the cost of a service is increased for a~~
284 ~~reason other than a customer entity's request made pursuant to~~
285 ~~sub-subparagraph d. Such a plan is required only if the service~~
286 ~~cost increase results in a net increase to a customer entity for~~
287 ~~that fiscal year.~~

288 ~~g. Standardizing and consolidating procurement and~~
289 ~~contracting practices.~~

290 ~~4. Collaborate~~ In collaboration with the Department of Law

576-02891-22

20222518__

291 Enforcement, to develop and implement ~~developing and~~
292 ~~implementing~~ a process for detecting, reporting, and responding
293 to cybersecurity incidents, breaches, and threats.

294 ~~5. Adopting rules relating to the operation of the state~~
295 ~~data center, including, but not limited to, budgeting and~~
296 ~~accounting procedures, cost recovery methodologies, and~~
297 ~~operating procedures.~~

298 (k) Conduct a market analysis not less frequently than
299 every 3 years beginning in 2021 to determine whether the
300 information technology resources within the enterprise are
301 utilized in the most cost-effective and cost-efficient manner,
302 while recognizing that the replacement of certain legacy
303 information technology systems within the enterprise may be cost
304 prohibitive or cost inefficient due to the remaining useful life
305 of those resources; whether the enterprise is complying with the
306 cloud-first policy specified in s. 282.206; and whether the
307 enterprise is utilizing best practices with respect to
308 information technology, information services, and the
309 acquisition of emerging technologies and information services.
310 Each market analysis shall be used to prepare a strategic plan
311 for continued and future information technology and information
312 services for the enterprise, including, but not limited to,
313 proposed acquisition of new services or technologies and
314 approaches to the implementation of any new services or
315 technologies. Copies of each market analysis and accompanying
316 strategic plan must be submitted to ~~the Executive Office of the~~
317 ~~Governor,~~ the President of the Senate, and the Speaker of the
318 House of Representatives not later than December 31 of each year
319 that a market analysis is conducted.

576-02891-22

20222518__

320 (l) Recommend other information technology services that
321 should be designed, delivered, and managed as enterprise
322 information technology services. Recommendations must include
323 the identification of existing information technology resources
324 associated with the services, if existing services must be
325 transferred as a result of being delivered and managed as
326 enterprise information technology services.

327 (m) In consultation with state agencies, propose a
328 methodology and approach for identifying and collecting both
329 current and planned information technology expenditure data at
330 the state agency level.

331 (n)1. Notwithstanding any other law, provide project
332 oversight on any information technology project of the
333 Department of Financial Services, the Department of Legal
334 Affairs, and the Department of Agriculture and Consumer Services
335 which has a total project cost of \$20 million or more. Such
336 information technology projects must also comply with the
337 applicable information technology architecture, project
338 management and oversight, and reporting standards established by
339 the center department, ~~acting through the Florida Digital~~
340 ~~Service~~.

341 2. When performing the project oversight function specified
342 in subparagraph 1., report at least quarterly to ~~the Executive~~
343 ~~Office of the Governor~~, the President of the Senate, and the
344 Speaker of the House of Representatives on any information
345 technology project that the center department, ~~acting through~~
346 ~~the Florida Digital Service~~, identifies as high-risk due to the
347 project exceeding acceptable variance ranges defined and
348 documented in the project plan. The report must ~~shall~~ include a

576-02891-22

20222518__

349 risk assessment, including fiscal risks, associated with
350 proceeding to the next stage of the project and a recommendation
351 for corrective actions required, including suspension or
352 termination of the project.

353 (o) If an information technology project implemented by a
354 state agency must be connected to or otherwise accommodated by
355 an information technology system administered by the Department
356 of Financial Services, the Department of Legal Affairs, or the
357 Department of Agriculture and Consumer Services, consult with
358 these departments regarding the risks and other effects of such
359 projects on their information technology systems and work
360 cooperatively with these departments regarding the connections,
361 interfaces, timing, or accommodations required to implement such
362 projects.

