

**By** the Committees on Appropriations; Banking and Insurance; and Innovation, Industry, and Technology; and Senators Hutson and Harrell

576-04569-20

20201870c3

1                                   A bill to be entitled  
2       An act relating to technology innovation; amending s.  
3       20.22, F.S.; establishing the Florida Digital Service  
4       and the Division of Telecommunications within the  
5       Department of Management Services; abolishing the  
6       Division of State Technology within the department;  
7       amending s. 110.205, F.S.; exempting the state chief  
8       data officer and the state chief information security  
9       officer within the Florida Digital Service from the  
10      Career Service System; providing for the salary and  
11      benefits of such positions to be set by the  
12      department; amending s. 282.0041, F.S.; defining  
13      terms; revising the definition of the term "open  
14      data"; amending s. 282.0051, F.S.; revising  
15      information technology-related powers, duties, and  
16      functions of the department acting through the Florida  
17      Digital Service; specifying the designation of the  
18      state chief information officer and the state chief  
19      data officer; specifying qualifications for such  
20      positions; specifying requirements, contingent upon  
21      legislative appropriation, for the department;  
22      authorizing the department to develop a certain  
23      process; prohibiting the department from retrieving or  
24      disclosing any data without a certain shared-data  
25      agreement in place; specifying rulemaking authority  
26      for the department; amending s. 282.00515, F.S.;  
27      requiring the Department of Legal Affairs, the  
28      Department of Financial Services, or the Department of  
29      Agriculture and Consumer Services to notify the

576-04569-20

20201870c3

30 Governor and the Legislature and provide a certain  
31 justification and explanation if such agency adopts  
32 alternative standards to certain enterprise  
33 architecture standards; providing construction;  
34 prohibiting the department from retrieving or  
35 disclosing any data without a certain shared-data  
36 agreement in place; conforming a cross-reference;  
37 amending ss. 282.318, 287.0591, 365.171, 365.172,  
38 365.173, and 943.0415, F.S.; conforming provisions to  
39 changes made by the act; creating s. 559.952, F.S.;

40 providing a short title; creating the Financial  
41 Technology Sandbox within the Office of Financial  
42 Regulation; defining terms; requiring the office, if  
43 certain conditions are met, to grant a license to a  
44 Financial Technology Sandbox applicant, grant  
45 exceptions to specified provisions of general law  
46 relating to consumer finance loans and money services  
47 businesses, and grant waivers of certain rules;  
48 authorizing a substantially affected person to seek a  
49 declaratory statement before applying to the Financial  
50 Technology Sandbox; specifying application  
51 requirements and procedures; specifying requirements  
52 and procedures for the office in reviewing and  
53 approving or denying applications; providing  
54 requirements for the office in specifying the number  
55 of the consumers authorized to receive an innovative  
56 financial product or service; specifying authorized  
57 actions of, limitations on, and requirements for  
58 licensees operating in the Financial Technology

576-04569-20

20201870c3

59 Sandbox; requiring licensees to make a specified  
60 disclosure to consumers; authorizing the office to  
61 enter into certain agreements with other regulatory  
62 agencies; authorizing the office to examine licensee  
63 records; authorizing a licensee to apply for one  
64 extension of an initial sandbox period for a certain  
65 timeframe; specifying requirements and procedures for  
66 applying for an extension; specifying requirements and  
67 procedures for, and authorized actions of, licensees  
68 when concluding a sandbox period or extension;  
69 requiring licensees to submit certain reports to the  
70 office at specified intervals; providing construction;  
71 specifying the liability of a licensee; authorizing  
72 the office to take certain disciplinary actions  
73 against a licensee under certain circumstances;  
74 providing construction relating to service of process;  
75 specifying the rulemaking authority of the Financial  
76 Services Commission; providing the office authority to  
77 issue orders and enforce the orders; providing an  
78 appropriation; providing that specified provisions of  
79 the act are contingent upon passage of other  
80 provisions addressing public records; providing  
81 effective dates.

82  
83 Be It Enacted by the Legislature of the State of Florida:

84  
85 Section 1. Subsection (2) of section 20.22, Florida  
86 Statutes, is amended to read:

87 20.22 Department of Management Services.—There is created a

576-04569-20

20201870c3

88 Department of Management Services.

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

91 (a) Facilities Program.

