

1                   A bill to be entitled  
2           An act relating to state agency information technology  
3           reorganization; transferring all powers, duties,  
4           functions, records, offices, personnel, associated  
5           administrative support positions, property, pending  
6           issues and existing contracts, administrative  
7           authority, certain administrative rules, trust funds,  
8           and unexpended balances of appropriations,  
9           allocations, and other funds of the state data center  
10          within the Agency for State Technology to the  
11          Department of Management Services and the Agency for  
12          State Technology to the Office of Technology and Data  
13          Solutions, respectively, by a type two transfer;  
14          providing that untransferred rules of the Agency for  
15          State Technology are repealed; providing that certain  
16          binding contracts and interagency agreements continue  
17          for remainder of terms; amending ss. 17.0315 and  
18          20.055, F.S.; conforming provisions to changes made by  
19          the act; amending s. 20.22, F.S.; establishing the  
20          State Data Center Program and the Office of Technology  
21          and Data Solutions within the Department of Management  
22          Services; repealing s. 20.61, F.S., relating to the  
23          Agency for State Technology; amending ss. 97.0525,  
24          110.205, 215.322, 215.96, and 216.292, F.S.;  
25          conforming provisions to changes made by the act;

26 | amending s. 282.003, F.S.; revising a short title;  
27 | amending s. 282.0041, F.S.; revising and providing  
28 | definitions; amending s. 282.0051, F.S.; transferring  
29 | powers, duties, and functions of the Agency for State  
30 | Technology to the Office of Technology and Data  
31 | Solutions and revising such powers, duties, and  
32 | functions; providing for the appointment of and  
33 | requirements for the state chief information officer,  
34 | the chief data officer, and the chief information  
35 | security officer; removing requirements that the  
36 | office publish certain policies and standards;  
37 | removing a requirement that the office provide certain  
38 | training opportunities to state agencies; requiring  
39 | the office to review state agency project oversight  
40 | deliverables and provide certain recommendations to  
41 | the Governor and the Legislature; requiring state  
42 | agencies to submit project oversight deliverables to  
43 | the office for certain information technology  
44 | projects; removing certain reporting requirements;  
45 | requiring the office, in collaboration with the  
46 | department, to recommend best practices for the  
47 | procurement of commercial cloud computing services and  
48 | an information technology policy for information  
49 | technology-related state contracts; requiring the  
50 | development of and providing requirements for an

51 enterprise data inventory; removing a requirement that  
52 the office conduct certain annual assessments;  
53 removing a requirement that the office provide  
54 operational management and oversight of the state data  
55 center; removing requirements that the office make  
56 certain recommendations; removing a requirement that  
57 the office provide project oversight on certain  
58 information technology projects of specified  
59 departments; amending s. 282.00515, F.S.; requiring  
60 specified departments to adopt certain standards and  
61 authorizing such departments to consult with the  
62 office; requiring specified departments to submit  
63 project oversight deliverables to the office for  
64 certain information technology projects; conforming a  
65 cross-reference; amending s. 282.201, F.S.;

66 transferring the state data center from the Agency for  
67 State Technology to the Department of Management  
68 Services and revising state data center duties;  
69 revising the method of hosting data center services;  
70 requiring the Secretary of Management Services to  
71 appoint a director of the state data center; deleting  
72 legislative intent; requiring the state data center to  
73 develop and implement necessary operating guidelines  
74 and procedures for a cost recovery mechanism;  
75 requiring the state data center, in collaboration with

76 | the Department of Law Enforcement, to develop and  
77 | implement a process for detecting, reporting, and  
78 | responding to information technology security  
79 | incidents, breaches, and threats; requiring the state  
80 | data center to establish a commercial cloud computing  
81 | services in certain circumstances; requiring the state  
82 | data center to provide a biennial report on the use of  
83 | cloud computing by state agency customer entities to  
84 | the Governor, the Legislature, and the Office of  
85 | Technology and Data Solutions; removing obsolete  
86 | language; creating s. 282.206, F.S.; requiring a state  
87 | agency customer entity to notify the state data center  
88 | biannually of changes in anticipated use of state data  
89 | center services; requiring a state agency customer  
90 | entity to develop a plan that includes specified  
91 | elements to address its applications located at the  
92 | state data center; requiring the use of commercial  
93 | cloud computing services in certain circumstances;  
94 | amending ss. 282.318, 287.057, 287.0591, 445.011,  
95 | 445.045, 668.50, and 943.0415, F.S.; conforming  
96 | provisions to changes made by the act; creating the  
97 | Florida Cybersecurity Task Force; providing membership  
98 | and duties of the task force; requiring the  
99 | cooperation of executive branch departments and  
100 | agencies; requiring a report to be submitted to the

101 Governor and the Legislature; providing for  
102 expiration; specifying that certain transfers do not  
103 require Legislative Budget Commission approval;  
104 providing appropriations; providing for the allocation  
105 of appropriated funds; providing an effective date.  
106

107 Be It Enacted by the Legislature of the State of Florida:  
108

109 Section 1. All powers; duties; functions; records;  
110 offices; personnel; associated administrative support positions;  
111 property; pending issues and existing contracts; administrative  
112 authority; administrative rules in chapter 74-3, Florida  
113 Administrative Code, in effect as of July 16, 2016; trust funds;  
114 and unexpended balances of appropriations, allocations, and  
115 other funds of the state data center, including data center  
116 administration, within the Agency for State Technology are  
117 transferred by a type two transfer pursuant to s. 20.06(2),  
118 Florida Statutes, to the Department of Management Services.

119 Section 2. All powers; duties; functions; records;  
120 offices; property; pending issues and existing contracts;  
121 administrative authority; administrative rules in chapters 74-1  
122 and 74-2, Florida Administrative Code, in effect as of August 1,  
123 2016; and unexpended balances of appropriations, allocations,  
124 and other funds of the executive direction entity of the Agency  
125 for State Technology are transferred by a type two transfer

126 pursuant to s. 20.06(2), Florida Statutes, to the Office of  
 127 Technology and Data Solutions, established in s. 20.22(2),  
 128 Florida Statutes, as amended by this act, within the Department  
 129 of Management Services.

130 Section 3. Except for those rules in chapters 74-1, 74-2,  
 131 and 74-3, Florida Administrative Code, transferred pursuant to  
 132 sections 1 and 2, other rules adopted by the Agency for State  
 133 Technology, if any, are repealed, and the Department of State  
 134 shall update the Florida Administrative Code to remove them.

135 Section 4. Any binding contract or interagency agreement  
 136 existing before July 1, 2017, between the Agency for State  
 137 Technology or any entity or agent of the agency, and any other  
 138 agency, entity, or person shall continue as a binding contract  
 139 or agreement for the remainder of the term of such contract or  
 140 agreement on the successor department or entity responsible for  
 141 the program, activity, or function relative to the contract or  
 142 agreement.

143 Section 5. Subsection (1) of section 17.0315, Florida  
 144 Statutes, is amended to read:

145 17.0315 Financial and cash management system; task force.—

146 (1) The Chief Financial Officer, as the constitutional  
 147 officer responsible for settling and approving accounts against  
 148 the state and keeping all state funds pursuant to s. 4, Art. IV  
 149 of the State Constitution, is the head of and shall appoint  
 150 members to a task force established to develop a strategic

151 business plan for a successor financial and cash management  
152 system. The task force shall include the state chief information  
153 officer ~~executive director of the Agency for State Technology~~  
154 and the director of the Office of Policy and Budget in the  
155 Executive Office of the Governor. Any member of the task force  
156 may appoint a designee.

157 Section 6. Paragraph (d) of subsection (1) of section  
158 20.055, Florida Statutes, is amended to read:

159 20.055 Agency inspectors general.—

160 (1) As used in this section, the term:

161 (d) "State agency" means each department created pursuant  
162 to this chapter and the Executive Office of the Governor, the  
163 Department of Military Affairs, the Fish and Wildlife  
164 Conservation Commission, the Office of Insurance Regulation of  
165 the Financial Services Commission, the Office of Financial  
166 Regulation of the Financial Services Commission, the Public  
167 Service Commission, the Board of Governors of the State  
168 University System, the Florida Housing Finance Corporation, ~~the~~  
169 ~~Agency for State Technology~~, the Office of Early Learning, and  
170 the state courts system.

171 Section 7. Subsection (2) of section 20.22, Florida  
172 Statutes, is amended to read:

173 20.22 Department of Management Services.—There is created  
174 a Department of Management Services.

175 (2) The following divisions, office, and programs within

176 | the Department of Management Services are established:

177 |       (a) Facilities Program.

178 |       (b)1. Technology Program.

179 |       2. State Data Center Program.

180 |       (c) Workforce Program.

181 |       (d)1. Support Program.

182 |       2. Federal Property Assistance Program.

183 |       (e) Administration Program.

184 |       (f) Division of Administrative Hearings.

185 |       (g) Division of Retirement.

186 |       (h) Division of State Group Insurance.

187 |       (i) Office of Technology and Data Solutions.

188 |       Section 8. Section 20.61, Florida Statutes, is repealed.

189 |       Section 9. Paragraph (b) of subsection (3) of section

190 | 97.0525, Florida Statutes, is amended to read:

191 |       97.0525 Online voter registration.—

192 |       (3)

193 |       (b) The division shall conduct a comprehensive risk  
 194 | assessment of the online voter registration system before making  
 195 | the system publicly available and every 2 years thereafter. The  
 196 | comprehensive risk assessment must comply with the risk  
 197 | assessment methodology developed by the Office of Technology and  
 198 | Data Solutions ~~Agency for State Technology~~ for identifying  
 199 | security risks, determining the magnitude of such risks, and  
 200 | identifying areas that require safeguards.