363 (p) If adherence to standards or policies adopted by or
364 established pursuant to this section causes conflict with
365 federal regulations or requirements imposed on an entity within
366 the enterprise and results in adverse action against an entity
367 or federal funding, work with the entity to provide alternative
368 standards, policies, or requirements that do not conflict with
369 the federal regulation or requirement. The center department,
370 ~~acting through the Florida Digital Service~~, shall annually
371 report such alternative standards to ~~the Executive Office of the~~
372 ~~Governor~~, the President of the Senate, and the Speaker of the
373 House of Representatives.

374 (q)1. Establish, in consultation with the department, an
375 information technology policy for all information technology-
376 related state contracts, including state term contracts for
377 information technology commodities, consultant services, and

576-02891-22

20222518__

378 staff augmentation services. The information technology policy
379 must include:

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

382 b. Requirements to be included in solicitations for state
383 term contracts.

384 c. Evaluation criteria for the award of information
385 technology-related state term contracts.

386 d. The term of each information technology-related state
387 term contract.

388 e. The maximum number of vendors authorized on each state
389 term contract.

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

393 g. For an information technology project wherein project
394 oversight is required pursuant to paragraph (d) or paragraph
395 (n), a requirement that independent verification and validation
396 be employed throughout the project life cycle with the primary
397 objective of independent verification and validation being to
398 provide an objective assessment of products and processes
399 throughout the project life cycle. An entity providing
400 independent verification and validation may not have technical,
401 managerial, or financial interest in the project and may not
402 have responsibility for, or participate in, any other aspect of
403 the project.

404 2. Evaluate vendor responses for information technology-
405 related state term contract solicitations and invitations to
406 negotiate.

576-02891-22

20222518__

407 3. Answer vendor questions on information technology-
408 related state term contract solicitations.

409 4. Ensure that the information technology policy
410 established pursuant to subparagraph 1. is included in all
411 solicitations and contracts that are administratively executed
412 by the department.

413 (r) Recommend potential methods for standardizing data
414 across state agencies which will promote interoperability and
415 reduce the collection of duplicative data.

416 (s) Recommend open data technical standards and
417 terminologies for use by the enterprise.

418 (t) Ensure that enterprise information technology solutions
419 are capable of utilizing an electronic credential and comply
420 with the enterprise architecture standards.

421 ~~(2) (a) The Secretary of Management Services shall designate~~
422 ~~a state chief information officer, who shall administer the~~
423 ~~Florida Digital Service. The state chief information officer,~~
424 ~~prior to appointment, must have at least 5 years of experience~~
425 ~~in the development of information system strategic planning and~~
426 ~~development or information technology policy, and, preferably,~~
427 ~~have leadership level experience in the design, development, and~~
428 ~~deployment of interoperable software and data solutions.~~

429 ~~(b) The state chief information officer, in consultation~~
430 ~~with the Secretary of Management Services, shall designate a~~
431 ~~state chief data officer. The chief data officer must be a~~
432 ~~proven and effective administrator who must have significant and~~
433 ~~substantive experience in data management, data governance,~~
434 ~~interoperability, and security.~~

435 ~~(3) The Enterprise Florida First Technology Center~~

576-02891-22

20222518__

436 ~~department, acting through the Florida Digital Service and from~~
437 funds appropriated to the center ~~Florida Digital Service~~, shall:

438 (a) Create, not later than December 1, 2022 ~~October 1,~~
439 ~~2021~~, and maintain a comprehensive indexed data catalog in
440 collaboration with the enterprise that lists the data elements
441 housed within the enterprise and the legacy system or
442 application in which these data elements are located. The data
443 catalog must, at a minimum, specifically identify all data that
444 is restricted from public disclosure based on federal or state
445 laws and regulations and require that all such information be
446 protected in accordance with s. 282.318.

447 (b) Develop and publish, not later than December 1, 2022
448 ~~October 1, 2021~~, in collaboration with the enterprise, a data
449 dictionary for each agency that reflects the nomenclature in the
450 comprehensive indexed data catalog.

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

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

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

460 (f) After submission of documented use cases developed in
461 conjunction with the affected agencies, assist the affected
462 agencies with the deployment, contingent upon a specific
463 appropriation therefor, of new interoperable applications and
464 solutions:

576-02891-22

20222518__

465 1. For the Department of Health, the Agency for Health Care
466 Administration, the Agency for Persons with Disabilities, the
467 Department of Education, the Department of Elderly Affairs, and
468 the Department of Children and Families.