92 (b) The Florida Digital Service ~~Division of State~~  
93 ~~Technology, the director of which is appointed by the secretary~~  
94 ~~of the department and shall serve as the state chief information~~  
95 ~~officer. The state chief information officer must be a proven,~~  
96 ~~effective administrator who must have at least 10 years of~~  
97 ~~executive-level experience in the public or private sector,~~  
98 ~~preferably with experience in the development of information~~  
99 ~~technology strategic planning and the development and~~  
100 ~~implementation of fiscal and substantive information technology~~  
101 ~~policy and standards.~~

102 (c) Workforce Program.

103 (d) 1. Support Program.

104 2. Federal Property Assistance Program.

105 (e) Administration Program.

106 (f) Division of Administrative Hearings.

107 (g) Division of Retirement.

108 (h) Division of State Group Insurance.

109 (i) Division of Telecommunications.

110 Section 2. Paragraph (e) of subsection (2) of section  
111 110.205, Florida Statutes, is amended to read:

112 110.205 Career service; exemptions.—

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

115 (e) The state chief information officer, the state chief  
116 data officer, and the state chief information security officer.

576-04569-20

20201870c3

117 ~~Unless otherwise fixed by law,~~ The Department of Management  
118 Services shall set the salary and benefits of these positions  
119 ~~this position~~ in accordance with the rules of the Senior  
120 Management Service.

121 Section 3. Section 282.0041, Florida Statutes, is amended  
122 to read:

123 282.0041 Definitions.—As used in this chapter, the term:

124 (1) "Agency assessment" means the amount each customer  
125 entity must pay annually for services from the Department of  
126 Management Services and includes administrative and data center  
127 services costs.

128 (2) "Agency data center" means agency space containing 10  
129 or more physical or logical servers.

130 (3) "Breach" has the same meaning as provided in s.  
131 501.171.

132 (4) "Business continuity plan" means a collection of  
133 procedures and information designed to keep an agency's critical  
134 operations running during a period of displacement or  
135 interruption of normal operations.

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

139 (6) "Computing facility" or "agency computing facility"  
140 means agency space containing fewer than a total of 10 physical  
141 or logical servers, but excluding single, logical-server  
142 installations that exclusively perform a utility function such  
143 as file and print servers.

144 (7) "Customer entity" means an entity that obtains services  
145 from the Department of Management Services.

576-04569-20

20201870c3

146 (8) "Data" means a subset of structured information in a  
147 format that allows such information to be electronically  
148 retrieved and transmitted.

149 (9) "Data governance" means the practice of organizing,  
150 classifying, securing, and implementing policies, procedures,  
151 and standards for the effective use of an organization's data.

152 (10) "Department" means the Department of Management  
153 Services.

154 ~~(11)~~ (10) "Disaster recovery" means the process, policies,  
155 procedures, and infrastructure related to preparing for and  
156 implementing recovery or continuation of an agency's vital  
157 technology infrastructure after a natural or human-induced  
158 disaster.

159 (12) "Electronic" means technology having electrical,  
160 digital, magnetic, wireless, optical, electromagnetic, or  
161 similar capabilities.

162 (13) "Electronic credential" means an electronic  
163 representation of the identity of a person, an organization, an  
164 application, or a device.

165 (14) "Enterprise" means state agencies and the Department  
166 of Legal Affairs, the Department of Financial Services, and the  
167 Department of Agriculture and Consumer Services.

168 (15) "Enterprise architecture" means a comprehensive  
169 operational framework that contemplates the needs and assets of  
170 the enterprise to support interoperability.

171 ~~(16)~~ (15) "Enterprise information technology service" means  
172 an information technology service that is used in all agencies  
173 or a subset of agencies and is established in law to be  
174 designed, delivered, and managed at the enterprise level.

576-04569-20

20201870c3

175        (17)~~(12)~~ "Event" means an observable occurrence in a system  
176 or network.

177        (18)~~(13)~~ "Incident" means a violation or imminent threat of  
178 violation, whether such violation is accidental or deliberate,  
179 of information technology resources, security, policies, or  
180 practices. An imminent threat of violation refers to a situation  
181 in which the state agency has a factual basis for believing that  
182 a specific incident is about to occur.