HB 5301

2017

201 Section 10. Paragraph (e) of subsection (2) of section  
202 110.205, Florida Statutes, is amended to read:

203 110.205 Career service; exemptions.—

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

206 (e) The state chief information officer ~~executive director~~  
207 ~~of the Agency for State Technology~~. Unless otherwise fixed by  
208 law, the Office of Technology and Data Solutions ~~Agency for~~  
209 ~~State Technology~~ shall set the salary and benefits of this  
210 position in accordance with the rules of the Senior Management  
211 Service.

212 Section 11. Subsections (2) and (9) of section 215.322,  
213 Florida Statutes, are amended to read:

214 215.322 Acceptance of credit cards, charge cards, debit  
215 cards, or electronic funds transfers by state agencies, units of  
216 local government, and the judicial branch.—

217 (2) A state agency as defined in s. 216.011, or the  
218 judicial branch, may accept credit cards, charge cards, debit  
219 cards, or electronic funds transfers in payment for goods and  
220 services with the prior approval of the Chief Financial Officer.  
221 If the Internet or other related electronic methods are to be  
222 used as the collection medium, the Office of Technology and Data  
223 Solutions ~~Agency for State Technology~~ shall review and recommend  
224 to the Chief Financial Officer whether to approve the request  
225 with regard to the process or procedure to be used.

226 (9) For payment programs in which credit cards, charge  
 227 cards, or debit cards are accepted by state agencies, the  
 228 judicial branch, or units of local government, the Chief  
 229 Financial Officer, in consultation with the Office of Technology  
 230 and Data Solutions ~~Agency for State Technology~~, may adopt rules  
 231 to establish uniform security safeguards for cardholder data and  
 232 to ensure compliance with the Payment Card Industry Data  
 233 Security Standards.

234 Section 12. Subsection (2) of section 215.96, Florida  
 235 Statutes, is amended to read:

236 215.96 Coordinating council and design and coordination  
 237 staff.—

238 (2) The coordinating council shall consist of the Chief  
 239 Financial Officer; the Commissioner of Agriculture; the Attorney  
 240 General; the Secretary of Management Services; the state chief  
 241 information officer ~~executive director of the Agency for State~~  
 242 ~~Technology~~; and the Director of Planning and Budgeting,  
 243 Executive Office of the Governor, or their designees. The Chief  
 244 Financial Officer, or his or her designee, shall be chair of the  
 245 council, and the design and coordination staff shall provide  
 246 administrative and clerical support to the council and the  
 247 board. The design and coordination staff shall maintain the  
 248 minutes of each meeting and make such minutes available to any  
 249 interested person. The Auditor General, the State Courts  
 250 Administrator, an executive officer of the Florida Association

251 of State Agency Administrative Services Directors, and an  
252 executive officer of the Florida Association of State Budget  
253 Officers, or their designees, shall serve without voting rights  
254 as ex officio members of the council. The chair may call  
255 meetings of the council as often as necessary to transact  
256 business; however, the council shall meet at least once a year.  
257 Action of the council shall be by motion, duly made, seconded  
258 and passed by a majority of the council voting in the  
259 affirmative for approval of items that are to be recommended for  
260 approval to the Financial Management Information Board.

261 Section 13. Subsection (9) of section 216.292, Florida  
262 Statutes, is renumbered as subsection (8), and present  
263 subsection (8) of that section is amended to read:

264 216.292 Appropriations nontransferable; exceptions.—

265 ~~(8) Notwithstanding subsections (2), (3), and (4), and for~~  
266 ~~the 2015-2016 fiscal year only, the Agency for State Technology,~~  
267 ~~with the approval of the Executive Office of the Governor, and~~  
268 ~~after 14 days prior notice, may transfer up to \$2.5 million of~~  
269 ~~recurring funds from the Working Capital Trust Fund within the~~  
270 ~~Agency for State Technology between appropriations categories~~  
271 ~~for operations, as needed, to realign funds, based upon the~~  
272 ~~final report of the third-party assessment required by January~~  
273 ~~15, 2016, to begin migration of cloud-ready applications at the~~  
274 ~~State Data Center to a cloud solution that complies with all~~  
275 ~~applicable federal and state security and privacy requirements,~~

HB 5301

2017

276 ~~to the extent feasible within available resources, while~~  
277 ~~continuing to provide computing services for existing data~~  
278 ~~center applications, until those applications can be cloud-~~  
279 ~~ready. Such transfers are subject to the notice and objection~~  
280 ~~provisions of s. 216.177. This subsection expires July 1, 2016.~~

281 Section 14. Section 282.003, Florida Statutes, is amended  
282 to read:

283 282.003 Short title.—This part may be cited as the  
284 ~~"Enterprise Information Technology Services Management Act."~~

285 Section 15. Subsections (2) and (3) of section 282.0041,  
286 Florida Statutes, are renumbered as subsections (3) and (4),  
287 respectively, present subsections (4) and (5) are renumbered as  
288 subsections (6) and (7), respectively, present subsections (6)  
289 and (7) are renumbered as subsections (11) and (12),  
290 respectively, present subsections (9) through (14) are  
291 renumbered as subsections (13) through (18), respectively,  
292 present subsections (15) through (28) are renumbered as  
293 subsections (21) through (33), respectively, present subsections  
294 (2), (8), and (10) are amended, and new subsections (2), (5),  
295 (8), (9), (10), (19), and (20) are added to that section, to  
296 read:

297 282.0041 Definitions.—As used in this chapter, the term:

298 (2) "Application programming interface" means a set of  
299 programming instructions and standards for accessing a web-based  
300 software application.

301        (3) (2) "Breach" has the same meaning as provided in s.  
302 501.171 means a confirmed event that compromises the  
303 confidentiality, integrity, or availability of information or  
304 data.

305        (5) "Cloud computing" has the same meaning as provided in  
306 Special Publication 800-145 issued by the National Institute of  
307 Standards and Technology.

308        (8) "Data" means a subset of structured information in a  
309 format that allows such information to be electronically  
310 retrieved and transmitted.

311        (9) "Data catalog" means a collection of descriptions of  
312 datasets.

313        (10) "Dataset" means an organized collection of related  
314 data held in an electronic format.

315        ~~(8) "Enterprise information technology service" means an~~  
316 ~~information technology service that is used in all agencies or a~~  
317 ~~subset of agencies and is established in law to be designed,~~  
318 ~~delivered, and managed at the enterprise level.~~

319        (14) (10) "Incident" means a violation or imminent threat  
320 of violation, whether such violation is accidental or  
321 deliberate, of information technology resources, security  
322 policies, acceptable use policies, or ~~standard security~~  
323 practices. An imminent threat of violation refers to a situation  
324 in which the state agency has a factual basis for believing that  
325 a specific incident is about to occur.

326        (19) "Machine-readable" means data that is in a format  
 327 that can be easily processed by a computer without human  
 328 intervention.

329        (20) "Open data" means data collected or created by a  
 330 state agency and structured in a way that enables the data to be  
 331 fully discoverable and usable by the public. The term does not  
 332 include data that is restricted from public distribution based  
 333 on federal or state privacy, confidentiality, and security laws  
 334 and regulations or data for which a state agency is statutorily  
 335 authorized to assess a fee for its distribution.

336        Section 16. Section 282.0051, Florida Statutes, is amended  
 337 to read:

338        282.0051 Office of Technology and Data Solutions ~~Agency~~  
 339 ~~for State Technology;~~ powers, duties, and functions.—The Office  
 340 of Technology and Data Solutions within the Department of  
 341 Management Services shall be headed by the state chief  
 342 information officer who shall be appointed by the Governor and  
 343 confirmed by the Senate. The state chief information officer  
 344 must be a proven, effective administrator with at least 10 years  
 345 of executive-level experience in either the public or private  
 346 sector with experience in the development of information  
 347 technology strategic planning and the development and  
 348 implementation of fiscal and substantive information technology  
 349 policy and standards. The office shall be a separate budget  
 350 entity and shall not be subject to control, supervision, or

351 direction by the Department of Management Services in any  
352 manner, including, but not limited to, personnel, purchasing,  
353 and budgetary matters. The state chief information officer shall  
354 appoint a chief data officer who must have experience in the  
355 development and implementation of open data initiatives. The  
356 state chief information officer shall appoint a chief  
357 information security officer who must have experience and  
358 expertise in security and risk management for communications and  
359 information technology resources. The office ~~Agency for State~~  
360 ~~Technology~~ shall have the following powers, duties, and  
361 functions:

362 (1) Develop and recommend ~~publish~~ information technology  
363 policy for the management of the state's information technology  
364 resources.

365 (2) Recommend information technology improvements for the  
366 delivery of state government services and ~~Establish and publish~~  
367 ~~information technology architecture standards to provide for the~~  
368 ~~most efficient use of the state's information technology~~  
369 ~~resources and to ensure compatibility and alignment with the~~  
370 ~~needs of state agencies. The agency shall assist state agencies~~  
371 ~~in complying with the standards.~~

372 (3) ~~By June 30, 2015,~~ Establish project management and  
373 oversight standards with which state agencies must comply when  
374 implementing information technology projects. ~~The agency shall~~  
375 ~~provide training opportunities to state agencies to assist in~~

376 ~~the adoption of the project management and oversight standards.~~

377 To support data-driven decisionmaking, the standards must

378 include, but are not limited to:

379 (a) Performance measurements and metrics that objectively  
380 reflect the status of an information technology project based on  
381 a defined and documented project scope, cost, and schedule.

382 (b) Methodologies for calculating acceptable variances in  
383 the projected versus actual scope, schedule, or cost of an  
384 information technology project.

385 (c) Reporting requirements, including requirements  
386 designed to alert all defined stakeholders that an information  
387 technology project has exceeded acceptable variances defined and  
388 documented in a project plan.

389 (d) Project management documentation, including, but not  
390 limited to, operational work plans, project spend plans, and  
391 project status reports, for use by state agencies.

392 (e) ~~(d)~~ Content, format, and frequency of project updates.