469 2. To support military members, veterans, and their
470 families.

471 (3)~~(4)~~ For information technology projects that have a
472 total project cost of \$10 million or more:

473 (a) State agencies must provide the Enterprise Florida
474 First Technology Center ~~Florida Digital Service~~ with written
475 notice of any planned procurement of an information technology
476 project.

477 (b) The center ~~Florida Digital Service~~ must participate in
478 the development of specifications and recommend modifications to
479 any planned procurement of an information technology project by
480 state agencies so that the procurement complies with the
481 enterprise architecture.

482 (c) The center ~~Florida Digital Service~~ must participate in
483 post-award contract monitoring.

484 (4)~~(5)~~ The Enterprise Florida First Technology Center
485 ~~department, acting through the Florida Digital Service,~~ may not
486 retrieve or disclose any data without a shared-data agreement in
487 place between the center ~~department~~ and the enterprise entity
488 that has primary custodial responsibility of, or data-sharing
489 responsibility for, that data.

490 (5)~~(6)~~ The Enterprise Florida First Technology Center
491 ~~department, acting through the Florida Digital Service,~~ shall
492 adopt rules to administer this section.

493 Section 8. Section 282.201, Florida Statutes, is repealed.

576-02891-22

20222518__

494 Section 9. Subsections (3), (4), (8), and (11) of section
495 282.318, Florida Statutes, are amended to read:

496 282.318 Cybersecurity.-

497 (3) The Enterprise Florida First Technology Center
498 ~~department, acting through the Florida Digital Service,~~ is the
499 lead entity responsible for establishing standards and processes
500 for assessing state agency cybersecurity risks and determining
501 appropriate security measures. Such standards and processes must
502 be consistent with generally accepted technology best practices,
503 including the National Institute for Standards and Technology
504 Cybersecurity Framework, for cybersecurity. The Enterprise
505 Florida First Technology Center ~~department, acting through the~~
506 ~~Florida Digital Service,~~ shall adopt rules that mitigate risks;
507 safeguard state agency digital assets, data, information, and
508 information technology resources to ensure availability,
509 confidentiality, and integrity; and support a security
510 governance framework. The center ~~department, acting through the~~
511 ~~Florida Digital Service,~~ shall also:

512 (a) Designate an employee of the center ~~Florida Digital~~
513 ~~Service~~ as the state chief information security officer. The
514 state chief information security officer must have experience
515 and expertise in security and risk management for communications
516 and information technology resources. The state chief
517 information security officer is responsible for the development,
518 operation, and oversight of cybersecurity for state technology
519 systems. The state chief information security officer shall be
520 notified of all confirmed or suspected incidents or threats of
521 state agency information technology resources and must report
522 such incidents or threats to the state chief information officer

576-02891-22

20222518__

523 and the Governor.

524 (b) Develop, and annually update by February 1, a statewide
525 cybersecurity strategic plan that includes security goals and
526 objectives for cybersecurity, including the identification and
527 mitigation of risk, proactive protections against threats,
528 tactical risk detection, threat reporting, and response and
529 recovery protocols for a cyber incident.

530 (c) Develop and publish for use by state agencies a
531 cybersecurity governance framework that, at a minimum, includes
532 guidelines and processes for:

533 1. Establishing asset management procedures to ensure that
534 an agency's information technology resources are identified and
535 managed consistent with their relative importance to the
536 agency's business objectives.

537 2. Using a standard risk assessment methodology that
538 includes the identification of an agency's priorities,
539 constraints, risk tolerances, and assumptions necessary to
540 support operational risk decisions.

541 3. Completing comprehensive risk assessments and
542 cybersecurity audits, which may be completed by a private sector
543 vendor, and submitting completed assessments and audits to the
544 center ~~department~~.

545 4. Identifying protection procedures to manage the
546 protection of an agency's information, data, and information
547 technology resources.

548 5. Establishing procedures for accessing information and
549 data to ensure the confidentiality, integrity, and availability
550 of such information and data.

551 6. Detecting threats through proactive monitoring of

576-02891-22

20222518__

552 events, continuous security monitoring, and defined detection
553 processes.