183        (19)~~(14)~~ "Information technology" means equipment,  
184 hardware, software, firmware, programs, systems, networks,  
185 infrastructure, media, and related material used to  
186 automatically, electronically, and wirelessly collect, receive,  
187 access, transmit, display, store, record, retrieve, analyze,  
188 evaluate, process, classify, manipulate, manage, assimilate,  
189 control, communicate, exchange, convert, converge, interface,  
190 switch, or disseminate information of any kind or form.

191        (20)~~(15)~~ "Information technology policy" means a definite  
192 course or method of action selected from among one or more  
193 alternatives that guide and determine present and future  
194 decisions.

195        (21)~~(16)~~ "Information technology resources" has the same  
196 meaning as provided in s. 119.011.

197        (22)~~(17)~~ "Information technology security" means the  
198 protection afforded to an automated information system in order  
199 to attain the applicable objectives of preserving the integrity,  
200 availability, and confidentiality of data, information, and  
201 information technology resources.

202        (23) "Interoperability" means the technical ability to  
203 share and use data across and throughout the enterprise.

576-04569-20

20201870c3

204        ~~(24)(18)~~ "Open data" means data collected or created by a  
205 state agency, the Department of Legal Affairs, the Department of  
206 Financial Services, and the Department of Agriculture and  
207 Consumer Services, and structured in a way that enables the data  
208 to be fully discoverable and usable by the public. The term does  
209 not include data that are restricted from public disclosure  
210 ~~distribution~~ based on federal or state ~~privacy, confidentiality,~~  
211 ~~and security~~ laws and regulations, including, but not limited  
212 to, those related to privacy, confidentiality, security,  
213 personal health, business or trade secret information, and  
214 exemptions from state public records laws; or data for which a  
215 state agency, the Department of Legal Affairs, the Department of  
216 Financial Services, or the Department of Agriculture and  
217 Consumer Services is statutorily authorized to assess a fee for  
218 its distribution.

219        ~~(25)(19)~~ "Performance metrics" means the measures of an  
220 organization's activities and performance.

221        ~~(26)(20)~~ "Project" means an endeavor that has a defined  
222 start and end point; is undertaken to create or modify a unique  
223 product, service, or result; and has specific objectives that,  
224 when attained, signify completion.

225        ~~(27)(21)~~ "Project oversight" means an independent review  
226 and analysis of an information technology project that provides  
227 information on the project's scope, completion timeframes, and  
228 budget and that identifies and quantifies issues or risks  
229 affecting the successful and timely completion of the project.

230        ~~(28)(22)~~ "Risk assessment" means the process of identifying  
231 security risks, determining their magnitude, and identifying  
232 areas needing safeguards.



576-04569-20

20201870c3

233        (29)~~(23)~~ "Service level" means the key performance  
234 indicators (KPI) of an organization or service which must be  
235 regularly performed, monitored, and achieved.

236        (30)~~(24)~~ "Service-level agreement" means a written contract  
237 between the Department of Management Services and a customer  
238 entity which specifies the scope of services provided, service  
239 level, the duration of the agreement, the responsible parties,  
240 and service costs. A service-level agreement is not a rule  
241 pursuant to chapter 120.

242        (31)~~(25)~~ "Stakeholder" means a person, group, organization,  
243 or state agency involved in or affected by a course of action.

244        (32)~~(26)~~ "Standards" means required practices, controls,  
245 components, or configurations established by an authority.

246        (33)~~(27)~~ "State agency" means any official, officer,  
247 commission, board, authority, council, committee, or department  
248 of the executive branch of state government; the Justice  
249 Administrative Commission; and the Public Service Commission.  
250 The term does not include university boards of trustees or state  
251 universities. As used in part I of this chapter, except as  
252 otherwise specifically provided, the term does not include the  
253 Department of Legal Affairs, the Department of Agriculture and  
254 Consumer Services, or the Department of Financial Services.

255        (34)~~(28)~~ "SUNCOM Network" means the state enterprise  
256 telecommunications system that provides all methods of  
257 electronic or optical telecommunications beyond a single  
258 building or contiguous building complex and used by entities  
259 authorized as network users under this part.