393 (4) (a) Review state agency project oversight deliverables  
394 and provide recommendations as necessary to the Governor, the  
395 President of the Senate, and the Speaker of the House of  
396 Representatives for the improvement of state agency information  
397 technology projects and project oversight. Beginning January 1,  
398 2018, except as otherwise provided by law, state agencies shall  
399 submit project oversight deliverables to the Office of  
400 Technology and Data Solutions for 2015, perform project

401 ~~oversight on all state agency~~ information technology projects  
402 that have total project costs of \$10 million or more and that  
403 are funded in the General Appropriations Act or any other law.  
404 ~~The agency shall report at least quarterly to the Executive~~  
405 ~~Office of the Governor, the President of the Senate, and the~~  
406 ~~Speaker of the House of Representatives on any information~~  
407 ~~technology project that the agency identifies as high-risk due~~  
408 ~~to the project exceeding acceptable variance ranges defined and~~  
409 ~~documented in a project plan. The report must include a risk~~  
410 ~~assessment, including fiscal risks, associated with proceeding~~  
411 ~~to the next stage of the project, and a recommendation for~~  
412 ~~corrective actions required, including suspension or termination~~  
413 ~~of the project.~~

414 (b) Review project oversight deliverables that are  
415 submitted to the Office of Technology and Data Solutions by the  
416 Department of Financial Services, the Department of Legal  
417 Affairs, and the Department of Agriculture and Consumer Services  
418 for information technology projects that have total project  
419 costs of \$25 million or more and that impact one or more other  
420 agencies and provide recommendations as necessary to the  
421 Governor, the President of the Senate, and the Speaker of the  
422 House of Representatives for the improvement of such projects  
423 and project oversight.

424 (c) If an information technology project implemented by a  
425 state agency must be connected to or otherwise accommodated by

426 an information technology system administered by the Department  
427 of Financial Services, the Department of Legal Affairs, or the  
428 Department of Agriculture and Consumer Services, consult with  
429 the department regarding the risks and other effects of such  
430 project on their information technology system and work  
431 cooperatively with the department regarding the connections,  
432 interfaces, timing, or accommodations required to implement such  
433 project.

434 ~~(5) By April 1, 2016, and biennially thereafter, identify~~  
435 ~~opportunities for standardization and consolidation of~~  
436 ~~information technology services that support business functions~~  
437 ~~and operations, including administrative functions such as~~  
438 ~~purchasing, accounting and reporting, cash management, and~~  
439 ~~personnel, and that are common across state agencies. The agency~~  
440 ~~shall provide recommendations for standardization and~~  
441 ~~consolidation to the Executive Office of the Governor, the~~  
442 ~~President of the Senate, and the Speaker of the House of~~  
443 ~~Representatives. The agency is not precluded from providing~~  
444 ~~recommendations before April 1, 2016.~~

445 (5)(6) In collaboration with the Department of Management  
446 Services, recommend ~~establish~~ best practices for the procurement  
447 of commercial cloud computing services ~~information technology~~  
448 ~~products~~ in order to reduce costs, increase quality of services  
449 ~~productivity~~, or improve data center services. ~~Such practices~~  
450 ~~must include a provision requiring the agency to review all~~

451 ~~information technology purchases made by state agencies that~~  
452 ~~have a total cost of \$250,000 or more, unless a purchase is~~  
453 ~~specifically mandated by the Legislature, for compliance with~~  
454 ~~the standards established pursuant to this section.~~

455 (6) In collaboration with the Department of Management  
456 Services, recommend an information technology policy for  
457 information technology-related state contracts, including state  
458 term contracts for information technology commodities,  
459 consultant services, and staff augmentation services.

460 (7) In consultation with state agencies, develop an  
461 enterprise data inventory that describes the data created or  
462 collected by a state agency, including geospatial data used in a  
463 state agency's geographic information system, and recommend  
464 options and associated costs for developing and maintaining an  
465 open data catalog that is machine-readable. For purposes of  
466 developing the inventory, the office shall:

467 (a) Establish a process and a reporting format for state  
468 agencies to provide an inventory that describes all current  
469 datasets aggregated or stored by the state agency. The inventory  
470 shall include, but is not limited to:

471 1. The title and description of the information contained  
472 within the dataset.

473 2. A description of how the data is maintained, including  
474 standards or terminologies used to structure the data.

475 3. Any existing or planned application programming

476 interface used to publish the data, a description of the data  
477 contained in any such existing interface, and a description of  
478 the data expected to be contained in any currently planned  
479 interface.

480 (b) Recommend any potential methods for standardizing data  
481 across state agencies that will promote interoperability and  
482 reduce the collection of duplicative data.

483 (c) Identify what state agency data may be considered open  
484 data.

485 (d) Recommend open data technical standards and  
486 terminologies for use by state agencies.

487 (e) Recommend options and all associated costs for the  
488 state to develop and maintain an open data catalog.

489 ~~(7)(a) Participate with the Department of Management~~  
490 ~~Services in evaluating, conducting, and negotiating competitive~~  
491 ~~solicitations for state term contracts for information~~  
492 ~~technology commodities, consultant services, or staff~~  
493 ~~augmentation contractual services pursuant to s. 287.0591.~~

494 ~~(b) Collaborate with the Department of Management Services~~  
495 ~~in information technology resource acquisition planning.~~

496 ~~(8) Develop standards for information technology reports~~  
497 ~~and updates, including, but not limited to, operational work~~  
498 ~~plans, project spend plans, and project status reports, for use~~  
499 ~~by state agencies.~~

500 ~~(9) Upon request, assist state agencies in the development~~

501 ~~of information technology-related legislative budget requests.~~

502 ~~(10) Beginning July 1, 2016, and annually thereafter,~~  
503 ~~conduct annual assessments of state agencies to determine~~  
504 ~~compliance with all information technology standards and~~  
505 ~~guidelines developed and published by the agency, and beginning~~  
506 ~~December 1, 2016, and annually thereafter, provide results of~~  
507 ~~the assessments to the Executive Office of the Governor, the~~  
508 ~~President of the Senate, and the Speaker of the House of~~  
509 ~~Representatives.~~

510 ~~(11) Provide operational management and oversight of the~~  
511 ~~state data center established pursuant to s. 282.201, which~~  
512 ~~includes:~~

513 ~~(a) Implementing industry standards and best practices for~~  
514 ~~the state data center's facilities, operations, maintenance,~~  
515 ~~planning, and management processes.~~

516 ~~(b) Developing and implementing cost-recovery mechanisms~~  
517 ~~that recover the full direct and indirect cost of services~~  
518 ~~through charges to applicable customer entities. Such cost-~~  
519 ~~recovery mechanisms must comply with applicable state and~~  
520 ~~federal regulations concerning distribution and use of funds and~~  
521 ~~must ensure that, for any fiscal year, no service or customer~~  
522 ~~entity subsidizes another service or customer entity.~~

523 ~~(c) Developing and implementing appropriate operating~~  
524 ~~guidelines and procedures necessary for the state data center to~~  
525 ~~perform its duties pursuant to s. 282.201. The guidelines and~~

526 ~~procedures must comply with applicable state and federal laws,~~  
527 ~~regulations, and policies and conform to generally accepted~~  
528 ~~governmental accounting and auditing standards. The guidelines~~  
529 ~~and procedures must include, but not be limited to:~~

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

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

538 ~~3. Providing rebates that may be credited against future~~  
539 ~~billings to customer entities when revenues exceed costs.~~

540 ~~4. Requiring customer entities to validate that sufficient~~  
541 ~~funds exist in the appropriate data processing appropriation~~  
542 ~~category or will be transferred into the appropriate data~~  
543 ~~processing appropriation category before implementation of a~~  
544 ~~customer entity's request for a change in the type or level of~~  
545 ~~service provided, if such change results in a net increase to~~  
546 ~~the customer entity's costs for that fiscal year.~~

547 ~~5. By September 1 of each year, providing to each customer~~  
548 ~~entity's agency head the projected costs of providing data~~  
549 ~~center services for the following fiscal year.~~

550 ~~6. Providing a plan for consideration by the Legislative~~

551 ~~Budget Commission if the cost of a service is increased for a~~  
552 ~~reason other than a customer entity's request made pursuant to~~  
553 ~~subparagraph 4. Such a plan is required only if the service cost~~  
554 ~~increase results in a net increase to a customer entity for that~~  
555 ~~fiscal year.~~

556 ~~7. Standardizing and consolidating procurement and~~  
557 ~~contracting practices.~~

558 ~~(d) In collaboration with the Department of Law~~  
559 ~~Enforcement, developing and implementing a process for~~  
560 ~~detecting, reporting, and responding to information technology~~  
561 ~~security incidents, breaches, and threats.~~

562 ~~(e) Adopting rules relating to the operation of the state~~  
563 ~~data center, including, but not limited to, budgeting and~~  
564 ~~accounting procedures, cost-recovery methodologies, and~~  
565 ~~operating procedures.~~

566 ~~(f) Beginning May 1, 2016, and annually thereafter,~~  
567 ~~conducting a market analysis to determine whether the state's~~  
568 ~~approach to the provision of data center services is the most~~  
569 ~~effective and efficient manner by which its customer entities~~  
570 ~~can acquire such services, based on federal, state, and local~~  
571 ~~government trends; best practices in service provision; and the~~  
572 ~~acquisition of new and emerging technologies. The results of the~~  
573 ~~market analysis shall assist the state data center in making~~  
574 ~~adjustments to its data center service offerings.~~

575 ~~(12) Recommend other information technology services that~~

576 ~~should be designed, delivered, and managed as enterprise~~  
577 ~~information technology services. Recommendations must include~~  
578 ~~the identification of existing information technology resources~~  
579 ~~associated with the services, if existing services must be~~  
580 ~~transferred as a result of being delivered and managed as~~  
581 ~~enterprise information technology services.~~