554 7. Establishing agency cybersecurity incident response
555 teams and describing their responsibilities for responding to
556 cybersecurity incidents, including breaches of personal
557 information containing confidential or exempt data.

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

561 9. Establishing a cybersecurity incident reporting process
562 that includes procedures and tiered reporting timeframes for
563 notifying the center ~~department~~ and the Department of Law
564 Enforcement of cybersecurity incidents. The tiered reporting
565 timeframes shall be based upon the level of severity of the
566 cybersecurity incidents being reported.

567 10. Incorporating information obtained through detection
568 and response activities into the agency's cybersecurity incident
569 response plans.

570 11. Developing agency strategic and operational
571 cybersecurity plans required pursuant to this section.

572 12. Establishing the managerial, operational, and technical
573 safeguards for protecting state government data and information
574 technology resources that align with the state agency risk
575 management strategy and that protect the confidentiality,
576 integrity, and availability of information and data.

577 13. Establishing procedures for procuring information
578 technology commodities and services that require the commodity
579 or service to meet the National Institute of Standards and
580 Technology Cybersecurity Framework.

576-02891-22

20222518__

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

582 (e) In collaboration with the Cybercrime Office of the
583 Department of Law Enforcement, annually provide training for
584 state agency information security managers and computer security
585 incident response team members that contains training on
586 cybersecurity, including cybersecurity threats, trends, and best
587 practices.

588 (f) Annually review the strategic and operational
589 cybersecurity plans of state agencies.

590 (g) Provide cybersecurity training to all state agency
591 technology professionals that develops, assesses, and documents
592 competencies by role and skill level. The training may be
593 provided in collaboration with the Cybercrime Office of the
594 Department of Law Enforcement, a private sector entity, or an
595 institution of the state university system.

596 (h) Operate and maintain a Cybersecurity Operations Center
597 led by the state chief information security officer, which must
598 be primarily virtual and staffed with tactical detection and
599 incident response personnel. The Cybersecurity Operations Center
600 shall serve as a clearinghouse for threat information and
601 coordinate with the Department of Law Enforcement to support
602 state agencies and their response to any confirmed or suspected
603 cybersecurity incident.

604 (i) Lead an Emergency Support Function, ESF CYBER, under
605 the state comprehensive emergency management plan as described
606 in s. 252.35.

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

608 (a) Designate an information security manager to administer
609 the cybersecurity program of the state agency. This designation

576-02891-22

20222518__

610 must be provided annually in writing to the Enterprise Florida
611 First Technology Center ~~department~~ by January 1. A state
612 agency's information security manager, for purposes of these
613 information security duties, shall report directly to the agency
614 head.

615 (b) In consultation with the center ~~department~~, ~~through the~~
616 ~~Florida Digital Service~~, and the Cybercrime Office of the
617 Department of Law Enforcement, establish an agency cybersecurity
618 response team to respond to a cybersecurity incident. The agency
619 cybersecurity response team shall convene upon notification of a
620 cybersecurity incident and must immediately report all confirmed
621 or suspected incidents to the state chief information security
622 officer, or his or her designee, and comply with all applicable
623 guidelines and processes established pursuant to paragraph
624 (3) (c).

625 (c) Submit to the Executive Office of the Governor
626 ~~department~~ annually by July 31, the state agency's strategic and
627 operational cybersecurity plans developed pursuant to rules and
628 guidelines established by the center ~~department~~, ~~through the~~
629 ~~Florida Digital Service~~.

630 1. The state agency strategic cybersecurity plan must cover
631 a 3-year period and, at a minimum, define security goals,
632 intermediate objectives, and projected agency costs for the
633 strategic issues of agency information security policy, risk
634 management, security training, security incident response, and
635 disaster recovery. The plan must be based on the statewide
636 cybersecurity strategic plan created by the center ~~department~~
637 and include performance metrics that can be objectively measured
638 to reflect the status of the state agency's progress in meeting

576-02891-22

20222518__

639 security goals and objectives identified in the agency's
640 strategic information security plan.

641 2. The state agency operational cybersecurity plan must
642 include a progress report that objectively measures progress
643 made towards the prior operational cybersecurity plan and a
644 project plan that includes activities, timelines, and
645 deliverables for security objectives that the state agency will
646 implement during the current fiscal year.