260        (35)~~(29)~~ "Telecommunications" means the science and  
261 technology of communication at a distance, including electronic

576-04569-20

20201870c3

262 systems used in the transmission or reception of information.

263 ~~(36)~~~~(30)~~ "Threat" means any circumstance or event that has  
264 the potential to adversely impact a state agency's operations or  
265 assets through an information system via unauthorized access,  
266 destruction, disclosure, or modification of information or  
267 denial of service.

268 ~~(37)~~~~(31)~~ "Variance" means a calculated value that  
269 illustrates how far positive or negative a projection has  
270 deviated when measured against documented estimates within a  
271 project plan.

272 Section 4. Section 282.0051, Florida Statutes, is amended  
273 to read:

274 282.0051 Department of Management Services; Florida Digital  
275 Service; powers, duties, and functions.—

276 (1) The Florida Digital Service has been created within the  
277 department to propose innovative solutions that securely  
278 modernize state government, including technology and information  
279 services, to achieve value through digital transformation and  
280 interoperability, and to fully support the cloud-first policy as  
281 specified in s. 282.206. The department, through the Florida  
282 Digital Service, shall have the following powers, duties, and  
283 functions:

284 (a)~~(1)~~ Develop and publish information technology policy  
285 for the management of the state's information technology  
286 resources.

287 (b)~~(2)~~ Develop an enterprise architecture that:

288 1. Acknowledges the unique needs of the entities within the  
289 enterprise in the development and publication of standards and  
290 terminologies to facilitate digital interoperability;

576-04569-20

20201870c3

291 2. Supports the cloud-first policy as specified in s.  
292 282.206; and

293 3. Addresses how information technology infrastructure may  
294 be modernized to achieve cloud-first objectives ~~Establish and~~  
295 ~~publish information technology architecture standards to provide~~  
296 ~~for the most efficient use of the state's information technology~~  
297 ~~resources and to ensure compatibility and alignment with the~~  
298 ~~needs of state agencies. The department shall assist state~~  
299 ~~agencies in complying with the standards.~~

300 (c)-(3) Establish project management and oversight standards  
301 with which state agencies must comply when implementing  
302 information technology projects. The department, acting through  
303 the Florida Digital Service, shall provide training  
304 opportunities to state agencies to assist in the adoption of the  
305 project management and oversight standards. To support data-  
306 driven decisionmaking, the standards must include, but are not  
307 limited to:

308 1.(a) Performance measurements and metrics that objectively  
309 reflect the status of an information technology project based on  
310 a defined and documented project scope, cost, and schedule.

311 2.(b) Methodologies for calculating acceptable variances in  
312 the projected versus actual scope, schedule, or cost of an  
313 information technology project.

314 3.(e) Reporting requirements, including requirements  
315 designed to alert all defined stakeholders that an information  
316 technology project has exceeded acceptable variances defined and  
317 documented in a project plan.

318 4.(d) Content, format, and frequency of project updates.

319 (d)-(4) Perform project oversight on all state agency

576-04569-20

20201870c3

320 information technology projects that have total project costs of  
321 \$10 million or more and that are funded in the General  
322 Appropriations Act or any other law. The department, acting  
323 through the Florida Digital Service, shall report at least  
324 quarterly to the Executive Office of the Governor, the President  
325 of the Senate, and the Speaker of the House of Representatives  
326 on any information technology project that the department  
327 identifies as high-risk due to the project exceeding acceptable  
328 variance ranges defined and documented in a project plan. The  
329 report must include a risk assessment, including fiscal risks,  
330 associated with proceeding to the next stage of the project, and  
331 a recommendation for corrective actions required, including  
332 suspension or termination of the project.

333 (e)~~(5)~~ Identify opportunities for standardization and  
334 consolidation of information technology services that support  
335 interoperability and the cloud-first policy, as specified in s.  
336 282.206, and business functions and operations, including  
337 administrative functions such as purchasing, accounting and  
338 reporting, cash management, and personnel, and that are common  
339 across state agencies. The department, acting through the  
340 Florida Digital Service, shall biennially on January 1 of each  
341 even-numbered year ~~April 1~~ provide recommendations for  
342 standardization and consolidation to the Executive Office of the  
343 Governor, the President of the Senate, and the Speaker of the  
344 House of Representatives.