582 ~~(13) Recommend additional consolidations of agency~~  
583 ~~computing facilities or data centers into the state data center~~  
584 ~~established pursuant to s. 282.201. Such recommendations shall~~  
585 ~~include a proposed timeline for consolidation.~~

586 ~~(14) In consultation with state agencies, propose a~~  
587 ~~methodology and approach for identifying and collecting both~~  
588 ~~current and planned information technology expenditure data at~~  
589 ~~the state agency level.~~

590 ~~(15) (a) Beginning January 1, 2015, and notwithstanding any~~  
591 ~~other law, provide project oversight on any information~~  
592 ~~technology project of the Department of Financial Services, the~~  
593 ~~Department of Legal Affairs, and the Department of Agriculture~~  
594 ~~and Consumer Services that has a total project cost of \$25~~  
595 ~~million or more and that impacts one or more other agencies.~~  
596 ~~Such information technology projects must also comply with the~~  
597 ~~applicable information technology architecture, project~~  
598 ~~management and oversight, and reporting standards established by~~  
599 ~~the agency.~~

600 ~~(b) When performing the project oversight function~~

601 ~~specified in paragraph (a), report at least quarterly to the~~  
602 ~~Executive Office of the Governor, the President of the Senate,~~  
603 ~~and the Speaker of the House of Representatives on any~~  
604 ~~information technology project that the agency identifies as~~  
605 ~~high risk due to the project exceeding acceptable variance~~  
606 ~~ranges defined and documented in the project plan. The report~~  
607 ~~shall include a risk assessment, including fiscal risks,~~  
608 ~~associated with proceeding to the next stage of the project and~~  
609 ~~a recommendation for corrective actions required, including~~  
610 ~~suspension or termination of the project.~~

611 ~~(16) If an information technology project implemented by a~~  
612 ~~state agency must be connected to or otherwise accommodated by~~  
613 ~~an information technology system administered by the Department~~  
614 ~~of Financial Services, the Department of Legal Affairs, or the~~  
615 ~~Department of Agriculture and Consumer Services, consult with~~  
616 ~~these departments regarding the risks and other effects of such~~  
617 ~~projects on their information technology systems and work~~  
618 ~~cooperatively with these departments regarding the connections,~~  
619 ~~interfaces, timing, or accommodations required to implement such~~  
620 ~~projects.~~

621 ~~(8)~~(17) If adherence to standards or policies adopted by  
622 or established pursuant to this section causes conflict with  
623 federal regulations or requirements imposed on a state agency  
624 and results in adverse action against the state agency or  
625 federal funding, work with the state agency to provide

626 alternative standards, policies, or requirements that do not  
627 conflict with the federal regulation or requirement. Each  
628 ~~Beginning~~ July 1, ~~2015~~, the agency shall ~~annually~~ report such  
629 alternative standards to the Governor, the President of the  
630 Senate, and the Speaker of the House of Representatives.

631 ~~(18) In collaboration with the Department of Management~~  
632 ~~Services:~~

633 ~~(a) Establish an information technology policy for all~~  
634 ~~information technology-related state contracts, including state~~  
635 ~~term contracts for information technology commodities,~~  
636 ~~consultant services, and staff augmentation services. The~~  
637 ~~information technology policy must include:~~

638 ~~1. Identification of the information technology product~~  
639 ~~and service categories to be included in state term contracts.~~

640 ~~2. Requirements to be included in solicitations for state~~  
641 ~~term contracts.~~

642 ~~3. Evaluation criteria for the award of information~~  
643 ~~technology related state term contracts.~~

644 ~~4. The term of each information technology-related state~~  
645 ~~term contract.~~

646 ~~5. The maximum number of vendors authorized on each state~~  
647 ~~term contract.~~

648 ~~(b) Evaluate vendor responses for state term contract~~  
649 ~~solicitations and invitations to negotiate.~~

650 ~~(c) Answer vendor questions on state term contract~~

651 solicitations.

652 ~~(d) Ensure that the information technology policy~~  
653 ~~established pursuant to paragraph (a) is included in all~~  
654 ~~solicitations and contracts which are administratively executed~~  
655 ~~by the department.~~

656 (9) ~~(19)~~ Adopt rules to administer this section.

657 Section 17. Section 282.00515, Florida Statutes, is  
658 amended to read:

659 282.00515 Duties of Cabinet agencies.—

660 (1) The Department of Legal Affairs, the Department of  
661 Financial Services, and the Department of Agriculture and  
662 Consumer Services shall adopt the standards established in s.  
663 282.0051(3) ~~282.0051(2), (3), and (8)~~ or adopt alternative  
664 standards based on best practices and industry standards, and  
665 may consult ~~contract~~ with the Office of Technology and Data  
666 Solutions for recommendations ~~Agency for State Technology to~~  
667 ~~provide or perform any of the services and functions described~~  
668 ~~in s. 282.0051 for the Department of Legal Affairs, the~~  
669 ~~Department of Financial Services, or the Department of~~  
670 ~~Agriculture and Consumer Services.~~

671 (2) Beginning January 1, 2018, and notwithstanding any  
672 other law, the Department of Financial Services, the Department  
673 of Legal Affairs, and the Department of Agriculture and Consumer  
674 Services shall submit project oversight deliverables to the  
675 Office of Technology and Data Solutions for all information

676 technology projects with a total project cost of \$25 million or  
677 more and which impact one or more other agencies. Such  
678 information technology projects must also comply with the  
679 project management and oversight standards established by the  
680 office.

681 Section 18. Section 282.201, Florida Statutes, is amended  
682 to read:

683 282.201 State data center.—The state data center is  
684 established within the Department of Management Services Agency  
685 ~~for State Technology~~ and shall provide data center services that  
686 are either hosted on premises or hosted externally through a  
687 commercial cloud computing third-party provider, whichever  
688 option meets the operational needs at the best cost and service  
689 levels as verified by a customer entity as an enterprise  
690 ~~information technology service~~. The provision of services must  
691 comply with applicable state and federal laws, regulations, and  
692 policies, including all applicable security, privacy, and  
693 auditing requirements. The Secretary of Management Services  
694 shall appoint a director of the state data center who has  
695 experience in leading data center facilities and expertise in  
696 cloud computing management. The state data center shall not be  
697 subject to the management or control of the Office of Technology  
698 and Data Solutions.

699 (1) USE OF THE STATE DATA CENTER.—

700 (a) The following are exempt from the use of the state

701 data center: the Department of Law Enforcement, the Department  
702 of the Lottery's gaming system, systems design and development  
703 in the Office of Policy and Budget, the regional traffic  
704 management centers that manage the computerized traffic systems  
705 and control devices described in s. 335.14(2) and toll  
706 operations of the Department of Transportation, the State Board  
707 of Administration, state attorneys, public defenders, criminal  
708 conflict and civil regional counsels, capital collateral  
709 regional counsels, and the Florida Housing Finance Corporation.

710 (b) Unless exempt from use of the state data center  
711 pursuant to this section or as authorized by the Legislature, a  
712 state agency may not:

713 1. Create a new agency computing facility or data center  
714 or expand the capability to support additional computer  
715 equipment in an existing agency computing facility or data  
716 center; or

717 2. Terminate services with the state data center without  
718 giving written notice to the center of intent to terminate  
719 services at least 180 days before such termination.

720 ~~(1) INTENT. The Legislature finds that the most efficient~~  
721 ~~and effective means of providing quality utility data processing~~  
722 ~~services to state agencies requires that computing resources be~~  
723 ~~concentrated in quality facilities that provide the proper~~  
724 ~~security, disaster recovery, infrastructure, and staff resources~~  
725 ~~to ensure that the state's data is maintained reliably and~~

726 ~~safely, and is recoverable in the event of a disaster. Unless~~  
727 ~~otherwise exempt by law, it is the intent of the Legislature~~  
728 ~~that all agency data centers and computing facilities shall be~~  
729 ~~consolidated into the state data center.~~

730 (2) STATE DATA CENTER DUTIES.—The state data center shall:

731 (a) Develop and implement appropriate operating guidelines  
732 and procedures that are necessary for the state data center to  
733 perform its duties pursuant to this subsection and that comply  
734 with applicable state and federal laws, regulations, and  
735 policies and that conform to generally accepted governmental  
736 accounting and auditing standards.

737 (b) Develop and implement a cost recovery mechanism that  
738 recovers the full direct and indirect costs of services through  
739 charges to applicable customer entities. Such cost recovery  
740 mechanism must comply with applicable state and federal  
741 regulations concerning distribution and use of funds and must  
742 ensure that, for any fiscal year, no service or customer entity  
743 subsidizes another service or customer entity. The cost recovery  
744 mechanism must include, but need not be limited to:

745 1. Implementing an annual reconciliation process.

746 2. Providing rebates that may be credited against future  
747 billings to customer entities when revenues exceed costs.

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

751 processing appropriation category before implementation of a  
752 customer entity's request for a change in the type or level of  
753 service provided, if such change results in a net increase to  
754 the customer entity's costs for that fiscal year.

755 4. By September 1 of each year, providing to each customer  
756 entity's agency head the projected costs of providing data  
757 center services for the following fiscal year.

758 5. Providing a plan for consideration by the Legislative  
759 Budget Commission if the cost of a service is increased for a  
760 reason other than a customer entity's request made pursuant to  
761 subparagraph 3. Such a plan is required only if the service cost  
762 increase results in a net increase to a customer entity for that  
763 fiscal year.

764 (c) In collaboration with the Department of Law  
765 Enforcement, develop and implement a process for detecting,  
766 reporting, and responding to information technology security  
767 incidents, breaches, and threats.

768 (d) Offer, develop, and support the services and  
769 applications defined in service-level agreements executed with  
770 its customer entities.

771 (e) ~~(b)~~ Maintain performance of the state data center by  
772 ensuring proper data backup, data backup recovery, disaster  
773 recovery, and appropriate security, power, cooling, fire  
774 suppression, and capacity.