647 (d) Conduct, and update every 3 years, a comprehensive risk
648 assessment, which may be completed by a private sector vendor,
649 to determine the security threats to the data, information, and
650 information technology resources, including mobile devices and
651 print environments, of the agency. The risk assessment must
652 comply with the risk assessment methodology developed by the
653 center ~~department~~ and is confidential and exempt from s.

654 119.07(1), except that such information shall be available to
655 the Auditor General, the center ~~Florida Digital Service within~~
656 ~~the department~~, the Cybercrime Office of the Department of Law
657 Enforcement, and, for state agencies under the jurisdiction of
658 the Governor, the Chief Inspector General. If a private sector
659 vendor is used to complete a comprehensive risk assessment, it
660 must attest to the validity of the risk assessment findings.

661 (e) Develop, and periodically update, written internal
662 policies and procedures, which include procedures for reporting
663 cybersecurity incidents and breaches to the Cybercrime Office of
664 the Department of Law Enforcement and the center ~~Florida Digital~~
665 ~~Service within the department~~. Such policies and procedures must
666 be consistent with the rules, guidelines, and processes
667 established by the center ~~department~~ to ensure the security of

576-02891-22

20222518__

668 the data, information, and information technology resources of
669 the agency. The internal policies and procedures that, if
670 disclosed, could facilitate the unauthorized modification,
671 disclosure, or destruction of data or information technology
672 resources are confidential information and exempt from s.
673 119.07(1), except that such information shall be available to
674 the Auditor General, the Cybercrime Office of the Department of
675 Law Enforcement, the center ~~Florida Digital Service within the~~
676 ~~department~~, and, for state agencies under the jurisdiction of
677 the Governor, the Chief Inspector General.

678 (f) Implement managerial, operational, and technical
679 safeguards and risk assessment remediation plans recommended by
680 the center ~~department~~ to address identified risks to the data,
681 information, and information technology resources of the agency.
682 The center ~~department, through the Florida Digital Service,~~
683 shall track implementation by state agencies upon development of
684 such remediation plans in coordination with agency inspectors
685 general.

686 (g) Ensure that periodic internal audits and evaluations of
687 the agency's cybersecurity program for the data, information,
688 and information technology resources of the agency are
689 conducted. The results of such audits and evaluations are
690 confidential information and exempt from s. 119.07(1), except
691 that such information shall be available to the Auditor General,
692 the Cybercrime Office of the Department of Law Enforcement, the
693 center ~~Florida Digital Service within the department~~, and, for
694 agencies under the jurisdiction of the Governor, the Chief
695 Inspector General.

696 (h) Ensure that the cybersecurity requirements in the

576-02891-22

20222518__

697 written specifications for the solicitation, contracts, and
698 service-level agreement of information technology and
699 information technology resources and services meet or exceed the
700 applicable state and federal laws, regulations, and standards
701 for cybersecurity, including the National Institute of Standards
702 and Technology Cybersecurity Framework. Service-level agreements
703 must identify service provider and state agency responsibilities
704 for privacy and security, protection of government data,
705 personnel background screening, and security deliverables with
706 associated frequencies.

707 (i) Provide cybersecurity awareness training to all state
708 agency employees in the first 30 days after commencing
709 employment concerning cybersecurity risks and the responsibility
710 of employees to comply with policies, standards, guidelines, and
711 operating procedures adopted by the state agency to reduce those
712 risks. The training may be provided in collaboration with the
713 Cybercrime Office of the Department of Law Enforcement, a
714 private sector entity, or an institution of the state university
715 system.

716 (j) Develop a process for detecting, reporting, and
717 responding to threats, breaches, or cybersecurity incidents
718 which is consistent with the security rules, guidelines, and
719 processes established by the center ~~department through the~~
720 ~~Florida Digital Service~~.

721 1. All cybersecurity incidents and breaches must be
722 reported to the center ~~Florida Digital Service within the~~
723 ~~department~~ and the Cybercrime Office of the Department of Law
724 Enforcement and must comply with the notification procedures and
725 reporting timeframes established pursuant to paragraph (3) (c).