345 (f)~~(6)~~ Establish best practices for the procurement of  
346 information technology products and cloud-computing services in  
347 order to reduce costs, increase the quality of data center  
348 services, or improve government services.

576-04569-20

20201870c3

349        (g)~~(7)~~ Develop standards for information technology reports  
350 and updates, including, but not limited to, operational work  
351 plans, project spend plans, and project status reports, for use  
352 by state agencies.

353        (h)~~(8)~~ Upon request, assist state agencies in the  
354 development of information technology-related legislative budget  
355 requests.

356        (i)~~(9)~~ Conduct annual assessments of state agencies to  
357 determine compliance with all information technology standards  
358 and guidelines developed and published by the department and  
359 provide results of the assessments to the Executive Office of  
360 the Governor, the President of the Senate, and the Speaker of  
361 the House of Representatives.

362        (j)~~(10)~~ Provide operational management and oversight of the  
363 state data center established pursuant to s. 282.201, which  
364 includes:

365            1.~~(a)~~ Implementing industry standards and best practices  
366 for the state data center's facilities, operations, maintenance,  
367 planning, and management processes.

368            2.~~(b)~~ Developing and implementing cost-recovery mechanisms  
369 that recover the full direct and indirect cost of services  
370 through charges to applicable customer entities. Such cost-  
371 recovery mechanisms must comply with applicable state and  
372 federal regulations concerning distribution and use of funds and  
373 must ensure that, for any fiscal year, no service or customer  
374 entity subsidizes another service or customer entity. The  
375 Florida Digital Service may recommend other payment mechanisms  
376 to the Executive Office of the Governor, the President of the  
377 Senate, and the Speaker of the House of Representatives. Such

576-04569-20

20201870c3

378 mechanism may be implemented only if specifically authorized by  
379 the Legislature.

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

387 a.1. Implementing a consolidated administrative support  
388 structure responsible for providing financial management,  
389 procurement, transactions involving real or personal property,  
390 human resources, and operational support.

391 b.2. Implementing an annual reconciliation process to  
392 ensure that each customer entity is paying for the full direct  
393 and indirect cost of each service as determined by the customer  
394 entity's use of each service.

395 c.3. Providing rebates that may be credited against future  
396 billings to customer entities when revenues exceed costs.

397 d.4. Requiring customer entities to validate that  
398 sufficient funds exist in the appropriate data processing  
399 appropriation category or will be transferred into the  
400 appropriate data processing appropriation category before  
401 implementation of a customer entity's request for a change in  
402 the type or level of service provided, if such change results in  
403 a net increase to the customer entity's cost for that fiscal  
404 year.

405 e.5. By November 15 of each year, providing to the Office  
406 of Policy and Budget in the Executive Office of the Governor and

576-04569-20

20201870c3

407 to the chairs of the legislative appropriations committees the  
408 projected costs of providing data center services for the  
409 following fiscal year.

410 ~~f.6.~~ Providing a plan for consideration by the Legislative  
411 Budget Commission if the cost of a service is increased for a  
412 reason other than a customer entity's request made pursuant to  
413 sub-subparagraph d. ~~subparagraph 4.~~ Such a plan is required only  
414 if the service cost increase results in a net increase to a  
415 customer entity for that fiscal year.

416 ~~g.7.~~ Standardizing and consolidating procurement and  
417 contracting practices.

418 ~~4.(d)~~ In collaboration with the Department of Law  
419 Enforcement, developing and implementing a process for  
420 detecting, reporting, and responding to information technology  
421 security incidents, breaches, and threats.

422 ~~5.(e)~~ Adopting rules relating to the operation of the state  
423 data center, including, but not limited to, budgeting and  
424 accounting procedures, cost-recovery methodologies, and  
425 operating procedures.