775 (f) ~~(e)~~ Develop and implement a business continuity plan

776 and a disaster recovery plan, and each ~~beginning~~ July 1, 2015,  
777 ~~and annually thereafter,~~ conduct a live exercise of each plan.

778 (g) ~~(d)~~ Enter into a service-level agreement with each  
779 customer entity to provide the required type and level of  
780 service or services. If a customer entity fails to execute an  
781 agreement within 60 days after commencement or change of a  
782 service, the state data center may cease service. A service-  
783 level agreement may not have a term exceeding 3 years and at a  
784 minimum must:

785 1. Identify the parties and their roles, duties, and  
786 responsibilities under the agreement.

787 2. State the duration of the contract term and specify the  
788 conditions for renewal.

789 3. Identify the scope of work.

790 4. Identify the products or services to be delivered with  
791 sufficient specificity to permit an external financial or  
792 performance audit.

793 5. Establish the services to be provided, the business  
794 standards that must be met for each service, the cost of each  
795 service by agency application, and the metrics and processes by  
796 which the business standards for each service are to be  
797 objectively measured and reported.

798 6. Provide a timely billing methodology to recover the  
799 cost of services provided to the customer entity pursuant to s.  
800 215.422.

801           7. Provide a procedure for modifying the service-level  
802 agreement based on changes in the type, level, and cost of a  
803 service.

804           8. Include a right-to-audit clause to ensure that the  
805 parties to the agreement have access to records for audit  
806 purposes during the term of the service-level agreement.

807           9. Provide that a service-level agreement may be  
808 terminated by either party for cause only after giving the other  
809 party and the Department of Management Services ~~Agency for State~~  
810 ~~Technology~~ notice in writing of the cause for termination and an  
811 opportunity for the other party to resolve the identified cause  
812 within a reasonable period.

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

815           (h)~~(e)~~ For purposes of chapter 273, be the custodian of  
816 resources and equipment located in and operated, supported, and  
817 managed by the state data center.

818           (i)~~(f)~~ Assume administrative access rights to resources  
819 and equipment, including servers, network components, and other  
820 devices, consolidated into the state data center.

821           1. Upon consolidating into the state data center ~~the date~~  
822 ~~of each consolidation specified in this section, the General~~  
823 ~~Appropriations Act, or any other law,~~ a state agency shall  
824 relinquish administrative rights to consolidated resources and  
825 equipment. State agencies required to comply with federal and

826 state criminal justice information security rules and policies  
827 shall retain administrative access rights sufficient to comply  
828 with the management control provisions of those rules and  
829 policies; however, the state data center shall have the  
830 appropriate type or level of rights to allow the center to  
831 comply with its duties pursuant to this section. The Department  
832 of Law Enforcement shall serve as the arbiter of disputes  
833 pertaining to the appropriate type and level of administrative  
834 access rights pertaining to the provision of management control  
835 in accordance with the federal criminal justice information  
836 guidelines.

837 2. The state data center shall provide customer entities  
838 with access to applications, servers, network components, and  
839 other devices necessary for entities to perform business  
840 activities and functions, and as defined and documented in a  
841 service-level agreement.

842 (j) Establish a commercial cloud computing service instead  
843 of purchasing, financing, leasing, or upgrading state data  
844 center infrastructure, when a cost benefit analysis verified by  
845 the customer entity validates that a commercial cloud computing  
846 service can reduce customer entity data center costs while  
847 delivering the same or improved levels of service and meets or  
848 exceeds the applicable state and federal standards for  
849 information technology security.

850 (k) Submit a report on the use of cloud computing by state

851 agency customer entities no later than November 15 of each even-  
852 numbered year to the Governor, the President of the Senate, the  
853 Speaker of the House of Representatives, and the Office of  
854 Technology and Data Solutions. The report must include cloud  
855 computing usage by customer entity that provided cost savings  
856 and other benefits, such as improved service levels and security  
857 enhancements. Each state agency shall cooperate with the  
858 department in the creation of the report by providing timely and  
859 accurate information and any assistance required by the  
860 department.

861 (1) Adopt rules to administer this section.

862 ~~(3) STATE AGENCY DUTIES.—~~

863 ~~(a) Each state agency shall provide to the Agency for~~  
864 ~~State Technology all requested information relating to its data~~  
865 ~~centers and computing facilities and any other information~~  
866 ~~relevant to the effective transition of an agency data center or~~  
867 ~~computing facility into the state data center.~~

868 ~~(b) Each state agency customer of the state data center~~  
869 ~~shall notify the state data center, by May 31 and November 30 of~~  
870 ~~each year, of any significant changes in anticipated utilization~~  
871 ~~of state data center services pursuant to requirements~~  
872 ~~established by the state data center.~~

873 ~~(4) SCHEDULE FOR CONSOLIDATIONS OF AGENCY DATA CENTERS.—~~

874 ~~(a) Consolidations of agency data centers and computing~~  
875 ~~facilities into the state data center shall be made by the dates~~

876 ~~specified in this section and in accordance with budget~~  
877 ~~adjustments contained in the General Appropriations Act.~~

878 ~~(b) During the 2013-2014 fiscal year, the following state~~  
879 ~~agencies shall be consolidated by the specified date:~~

880 ~~1. By October 31, 2013, the Department of Economic~~  
881 ~~Opportunity.~~

882 ~~2. By December 31, 2013, the Executive Office of the~~  
883 ~~Governor, to include the Division of Emergency Management except~~  
884 ~~for the Emergency Operation Center's management system in~~  
885 ~~Tallahassee and the Camp Blanding Emergency Operations Center in~~  
886 ~~Starke.~~

887 ~~3. By March 31, 2014, the Department of Elderly Affairs.~~

888 ~~4. By October 30, 2013, the Fish and Wildlife Conservation~~  
889 ~~Commission, except for the commission's Fish and Wildlife~~  
890 ~~Research Institute in St. Petersburg.~~

891 ~~(c) The following are exempt from state data center~~  
892 ~~consolidation under this section: the Department of Law~~  
893 ~~Enforcement, the Department of the Lottery's Gaming System,~~  
894 ~~Systems Design and Development in the Office of Policy and~~  
895 ~~Budget, the regional traffic management centers as described in~~  
896 ~~s. 335.14(2) and the Office of Toll Operations of the Department~~  
897 ~~of Transportation, the State Board of Administration, state~~  
898 ~~attorneys, public defenders, criminal conflict and civil~~  
899 ~~regional counsel, capital collateral regional counsel, and the~~  
900 ~~Florida Housing Finance Corporation.~~

901 ~~(d) A state agency that is consolidating its agency data~~  
902 ~~center or computing facility into the state data center must~~  
903 ~~execute a new or update an existing service-level agreement~~  
904 ~~within 60 days after the commencement of the service. If a state~~  
905 ~~agency and the state data center are unable to execute a~~  
906 ~~service-level agreement by that date, the agency shall submit a~~  
907 ~~report to the Executive Office of the Governor within 5 working~~  
908 ~~days after that date which explains the specific issues~~  
909 ~~preventing execution and describing the plan and schedule for~~  
910 ~~resolving those issues.~~

911 ~~(e) Each state agency scheduled for consolidation into the~~  
912 ~~state data center shall submit a transition plan to the Agency~~  
913 ~~for State Technology by July 1 of the fiscal year before the~~  
914 ~~fiscal year in which the scheduled consolidation will occur.~~  
915 ~~Transition plans shall be developed in consultation with the~~  
916 ~~state data center and must include:~~

917 ~~1. An inventory of the agency data center's resources~~  
918 ~~being consolidated, including all hardware and its associated~~  
919 ~~life cycle replacement schedule, software, staff, contracted~~  
920 ~~services, and facility resources performing data center~~  
921 ~~management and operations, security, backup and recovery,~~  
922 ~~disaster recovery, system administration, database~~  
923 ~~administration, system programming, job control, production~~  
924 ~~control, print, storage, technical support, help desk, and~~  
925 ~~managed services, but excluding application development, and the~~

926 ~~agency's costs supporting these resources.~~

927 ~~2. A list of contracts in effect, including, but not~~  
928 ~~limited to, contracts for hardware, software, and maintenance,~~  
929 ~~which identifies the expiration date, the contract parties, and~~  
930 ~~the cost of each contract.~~

931 ~~3. A detailed description of the level of services needed~~  
932 ~~to meet the technical and operational requirements of the~~  
933 ~~platforms being consolidated.~~

934 ~~4. A timetable with significant milestones for the~~  
935 ~~completion of the consolidation.~~

936 ~~(f) Each state agency scheduled for consolidation into the~~  
937 ~~state data center shall submit with its respective legislative~~  
938 ~~budget request the specific recurring and nonrecurring budget~~  
939 ~~adjustments of resources by appropriation category into the~~  
940 ~~appropriate data processing category pursuant to the legislative~~  
941 ~~budget request instructions in s. 216.023.~~

942 ~~(5) AGENCY LIMITATIONS.—~~

943 ~~(a) Unless exempt from data center consolidation pursuant~~  
944 ~~to this section or authorized by the Legislature or as provided~~  
945 ~~in paragraph (b), a state agency may not:~~

946 ~~1. Create a new agency computing facility or data center,~~  
947 ~~or expand the capability to support additional computer~~  
948 ~~equipment in an existing agency computing facility or data~~  
949 ~~center;~~

950 ~~2. Spend funds before the state agency's scheduled~~

951 ~~consolidation into the state data center to purchase or modify~~  
952 ~~hardware or operations software that does not comply with~~  
953 ~~standards established by the Agency for State Technology~~  
954 ~~pursuant to s. 282.0051;~~

955 ~~3. Transfer existing computer services to any data center~~  
956 ~~other than the state data center;~~