576-02891-22

20222518__

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

728 (8) The portions of records made confidential and exempt in
729 subsections (5), (6), and (7) shall be available to the Auditor
730 General, the Cybercrime Office of the Department of Law
731 Enforcement, the center Florida Digital Service within the
732 ~~department~~, and, for agencies under the jurisdiction of the
733 Governor, the Chief Inspector General. Such portions of records
734 may be made available to a local government, another state
735 agency, or a federal agency for cybersecurity purposes or in
736 furtherance of the state agency's official duties.

737 (11) The Enterprise Florida First Technology Center
738 ~~department~~ shall adopt rules relating to cybersecurity and to
739 administer this section.

740 Section 10. Subsections (1), (3), (6), and (9) of section
741 282.319, Florida Statutes, are amended to read:

742 282.319 Florida Cybersecurity Advisory Council.—

743 (1) The Florida Cybersecurity Advisory Council, an advisory
744 council as defined in s. 20.03(7), is housed ~~created~~ within the
745 Executive Office of the Governor ~~department~~. Except as otherwise
746 provided in this section, the advisory council shall operate in
747 a manner consistent with s. 20.052.

748 (3) The council shall assist the Enterprise Florida First
749 Technology Center ~~Florida Digital Service~~ in implementing best
750 cybersecurity practices, taking into consideration the final
751 recommendations of the Florida Cybersecurity Task Force created
752 under chapter 2019-118, Laws of Florida.

753 (6) The director of the Office of Policy and Budget
754 ~~Secretary of Management Services~~, or his or her designee, shall

576-02891-22

20222518__

755 serve as the ex officio, nonvoting executive director of the
756 council.

757 (9) The council shall meet at least quarterly to:

758 (a) Review existing state agency cybersecurity policies.

759 (b) Assess ongoing risks to state agency information
760 technology.

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

763 (d) Recommend data breach simulation exercises.

764 (e) Assist the Enterprise Florida First Technology Center
765 ~~Florida Digital Service~~ in developing cybersecurity best
766 practice recommendations for state agencies which ~~that~~ include
767 recommendations regarding:

768 1. Continuous risk monitoring.

769 2. Password management.

770 3. Protecting data in legacy and new systems.

771 (f) Examine inconsistencies between state and federal law
772 regarding cybersecurity.

773 Section 11. Subsections (4) and (6) of section 287.0591,
774 Florida Statutes, are amended to read:

775 287.0591 Information technology; vendor disqualification.-

776 (4) If the department issues a competitive solicitation for
777 information technology commodities, consultant services, or
778 staff augmentation contractual services, the Enterprise Florida
779 First Technology Center ~~Florida Digital Service~~ within the
780 Executive Office of the Governor must ~~department shall~~
781 participate in such solicitations.

782 (6) Beginning October 1, 2021, and each October 1
783 thereafter, the department, in consultation with the Enterprise

576-02891-22

20222518__

784 Florida First Technology Center, shall prequalify firms and
785 individuals to provide information technology staff augmentation
786 contractual services on state term contract. In order to
787 prequalify a firm or individual for participation on the state
788 term contract, the department must consider, at a minimum, the
789 capability, experience, and past performance record of the firm
790 or individual. A firm or individual removed from the source of
791 supply pursuant to s. 287.042(1)(b) or placed on a disqualified
792 vendor list pursuant to s. 287.133 or s. 287.134 is immediately
793 disqualified from state term contract eligibility. Once a firm
794 or individual has been prequalified to provide information
795 technology staff augmentation contractual services on state term
796 contract, the firm or individual may respond to requests for
797 quotes from an agency to provide such services.

798 Section 12. Section 1004.649, Florida Statutes, is amended
799 to read:

800 1004.649 Northwest Regional Data Center.—

801 (1) The Northwest Regional Data Center is designated as the
802 state data center and preferred cloud services provider for all
803 state agencies. The Northwest Regional Data Center can provide
804 data center services to state agencies from multiple facilities
805 as funded in the General Appropriations Act.

806 (2) For the purpose of providing data center services to
807 its state agency customers, the Northwest Regional Data Center
808 shall:

809 (a) Operate under a governance structure that represents
810 its customers proportionally.