426 (k) Conduct a market analysis not less frequently than  
427 every 3 years beginning in 2021 to determine whether the  
428 information technology resources within the enterprise are  
429 utilized in the most cost-effective and cost-efficient manner,  
430 while recognizing that the replacement of certain legacy  
431 information technology systems within the enterprise may be cost  
432 prohibitive or cost inefficient due to the remaining useful life  
433 of those resources; whether the enterprise is complying with the  
434 cloud-first policy specified in s. 282.206; and whether the  
435 enterprise is utilizing best practices with respect to

576-04569-20

20201870c3

436 information technology, information services, and the  
437 acquisition of emerging technologies and information services.  
438 Each market analysis shall be used to prepare a strategic plan  
439 for continued and future information technology and information  
440 services for the enterprise, including, but not limited to,  
441 proposed acquisition of new services or technologies and  
442 approaches to the implementation of any new services or  
443 technologies. Copies of each market analysis and accompanying  
444 strategic plan must be submitted to the Executive Office of the  
445 Governor, the President of the Senate, and the Speaker of the  
446 House of Representatives not later than December 31 of each year  
447 that a market analysis is conducted.

448 ~~(f) Conducting an annual market analysis to determine~~  
449 ~~whether the state's approach to the provision of data center~~  
450 ~~services is the most effective and cost-efficient manner by~~  
451 ~~which its customer entities can acquire such services, based on~~  
452 ~~federal, state, and local government trends; best practices in~~  
453 ~~service provision; and the acquisition of new and emerging~~  
454 ~~technologies. The results of the market analysis shall assist~~  
455 ~~the state data center in making adjustments to its data center~~  
456 ~~service offerings.~~

457 (1)~~(11)~~ Recommend other information technology services  
458 that should be designed, delivered, and managed as enterprise  
459 information technology services. Recommendations must include  
460 the identification of existing information technology resources  
461 associated with the services, if existing services must be  
462 transferred as a result of being delivered and managed as  
463 enterprise information technology services.

464 (m)~~(12)~~ In consultation with state agencies, propose a



576-04569-20

20201870c3

465 methodology and approach for identifying and collecting both  
466 current and planned information technology expenditure data at  
467 the state agency level.

468 (n) 1. (13) (a) Notwithstanding any other law, provide project  
469 oversight on any information technology project of the  
470 Department of Financial Services, the Department of Legal  
471 Affairs, and the Department of Agriculture and Consumer Services  
472 which has a total project cost of \$25 million or more and which  
473 impacts one or more other agencies. Such information technology  
474 projects must also comply with the applicable information  
475 technology architecture, project management and oversight, and  
476 reporting standards established by the department, acting  
477 through the Florida Digital Service.

478 2. (b) When performing the project oversight function  
479 specified in subparagraph 1. paragraph (a), report at least  
480 quarterly to the Executive Office of the Governor, the President  
481 of the Senate, and the Speaker of the House of Representatives  
482 on any information technology project that the department,  
483 acting through the Florida Digital Service, identifies as high-  
484 risk due to the project exceeding acceptable variance ranges  
485 defined and documented in the project plan. The report shall  
486 include a risk assessment, including fiscal risks, associated  
487 with proceeding to the next stage of the project and a  
488 recommendation for corrective actions required, including  
489 suspension or termination of the project.

490 (o) (14) If an information technology project implemented by  
491 a state agency must be connected to or otherwise accommodated by  
492 an information technology system administered by the Department  
493 of Financial Services, the Department of Legal Affairs, or the

576-04569-20

20201870c3

494 Department of Agriculture and Consumer Services, consult with  
495 these departments regarding the risks and other effects of such  
496 projects on their information technology systems and work  
497 cooperatively with these departments regarding the connections,  
498 interfaces, timing, or accommodations required to implement such  
499 projects.

500 (p) ~~(15)~~ If adherence to standards or policies adopted by or  
501 established pursuant to this section causes conflict with  
502 federal regulations or requirements imposed on an entity within  
503 the enterprise ~~a state agency~~ and results in adverse action  
504 against an entity ~~the state agency~~ or federal funding, work with  
505 the entity ~~state agency~~ to provide alternative standards,  
506 policies, or requirements that do not conflict with the federal  
507 regulation or requirement. The department, acting through the  
508 Florida Digital Service, shall annually report such alternative  
509 standards to the Executive Office of the Governor, the President  
510 of the Senate, and the Speaker of the House of Representatives.

511 (q) 1. ~~(16) (a)~~ Establish an information technology policy for  
512 all information technology-related state contracts, including  
513 state term contracts for information technology commodities,  
514 consultant services, and staff augmentation services. The  
515 information technology policy must include:

516 a.1. ~~1.~~ Identification of the information technology product  
517 and service categories to be included in state term contracts.