957 ~~4. Terminate services with the state data center without~~  
958 ~~giving written notice of intent to terminate services 180 days~~  
959 ~~before such termination; or~~

960 ~~5. Initiate a new computer service except with the state~~  
961 ~~data center.~~

962 ~~(b) Exceptions to the limitations in subparagraphs (a)1.,~~  
963 ~~2., 3., and 5. may be granted by the Agency for State Technology~~  
964 ~~if there is insufficient capacity in the state data center to~~  
965 ~~absorb the workload associated with agency computing services,~~  
966 ~~if expenditures are compatible with the standards established~~  
967 ~~pursuant to s. 282.0051, or if the equipment or resources are~~  
968 ~~needed to meet a critical agency business need that cannot be~~  
969 ~~satisfied by the state data center. The Agency for State~~  
970 ~~Technology shall establish requirements that a state agency must~~  
971 ~~follow when submitting and documenting a request for an~~  
972 ~~exception. The Agency for State Technology shall also publish~~  
973 ~~guidelines for its consideration of exception requests. However,~~  
974 ~~the decision of the Agency for State Technology regarding an~~  
975 ~~exception request is not subject to chapter 120.~~

976 Section 19. Section 282.206, Florida Statutes, is created  
977 to read:

978 282.206 Information technology management; state  
979 agencies.—

980 (1) By May 31 and November 30 of each year, each state  
981 agency customer entity shall notify the state data center of any  
982 significant changes in anticipated use of state data center  
983 services, including the status of agency applications supported  
984 by the state data center which are planned for replacement or  
985 migration to commercial cloud computing services, pursuant to  
986 requirements established by the state data center.

987 (2) Each state agency customer entity shall develop a plan  
988 to be updated annually to address its applications located at  
989 the state data center. Each agency shall submit the plan by  
990 November 1 of each year to the Office of Policy and Budget in  
991 the Executive Office of the Governor and to the chair of the  
992 appropriations committee of each house of the Legislature. For  
993 each application, the plan must identify the appropriate  
994 strategy for migration to a commercial cloud computing service  
995 and evaluate options such as replacement, remediation, and  
996 replatforming. The plan must include a high-level migration  
997 timeline by fiscal year for each application, and, for each  
998 application that may begin migration activities, the plan shall  
999 include:

1000 (a) A proposed project and budget estimate to implement

HB 5301

2017

1001 the migration.

1002 (b) Validation in a cost benefit analysis that a  
1003 commercial cloud computing service can reduce customer entity  
1004 data center costs, deliver the same or improved levels of  
1005 service, and meet or exceed the applicable state and federal  
1006 standards for information technology security.

1007 (3) A state agency customer entity shall use a commercial  
1008 cloud computing service in developing, upgrading, or purchasing  
1009 software when a cost benefit analysis confirms that a commercial  
1010 cloud computing service can deliver the same or improved levels  
1011 of service and meets or exceeds the applicable state and federal  
1012 standards for information technology security.

1013 Section 20. Subsections (3), (4), (5), and (6) of section  
1014 282.318, Florida Statutes, are amended to read:

1015 282.318 Security of data and information technology.—

1016 (3) The Office of Technology and Data Solutions ~~Agency for~~  
1017 ~~State Technology~~ is responsible for establishing standards and  
1018 processes consistent with generally accepted best practices for  
1019 information technology security, to include cybersecurity, and  
1020 adopting rules that safeguard an agency's data, information, and  
1021 information technology resources to ensure availability,  
1022 confidentiality, and integrity and to mitigate risks. The agency  
1023 shall also:

1024 (a) Develop, and annually update by February 1, a  
1025 statewide information technology security strategic plan that

1026 | includes security goals and objectives for the strategic issues  
 1027 | of information technology security policy, risk management,  
 1028 | training, incident management, and disaster recovery planning.

1029 | (b) Develop and publish for use by state agencies an  
 1030 | information technology security framework that, at a minimum,  
 1031 | includes guidelines and processes for:

1032 | 1. Establishing asset management procedures to ensure that  
 1033 | an agency's information technology resources are identified and  
 1034 | managed consistent with their relative importance to the  
 1035 | agency's business objectives.

1036 | 2. Using a standard risk assessment methodology that  
 1037 | includes the identification of an agency's priorities,  
 1038 | constraints, risk tolerances, and assumptions necessary to  
 1039 | support operational risk decisions.

1040 | 3. Completing comprehensive risk assessments and  
 1041 | information technology security audits, which may be completed  
 1042 | by a private sector vendor, and submitting completed assessments  
 1043 | and audits to the Office of Technology and Data Solutions ~~Agency~~  
 1044 | ~~for State Technology~~.

1045 | 4. Identifying protection procedures to manage the  
 1046 | protection of an agency's information, data, and information  
 1047 | technology resources.

1048 | 5. Establishing procedures for accessing information and  
 1049 | data to ensure the confidentiality, integrity, and availability  
 1050 | of such information and data.

1051           6. Detecting threats through proactive monitoring of  
1052 events, continuous security monitoring, and defined detection  
1053 processes.

1054           7. Establishing agency computer security incident response  
1055 teams and describing their responsibilities for responding to  
1056 information technology security incidents, including breaches of  
1057 personal information containing confidential or exempt data.

1058           8. Recovering information and data in response to an  
1059 information technology security incident. The recovery may  
1060 include recommended improvements to the agency processes,  
1061 policies, or guidelines.

1062           9. Establishing an information technology security  
1063 incident reporting process that includes procedures and tiered  
1064 reporting timeframes for notifying the Office of Technology and  
1065 Data Solutions ~~Agency for State Technology~~ and the Department of  
1066 Law Enforcement of information technology security incidents.  
1067 The tiered reporting timeframes shall be based upon the level of  
1068 severity of the information technology security incidents being  
1069 reported.

1070           10. Incorporating information obtained through detection  
1071 and response activities into the agency's information technology  
1072 security incident response plans.

1073           11. Developing agency strategic and operational  
1074 information technology security plans required pursuant to this  
1075 section.

1076           12. Establishing the managerial, operational, and  
1077 technical safeguards for protecting state government data and  
1078 information technology resources that align with the state  
1079 agency risk management strategy and that protect the  
1080 confidentiality, integrity, and availability of information and  
1081 data.

1082           (c) Assist state agencies in complying with this section.

1083           (d) In collaboration with the Cybercrime Office of the  
1084 Department of Law Enforcement, annually provide training for  
1085 state agency information security managers and computer security  
1086 incident response team members that contains training on  
1087 information technology security, including cybersecurity,  
1088 threats, trends, and best practices.

1089           (e) Annually review the strategic and operational  
1090 information technology security plans of executive branch  
1091 agencies.

1092           (4) Each state agency head shall, at a minimum:

1093           (a) Designate an information security manager to  
1094 administer the information technology security program of the  
1095 state agency. This designation must be provided annually in  
1096 writing to the Office of Technology and Data Solutions ~~Agency~~  
1097 ~~for State Technology~~ by January 1. A state agency's information  
1098 security manager, for purposes of these information security  
1099 duties, shall report directly to the agency head.

1100           (b) In consultation with the Office of Technology and Data

1101 ~~Solutions Agency for State Technology~~ and the Cybercrime Office  
1102 of the Department of Law Enforcement, establish an agency  
1103 computer security incident response team to respond to an  
1104 information technology security incident. The agency computer  
1105 security incident response team shall convene upon notification  
1106 of an information technology security incident and must comply  
1107 with all applicable guidelines and processes established  
1108 pursuant to paragraph (3) (b).

1109 (c) Submit to the Office of Technology and Data Solutions  
1110 ~~Agency for State Technology~~ annually by July 31, the state  
1111 agency's strategic and operational information technology  
1112 security plans developed pursuant to rules and guidelines  
1113 established by the Office of Technology and Data Solutions  
1114 ~~Agency for State Technology~~.

1115 1. The state agency strategic information technology  
1116 security plan must cover a 3-year period and, at a minimum,  
1117 define security goals, intermediate objectives, and projected  
1118 agency costs for the strategic issues of agency information  
1119 security policy, risk management, security training, security  
1120 incident response, and disaster recovery. The plan must be based  
1121 on the statewide information technology security strategic plan  
1122 created by the Office of Technology and Data Solutions ~~Agency~~  
1123 ~~for State Technology~~ and include performance metrics that can be  
1124 objectively measured to reflect the status of the state agency's  
1125 progress in meeting security goals and objectives identified in

1126 the agency's strategic information security plan.

1127         2. The state agency operational information technology  
1128 security plan must include a progress report that objectively  
1129 measures progress made towards the prior operational information  
1130 technology security plan and a project plan that includes  
1131 activities, timelines, and deliverables for security objectives  
1132 that the state agency will implement during the current fiscal  
1133 year.

1134         (d) Conduct, and update every 3 years, a comprehensive  
1135 risk assessment, which may be completed by a private sector  
1136 vendor, to determine the security threats to the data,  
1137 information, and information technology resources, including  
1138 mobile devices and print environments, of the agency. The risk  
1139 assessment must comply with the risk assessment methodology  
1140 developed by the Office of Technology and Data Solutions ~~Agency~~  
1141 ~~for State Technology~~ and is confidential and exempt from s.  
1142 119.07(1), except that such information shall be available to  
1143 the Auditor General, the Office of Technology and Data Solutions  
1144 ~~Agency for State Technology~~, the Cybercrime Office of the  
1145 Department of Law Enforcement, and, for state agencies under the  
1146 jurisdiction of the Governor, the Chief Inspector General.