811 (b) Maintain an appropriate cost-allocation methodology
812 that accurately bills state agency customers based solely on the

576-02891-22

20222518__

813 actual direct and indirect costs of the services provided to
814 state agency customers, and ensures that for any fiscal year,
815 state agency customers are not subsidizing other customers of
816 the data center. Such cost-allocation methodology must comply
817 with applicable state and federal regulations concerning the
818 distribution and use of state and federal funds.

819 (c) Enter into a service-level agreement with each state
820 agency customer to provide services as defined and approved by
821 the governing board of the center. At a minimum, such service-
822 level agreements must:

823 1. Identify the parties and their roles, duties, and
824 responsibilities under the agreement;

825 2. State the duration of the agreement term, which may not
826 exceed 3 years, and specify the conditions for up to two
827 optional 1-year renewals of the agreement before execution of a
828 new agreement renewal;

829 3. Identify the scope of work;

830 4. Establish the services to be provided, the business
831 standards that must be met for each service, the cost of each
832 service, and the process by which the business standards for
833 each service are to be objectively measured and reported;

834 5. Provide a timely billing methodology for recovering the
835 cost of services provided pursuant to s. 215.422;

836 6. Provide a procedure for modifying the service-level
837 agreement to address any changes in projected costs of service;

838 7. Include a right-to-audit clause to ensure that the
839 parties to the agreement have access to records for audit
840 purposes during the term of the service-level agreement ~~Prohibit~~
841 ~~the transfer of computing services between the Northwest~~

576-02891-22

20222518__

842 ~~Regional Data Center and the state data center established~~
843 ~~pursuant to s. 282.201 without at least 180 days' written~~
844 ~~notification of service cancellation;~~

845 8. Identify the products or services to be delivered with
846 sufficient specificity to permit an external financial or
847 performance audit; ~~and~~

848 9. Provide that the service-level agreement may be
849 terminated by either party for cause only after giving the other
850 party notice in writing of the cause for termination and an
851 opportunity for the other party to resolve the identified cause
852 within a reasonable period; and

853 10. Provide state agency customer entities with access to
854 application, servers, network components, and other devices
855 necessary for entities to perform business activities and
856 functions and as defined and documented in a service-level
857 agreement.

858 (d) In its procurement process, show preference for cloud-
859 based computing solutions that minimize or do not require the
860 purchasing, financing, or leasing of state data center
861 infrastructure, that meet the needs of state agency customer
862 entities that reduce costs, and that meet or exceed the
863 applicable state and federal laws, regulations, and standards
864 for cybersecurity.

865 (e) Assist state agency customer entities in transitioning
866 from state data center services to third-party cloud-based
867 computing services procured by a customer entity or by the
868 Northwest Regional Data Center on behalf of the customer entity.

869 (f) Provide to the Board of Governors the total annual
870 budget by major expenditure category, including, but not limited

576-02891-22

20222518__

871 to, salaries, expenses, operating capital outlay, contracted
872 services, or other personnel services by July 30 each fiscal
873 year.

874 (g)~~(e)~~ Provide to each state agency customer its projected
875 annual cost for providing the agreed-upon data center services
876 by September 1 each fiscal year.

877 (h)~~(f)~~ Provide a plan for consideration by the Legislative
878 Budget Commission if the governing body of the center approves
879 the use of a billing rate schedule after the start of the fiscal
880 year that increases any state agency customer's costs for that
881 fiscal year.

882 (i) Provide data center services that comply with
883 applicable state and federal laws, regulations, and policies,
884 including all applicable security, privacy, and auditing
885 requirements.

886 (j) Maintain performance of the data center facilities by
887 ensuring proper data backup, data backup recovery, disaster
888 recovery, and appropriate security, power, cooling, fire
889 suppression, and capacity.

890 (3) The following entities are exempt from the requirement
891 to use the Northwest Regional Data Center:

892 (a) The Department of Law Enforcement.

893 (b) The Department of the Lottery's Gaming System.

894 (c) Systems Design and Development in the Office of Policy
895 and Budget.

896 (d) The regional traffic management centers described in s.
897 335.14(2) and the Office of Toll Operations of the Department of
898 Transportation.

899 (e) The State Board of Administration.

576-02891-22

20222518__

900 (f) The offices of the state attorneys, public defenders,
901 criminal conflict and regional counsels, and the capital
902 collateral regional counsel.