518 b.2. ~~2.~~ Requirements to be included in solicitations for state  
519 term contracts.

520 c.3. ~~3.~~ Evaluation criteria for the award of information  
521 technology-related state term contracts.

522 d.4. ~~4.~~ The term of each information technology-related state

576-04569-20

20201870c3

523 term contract.

524 ~~e.5.~~ The maximum number of vendors authorized on each state  
525 term contract.

526 ~~2.(b)~~ Evaluate vendor responses for information technology-  
527 related state term contract solicitations and invitations to  
528 negotiate.

529 ~~3.(e)~~ Answer vendor questions on information technology-  
530 related state term contract solicitations.

531 ~~4.(d)~~ Ensure that the information technology policy  
532 established pursuant to subparagraph 1. ~~paragraph (a)~~ is  
533 included in all solicitations and contracts that are  
534 administratively executed by the department.

535 ~~(r) (17)~~ Recommend potential methods for standardizing data  
536 across state agencies which will promote interoperability and  
537 reduce the collection of duplicative data.

538 ~~(s) (18)~~ Recommend open data technical standards and  
539 terminologies for use by the enterprise state agencies.

540 (t) Ensure that enterprise information technology solutions  
541 are capable of utilizing an electronic credential and comply  
542 with the enterprise architecture standards.

543 (2) (a) The Secretary of Management Services shall designate  
544 a state chief information officer, who shall administer the  
545 Florida Digital Service. The state chief information officer,  
546 prior to appointment, must have at least 5 years of experience  
547 in the development of information system strategic planning and  
548 development or information technology policy, and, preferably,  
549 have leadership-level experience in the design, development, and  
550 deployment of interoperable software and data solutions.

551 (b) The state chief information officer, in consultation

576-04569-20

20201870c3

552 with the Secretary of Management Services, shall designate a  
553 state chief data officer. The chief data officer must be a  
554 proven and effective administrator who must have significant and  
555 substantive experience in data management, data governance,  
556 interoperability, and security.

557 (3) The department, acting through the Florida Digital  
558 Service and from funds appropriated to the Florida Digital  
559 Service, shall:

560 (a) Create, not later than October 1, 2021, and maintain a  
561 comprehensive indexed data catalog in collaboration with the  
562 enterprise that lists the data elements housed within the  
563 enterprise and the legacy system or application in which these  
564 data elements are located. The data catalog must, at a minimum,  
565 specifically identify all data that is restricted from public  
566 disclosure based on federal or state laws and regulations and  
567 require that all such information be protected in accordance  
568 with s. 282.318.

569 (b) Develop and publish, not later than October 1, 2021, in  
570 collaboration with the enterprise, a data dictionary for each  
571 agency that reflects the nomenclature in the comprehensive  
572 indexed data catalog.

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

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

579 (e) Adopt, by rule, standards that facilitate the  
580 deployment of applications or solutions to the existing

576-04569-20

20201870c3

581 enterprise system in a controlled and phased approach.

582 (f) After submission of documented use cases developed in  
583 conjunction with the affected agencies, assist the affected  
584 agencies with the deployment, contingent upon a specific  
585 appropriation therefor, of new interoperable applications and  
586 solutions:

587 1. For the Department of Health, the Agency for Health Care  
588 Administration, the Agency for Persons with Disabilities, the  
589 Department of Education, the Department of Elderly Affairs, and  
590 the Department of Children and Families.

591 2. To support military members, veterans, and their  
592 families.

593 (4) Upon the adoption of the enterprise architecture  
594 standards in rule, the department, acting through the Florida  
595 Digital Service, may develop a process to:

596 (a) Receive written notice from the entities within the  
597 enterprise of any planned procurement of an information  
598 technology project that is subject to enterprise architecture  
599 standards.

600 (b) Participate in the development of specifications and  
601 recommend modifications to any planned procurement by state  
602 agencies so that the procurement complies with the enterprise  
603 architecture.

604 (5) The department, acting through the Florida Digital  
605 Service, may not retrieve or disclose any data without a shared-  
606 data agreement in place between the department and the  
607 enterprise entity that has primary custodial responsibility of,  
608 or data-sharing responsibility for, that data.