1147         (e) Develop, and periodically update, written internal  
1148 policies and procedures, which include procedures for reporting  
1149 information technology security incidents and breaches to the  
1150 Cybercrime Office of the Department of Law Enforcement and the

1151 Office of Technology and Data Solutions ~~Agency for State~~  
1152 ~~Technology~~. Such policies and procedures must be consistent with  
1153 the rules, guidelines, and processes established by the Office  
1154 of Technology and Data Solutions ~~Agency for State Technology~~ to  
1155 ensure the security of the data, information, and information  
1156 technology resources of the agency. The internal policies and  
1157 procedures that, if disclosed, could facilitate the unauthorized  
1158 modification, disclosure, or destruction of data or information  
1159 technology resources are confidential information and exempt  
1160 from s. 119.07(1), except that such information shall be  
1161 available to the Auditor General, the Cybercrime Office of the  
1162 Department of Law Enforcement, the Office of Technology and Data  
1163 Solutions ~~Agency for State Technology~~, and, for state agencies  
1164 under the jurisdiction of the Governor, the Chief Inspector  
1165 General.

1166 (f) Implement managerial, operational, and technical  
1167 safeguards and risk assessment remediation plans recommended by  
1168 the Office of Technology and Data Solutions ~~Agency for State~~  
1169 ~~Technology~~ to address identified risks to the data, information,  
1170 and information technology resources of the agency.

1171 (g) Ensure that periodic internal audits and evaluations  
1172 of the agency's information technology security program for the  
1173 data, information, and information technology resources of the  
1174 agency are conducted. The results of such audits and evaluations  
1175 are confidential information and exempt from s. 119.07(1),

1176 except that such information shall be available to the Auditor  
1177 General, the Cybercrime Office of the Department of Law  
1178 Enforcement, the Office of Technology and Data Solutions ~~Agency~~  
1179 ~~for State Technology~~, and, for agencies under the jurisdiction  
1180 of the Governor, the Chief Inspector General.

1181 (h) Recommend ~~Include~~ appropriate information technology  
1182 security requirements in the written specifications for the  
1183 solicitation of information technology and information  
1184 technology resources and services, which are consistent with the  
1185 rules and guidelines established by the Office of Technology and  
1186 Data Solutions ~~Agency for State Technology~~ in collaboration with  
1187 the Department of Management Services.

1188 (i) Provide information technology security and  
1189 cybersecurity awareness training to all state agency employees  
1190 in the first 30 days after commencing employment concerning  
1191 information technology security risks and the responsibility of  
1192 employees to comply with policies, standards, guidelines, and  
1193 operating procedures adopted by the state agency to reduce those  
1194 risks. The training may be provided in collaboration with the  
1195 Cybercrime Office of the Department of Law Enforcement.

1196 (j) Develop a process for detecting, reporting, and  
1197 responding to threats, breaches, or information technology  
1198 security incidents which is consistent with the security rules,  
1199 guidelines, and processes established by the Office of  
1200 Technology and Data Solutions ~~Agency for State Technology~~.

1201           1. All information technology security incidents and  
 1202 breaches must be reported to the Office of Technology and Data  
 1203 Solutions Agency for State Technology and the Cybercrime Office  
 1204 of the Department of Law Enforcement and must comply with the  
 1205 notification procedures and reporting timeframes established  
 1206 pursuant to paragraph (3) (b).

1207           2. For information technology security breaches, state  
 1208 agencies shall provide notice in accordance with s. 501.171.

1209           3. Records held by a state agency which identify  
 1210 detection, investigation, or response practices for suspected or  
 1211 confirmed information technology security incidents, including  
 1212 suspected or confirmed breaches, are confidential and exempt  
 1213 from s. 119.07(1) and s. 24(a), Art. I of the State  
 1214 Constitution, if the disclosure of such records would facilitate  
 1215 unauthorized access to or the unauthorized modification,  
 1216 disclosure, or destruction of:

1217           a. Data or information, whether physical or virtual; or

1218           b. Information technology resources, which includes:

1219           (I) Information relating to the security of the agency's  
 1220 technologies, processes, and practices designed to protect  
 1221 networks, computers, data processing software, and data from  
 1222 attack, damage, or unauthorized access; or

1223           (II) Security information, whether physical or virtual,  
 1224 which relates to the agency's existing or proposed information  
 1225 technology systems.

1226  
1227 Such records shall be available to the Auditor General, the  
1228 Office of Technology and Data Solutions ~~Agency for State~~  
1229 ~~Technology~~, the Cybercrime Office of the Department of Law  
1230 Enforcement, and, for state agencies under the jurisdiction of  
1231 the Governor, the Chief Inspector General. Such records may be  
1232 made available to a local government, another state agency, or a  
1233 federal agency for information technology security purposes or  
1234 in furtherance of the state agency's official duties. This  
1235 exemption applies to such records held by a state agency before,  
1236 on, or after the effective date of this exemption. This  
1237 subparagraph is subject to the Open Government Sunset Review Act  
1238 in accordance with s. 119.15 and shall stand repealed on October  
1239 2, 2021, unless reviewed and saved from repeal through  
1240 reenactment by the Legislature.

1241 (5) The portions of risk assessments, evaluations,  
1242 external audits, and other reports of a state agency's  
1243 information technology security program for the data,  
1244 information, and information technology resources of the state  
1245 agency which are held by a state agency are confidential and  
1246 exempt from s. 119.07(1) and s. 24(a), Art. I of the State  
1247 Constitution if the disclosure of such portions of records would  
1248 facilitate unauthorized access to or the unauthorized  
1249 modification, disclosure, or destruction of:

1250 (a) Data or information, whether physical or virtual; or

1251 (b) Information technology resources, which include:  
 1252 1. Information relating to the security of the agency's  
 1253 technologies, processes, and practices designed to protect  
 1254 networks, computers, data processing software, and data from  
 1255 attack, damage, or unauthorized access; or  
 1256 2. Security information, whether physical or virtual,  
 1257 which relates to the agency's existing or proposed information  
 1258 technology systems.  
 1259  
 1260 Such portions of records shall be available to the Auditor  
 1261 General, the Cybercrime Office of the Department of Law  
 1262 Enforcement, the Office of Technology and Data Solutions Agency  
 1263 ~~for State Technology~~, and, for agencies under the jurisdiction  
 1264 of the Governor, the Chief Inspector General. Such portions of  
 1265 records may be made available to a local government, another  
 1266 state agency, or a federal agency for information technology  
 1267 security purposes or in furtherance of the state agency's  
 1268 official duties. For purposes of this subsection, "external  
 1269 audit" means an audit that is conducted by an entity other than  
 1270 the state agency that is the subject of the audit. This  
 1271 exemption applies to such records held by a state agency before,  
 1272 on, or after the effective date of this exemption. This  
 1273 subsection is subject to the Open Government Sunset Review Act  
 1274 in accordance with s. 119.15 and shall stand repealed on October  
 1275 2, 2021, unless reviewed and saved from repeal through

1276 reenactment by the Legislature.

1277 (6) The Office of Technology and Data Solutions ~~Agency for~~  
 1278 ~~State Technology~~ shall adopt rules relating to information  
 1279 technology security and to administer this section.

1280 Section 21. Subsection (22) of section 287.057, Florida  
 1281 Statutes, is amended to read:

1282 287.057 Procurement of commodities or contractual  
 1283 services.—

1284 (22) The department, in consultation with the Chief  
 1285 Financial Officer and the Office of Technology and Data  
 1286 Solutions ~~Agency for State Technology~~, shall maintain a program  
 1287 for online procurement of commodities and contractual services.  
 1288 To enable the state to promote open competition and leverage its  
 1289 buying power, agencies shall participate in the online  
 1290 procurement program, and eligible users may participate in the  
 1291 program. Only vendors prequalified as meeting mandatory  
 1292 requirements and qualifications criteria may participate in  
 1293 online procurement.

1294 (a) The department, ~~in consultation with the Agency for~~  
 1295 ~~State Technology and in compliance with the standards of the~~  
 1296 ~~agency~~, may contract for equipment and services necessary to  
 1297 develop and implement online procurement.

1298 (b) The department shall adopt rules to administer the  
 1299 program for online procurement. The rules must include, but not  
 1300 be limited to:

1301 1. Determining the requirements and qualification criteria  
 1302 for prequalifying vendors.

1303 2. Establishing the procedures for conducting online  
 1304 procurement.

1305 3. Establishing the criteria for eligible commodities and  
 1306 contractual services.

1307 4. Establishing the procedures for providing access to  
 1308 online procurement.

1309 5. Determining the criteria warranting any exceptions to  
 1310 participation in the online procurement program.

1311 (c) The department may impose and shall collect all fees  
 1312 for the use of the online procurement systems.

1313 1. The fees may be imposed on an individual transaction  
 1314 basis or as a fixed percentage of the cost savings generated. At  
 1315 a minimum, the fees must be set in an amount sufficient to cover  
 1316 the projected costs of the services, including administrative  
 1317 and project service costs in accordance with the policies of the  
 1318 department.

1319 2. If the department contracts with a provider for online  
 1320 procurement, the department, pursuant to appropriation, shall  
 1321 compensate the provider from the fees after the department has  
 1322 satisfied all ongoing costs. The provider shall report  
 1323 transaction data to the department each month so that the  
 1324 department may determine the amount due and payable to the  
 1325 department from each vendor.

1326           3. All fees that are due and payable to the state on a  
 1327 transactional basis or as a fixed percentage of the cost savings  
 1328 generated are subject to s. 215.31 and must be remitted within  
 1329 40 days after receipt of payment for which the fees are due. For  
 1330 fees that are not remitted within 40 days, the vendor shall pay  
 1331 interest at the rate established under s. 55.03(1) on the unpaid  
 1332 balance from the expiration of the 40-day period until the fees  
 1333 are remitted.

1334           4. All fees and surcharges collected under this paragraph  
 1335 shall be deposited in the Operating Trust Fund as provided by  
 1336 law.