903 (g) The Florida Housing Finance Corporation.

904 (4) Unless exempt from the requirement to use the Northwest
905 Regional Data Center pursuant to this section or as authorized
906 by the Legislature, a state agency may not do any of the
907 following:

908 (a) Create a new agency computing facility or data center
909 or expand the capability to support additional computer
910 equipment in an existing agency computing facility or data
911 center.

912 (b) Terminate services with the Northwest Regional Data
913 Center without giving written notice of intent to terminate
914 services 180 days before such termination.

915 (c) Procure third-party cloud-based computing services
916 without evaluating the cloud-based computing services provided
917 by the Northwest Regional Data Center.

918 (5) ~~(2)~~ The Northwest Regional Data Center's authority to
919 provide data center services to its state agency customers may
920 be terminated if:

921 (a) The center requests such termination to the Board of
922 Governors, the Senate President, and the Speaker of the House of
923 Representatives; or

924 (b) The center fails to comply with the provisions of this
925 section.

926 (6) ~~(3)~~ If such authority is terminated, the center has
927 ~~shall have~~ 1 year to provide for the transition of its state
928 agency customers to a qualified alternative cloud-based data

576-02891-22

20222518__

929 center that meets the enterprise architecture standards
930 established by the Enterprise Florida First Technology Center
931 ~~the state data center established pursuant to s. 282.201.~~

932 Section 13. Subsections (1) and (4) of section 282.00515,
933 Florida Statutes, are amended to read:

934 282.00515 Duties of Cabinet agencies.—

935 (1) The Department of Legal Affairs, the Department of
936 Financial Services, and the Department of Agriculture and
937 Consumer Services shall adopt the standards established in s.
938 282.0051(1)(b), (c), and (s) and (2)(e) ~~(3)(e)~~ or adopt
939 alternative standards based on best practices and industry
940 standards that allow for open data interoperability.

941 (4)(a) Nothing in this section or in s. 282.0051 requires
942 the Department of Legal Affairs, the Department of Financial
943 Services, or the Department of Agriculture and Consumer Services
944 to integrate with information technology outside its own
945 department or with the Enterprise Florida First Technology
946 Center Florida Digital Service.

947 (b) The center department, ~~acting through the Florida~~
948 ~~Digital Service~~, may not retrieve or disclose any data without a
949 shared-data agreement in place between the center department and
950 the Department of Legal Affairs, the Department of Financial
951 Services, or the Department of Agriculture and Consumer
952 Services.

953 Section 14. Subsection (4) of section 443.1113, Florida
954 Statutes, is amended to read:

955 443.1113 Reemployment Assistance Claims and Benefits
956 Information System.—

957 (4)(a) The Department of Economic Opportunity shall perform

576-02891-22

20222518__

958 an annual review of the system and identify enhancements or
959 modernization efforts that improve the delivery of services to
960 claimants and employers and reporting to state and federal
961 entities. These improvements must include, but need not be
962 limited to:

- 963 1. Infrastructure upgrades through cloud services.
- 964 2. Software improvements.
- 965 3. Enhanced data analytics and reporting.
- 966 4. Increased cybersecurity pursuant to s. 282.318.

967 (b) The department shall seek input on recommended
968 enhancements from, at a minimum, the following entities:

969 1. The Enterprise Florida First Technology Center ~~Florida~~
970 ~~Digital Service~~ within the Executive Office of the Governor
971 ~~Department of Management Services~~.

972 2. The General Tax Administration Program Office within the
973 Department of Revenue.

974 3. The Division of Accounting and Auditing within the
975 Department of Financial Services.

976 Section 15. Subsection (5) of section 943.0415, Florida
977 Statutes, is amended to read:

978 943.0415 Cybercrime Office.—There is created within the
979 Department of Law Enforcement the Cybercrime Office. The office
980 may:

981 (5) Consult with the Enterprise Florida First Technology
982 Center ~~Florida Digital Service~~ within the Executive Office of
983 the Governor ~~Department of Management Services~~ in the adoption
984 of rules relating to the information technology security
985 provisions in s. 282.318.

986 Section 16. This act shall take effect July 1, 2022.