1337           Section 22. Subsection (3) of section 287.0591, Florida  
 1338 Statutes, is amended to read:

1339           287.0591 Information technology.—

1340           (3) The department may execute a state term contract for  
 1341 information technology commodities, consultant services, or  
 1342 staff augmentation contractual services that exceeds the 48-  
 1343 month requirement if the Secretary of Management Services  
 1344 certifies and the executive director of the Agency for State  
 1345 ~~Technology certify~~ to the Executive Office of the Governor that  
 1346 a longer contract term is in the best interest of the state.

1347           Section 23. Subsection (4) of section 445.011, Florida  
 1348 Statutes, is amended to read:

1349           445.011 Workforce information systems.—

1350           ~~(4) CareerSource Florida, Inc., shall coordinate~~

1351 ~~development and implementation of workforce information systems~~  
1352 ~~with the executive director of the Agency for State Technology~~  
1353 ~~to ensure compatibility with the state's information system~~  
1354 ~~strategy and enterprise architecture.~~

1355 Section 24. Subsections (2) and (4) of section 445.045,  
1356 Florida Statutes, are amended to read:

1357 445.045 Development of an Internet-based system for  
1358 information technology industry promotion and workforce  
1359 recruitment.—

1360 (2) CareerSource Florida, Inc., shall coordinate with ~~the~~  
1361 ~~Agency for State Technology and~~ the Department of Economic  
1362 Opportunity to ensure links, as feasible and appropriate, to  
1363 existing job information websites maintained by the state and  
1364 state agencies and to ensure that information technology  
1365 positions offered by the state and state agencies are posted on  
1366 the information technology website.

1367 (4) ~~(a) CareerSource Florida, Inc., shall coordinate~~  
1368 ~~development and maintenance of the website under this section~~  
1369 ~~with the executive director of the Agency for State Technology~~  
1370 ~~to ensure compatibility with the state's information system~~  
1371 ~~strategy and enterprise architecture.~~

1372 (a) ~~(b)~~ CareerSource Florida, Inc., may enter into an  
1373 agreement with ~~the Agency for State Technology,~~ the Department  
1374 of Economic Opportunity, or any other public agency with the  
1375 requisite information technology expertise for the provision of

1376 design, operating, or other technological services necessary to  
 1377 develop and maintain the website.

1378 (b)~~(e)~~ CareerSource Florida, Inc., may procure services  
 1379 necessary to implement this section, if it employs competitive  
 1380 processes, including requests for proposals, competitive  
 1381 negotiation, and other competitive processes to ensure that the  
 1382 procurement results in the most cost-effective investment of  
 1383 state funds.

1384 Section 25. Paragraph (b) of subsection (18) of section  
 1385 668.50, Florida Statutes, is amended to read:

1386 668.50 Uniform Electronic Transaction Act.—

1387 (18) ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY  
 1388 GOVERNMENTAL AGENCIES.—

1389 (b) To the extent that a governmental agency uses  
 1390 electronic records and electronic signatures under paragraph  
 1391 (a), the Office of Technology and Data Solutions ~~Agency for~~  
 1392 ~~State Technology~~, in consultation with the governmental agency,  
 1393 giving due consideration to security, may specify:

1394 1. The manner and format in which the electronic records  
 1395 must be created, generated, sent, communicated, received, and  
 1396 stored and the systems established for those purposes.

1397 2. If electronic records must be signed by electronic  
 1398 means, the type of electronic signature required, the manner and  
 1399 format in which the electronic signature must be affixed to the  
 1400 electronic record, and the identity of, or criteria that must be

1401 met by, any third party used by a person filing a document to  
 1402 facilitate the process.

1403 3. Control processes and procedures as appropriate to  
 1404 ensure adequate preservation, disposition, integrity, security,  
 1405 confidentiality, and auditability of electronic records.

1406 4. Any other required attributes for electronic records  
 1407 which are specified for corresponding nonelectronic records or  
 1408 reasonably necessary under the circumstances.

1409 Section 26. Subsections (4) and (5) of section 943.0415,  
 1410 Florida Statutes, are amended to read:

1411 943.0415 Cybercrime Office.—There is created within the  
 1412 Department of Law Enforcement the Cybercrime Office. The office  
 1413 may:

1414 (4) Provide security awareness training and information to  
 1415 state agency employees concerning cybersecurity, online sexual  
 1416 exploitation of children, and security risks, and the  
 1417 responsibility of employees to comply with policies, standards,  
 1418 guidelines, and operating procedures adopted by the Office of  
 1419 Technology and Data Solutions ~~Agency for State Technology~~.

1420 (5) Consult with the Office of Technology and Data  
 1421 Solutions ~~Agency for State Technology~~ in the adoption of rules  
 1422 relating to the information technology security provisions in s.  
 1423 282.318.

1424 Section 27. Florida Cybersecurity Task Force.—

1425 (1) There is created the Florida Cybersecurity Task Force

1426 to review and conduct an assessment of the state's cybersecurity  
1427 infrastructure, governance, and operations.

1428 (2) The Florida Cybersecurity Task Force shall consist of  
1429 the following members:

1430 (a) A representative of the computer crime center of the  
1431 Florida Department of Law Enforcement who shall be appointed by  
1432 the executive director of the department.

1433 (b) A representative of the fusion center of the Florida  
1434 Department of Law Enforcement who shall be appointed by the  
1435 executive director of the department.

1436 (c) The chief information security officer of the Office  
1437 of Technology and Data Solutions.

1438 (d) A representative of the Division of Telecommunications  
1439 of the Department of Management Services who shall be appointed  
1440 by the secretary of the department.

1441 (e) A representative of the Division of Emergency  
1442 Management in the Executive Office of the Governor who shall be  
1443 appointed by the director of the division.

1444 (f) A representative of the Office of the Chief Inspector  
1445 General in the Executive Office of the Governor who shall be  
1446 appointed by the Chief Inspector General.

1447 (3) The task force shall elect a chair from among its  
1448 members.

1449 (4) The task force shall convene by October 1, 2017, and  
1450 shall meet as necessary, but at least quarterly, at the call of

1451 the chair. The Department of Law Enforcement shall provide  
1452 administrative support to the task force.

1453 (5) The task force shall:

1454 (a) Recommend methods to secure the state's network  
1455 systems and data, including standardized plans and procedures to  
1456 identify developing threats and to prevent unauthorized access  
1457 and destruction of data.

1458 (b) Identify and recommend remediation, if necessary, of  
1459 high-risk cybersecurity issues facing state government.

1460 (c) Recommend a process to regularly assess cybersecurity  
1461 infrastructure and activities of executive branch agencies.

1462 (d) Identify gaps in the state's overall cybersecurity  
1463 infrastructure, governance, and current operations. Based on any  
1464 findings of gaps or deficiencies, the task force shall make  
1465 recommendations for improvement.

1466 (e) Recommend cybersecurity improvements for the state's  
1467 emergency management and disaster response systems.

1468 (f) Recommend cybersecurity improvements of the state data  
1469 center.

1470 (g) Review and recommend improvements relating to the  
1471 state's current operational plans for the response,  
1472 coordination, and recovery from a cybersecurity attack.

1473 (6) All executive branch departments and agencies shall  
1474 cooperate fully with requests for information by the task force.

1475 (7) On or before November 1, 2018, the Florida

1476 Cybersecurity Task Force shall submit a final report of its  
1477 findings and recommendations to the Governor, the President of  
1478 the Senate, and the Speaker of the House of Representatives.

1479 (8) This section expires January 1, 2019.

1480 Section 28. Notwithstanding s. 216.292(4)(d), Florida  
1481 Statutes, the transfers authorized in sections 1 and 2 of this  
1482 act do not require Legislative Budget Commission approval.

1483 Section 29. (1) For the 2017-2018 fiscal year, the sum of  
1484 \$1,813,664 in recurring funds is appropriated from the General  
1485 Revenue Fund to the Office of Technology and Data Solutions  
1486 within the Department of Management Services, and seven full-  
1487 time equivalent positions with associated salary rate of 665,684  
1488 are authorized.

1489 (2) The recurring general revenue funds appropriated to  
1490 the Office of Technology and Data Solution within the Department  
1491 of Management Services shall be allocated to specific  
1492 appropriation categories as follows: \$890,158 in Salaries and  
1493 Benefits; \$71,547 in Expenses; \$738,951 in Contracted Services;  
1494 \$2,800 in Operating Capital Outlay; \$4,319 in DMS State Data  
1495 Center; \$3,483 in Risk Management Insurance; \$2,406 in Transfer  
1496 to Department of Management Services - Human Resources Services  
1497 Purchased Per Statewide Contract; and \$100,000 in Administrative  
1498 Overhead.

1499 Section 30. (1) From the funds appropriated in section  
1500 29, \$500,000 provided in the Contracted Services appropriation

HB 5301

2017

1501 category shall be used by the Office of Technology and Data  
1502 Solutions within the Department of Management Services to  
1503 contract with a third party consulting firm with experience in  
1504 conducting independent verification and validation assessments  
1505 to provide independent advisory services for the planning and  
1506 feasibility of initiatives proposed by the Office of Technology  
1507 and Data Solutions that may affect more than one agency. The  
1508 contract shall require all deliverables to be simultaneously  
1509 submitted to the state chief information officer and the Office  
1510 of Policy and Budget in the Executive Office of the Governor,  
1511 and shall be submitted upon request to the chair of the  
1512 appropriations committee of each house of the Legislature.

1513 (2) From the funds appropriated in section 29, \$238,000  
1514 provided in the Contracted Services appropriation category shall  
1515 be used by the Office of Technology and Data Solutions within  
1516 the Department of Management Services to contract with a third  
1517 party consulting firm for technology research and advisory  
1518 services.

1519 Section 31. For the 2017-2018 fiscal year, the sum of  
1520 \$100,000 in nonrecurring funds is appropriated from the General  
1521 Revenue Fund to the Florida Department of Law Enforcement to  
1522 cover the administrative costs associated with the Florida  
1523 Cybersecurity Task Force provisions of this act.

1524 Section 32. This act shall take effect July 1, 2017.