609 (6) The department, acting through the Florida Digital

576-04569-20

20201870c3

610 Service, shall adopt rules to administer this section.

611 ~~(19) Adopt rules to administer this section.~~

612 Section 5. Section 282.00515, Florida Statutes, is amended  
613 to read:

614 282.00515 Duties of Cabinet agencies.—

615 (1) The Department of Legal Affairs, the Department of  
616 Financial Services, and the Department of Agriculture and  
617 Consumer Services shall adopt the standards established in s.  
618 282.0051(1)(b), (c), and (s) and (3)(e) s. 282.0051(2), (3), and  
619 ~~(7)~~ or adopt alternative standards based on best practices and  
620 industry standards that allow for open data interoperability.

621 (2) If the Department of Legal Affairs, the Department of  
622 Financial Services, or the Department of Agriculture and  
623 Consumer Services adopts alternative standards in lieu of the  
624 enterprise architecture standards adopted pursuant to s.  
625 282.0051, such department must notify the Governor, the  
626 President of the Senate, and the Speaker of the House of  
627 Representatives in writing of the adoption of the alternative  
628 standards and provide a justification for adoption of the  
629 alternative standards and explain how the agency will achieve  
630 open data interoperability.

631 (3) The Department of Legal Affairs, the Department of  
632 Financial Services, and the Department of Agriculture and  
633 Consumer Services, and may contract with the department to  
634 provide or perform any of the services and functions described  
635 in s. 282.0051 for the Department of Legal Affairs, the  
636 Department of Financial Services, or the Department of  
637 Agriculture and Consumer Services.

638 (4) (a) Nothing in this section or in s. 282.0051 requires

576-04569-20

20201870c3

639 the Department of Legal Affairs, the Department of Financial  
640 Services, or the Department of Agriculture and Consumer Services  
641 to integrate with information technology outside its own  
642 department or with the Florida Digital Service.

643 (b) The department, acting through the Florida Digital  
644 Service, may not retrieve or disclose any data without a shared-  
645 data agreement in place between the department and the  
646 Department of Legal Affairs, the Department of Financial  
647 Services, or the Department of Agriculture and Consumer  
648 Services.

649 Section 6. Paragraph (a) of subsection (3), paragraphs (d),  
650 (e), (g), and (j) of subsection (4), and subsection (5) of  
651 section 282.318, Florida Statutes, are amended to read:

652 282.318 Security of data and information technology.—

653 (3) The department is responsible for establishing  
654 standards and processes consistent with generally accepted best  
655 practices for information technology security, to include  
656 cybersecurity, and adopting rules that safeguard an agency's  
657 data, information, and information technology resources to  
658 ensure availability, confidentiality, and integrity and to  
659 mitigate risks. The department shall also:

660 (a) Designate an employee of the Florida Digital Service as  
661 the a state chief information security officer. The state chief  
662 information security officer ~~who~~ must have experience and  
663 expertise in security and risk management for communications and  
664 information technology resources.

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

666 (d) Conduct, and update every 3 years, a comprehensive risk  
667 assessment, which may be completed by a private sector vendor,

576-04569-20

20201870c3

668 to determine the security threats to the data, information, and  
669 information technology resources, including mobile devices and  
670 print environments, of the agency. The risk assessment must  
671 comply with the risk assessment methodology developed by the  
672 department and is confidential and exempt from s. 119.07(1),  
673 except that such information shall be available to the Auditor  
674 General, the Florida Digital Service ~~Division of State~~  
675 ~~Technology~~ within the department, the Cybercrime Office of the  
676 Department of Law Enforcement, and, for state agencies under the  
677 jurisdiction of the Governor, the Chief Inspector General.

678 (e) Develop, and periodically update, written internal  
679 policies and procedures, which include procedures for reporting  
680 information technology security incidents and breaches to the  
681 Cybercrime Office of the Department of Law Enforcement and the  
682 Florida Digital Service ~~Division of State Technology~~ within the  
683 department. Such policies and procedures must be consistent with  
684 the rules, guidelines, and processes established by the  
685 department to ensure the security of the data, information, and  
686 information technology resources of the agency. The internal  
687 policies and procedures that, if disclosed, could facilitate the  
688 unauthorized modification, disclosure, or destruction of data or  
689 information technology resources are confidential information  
690 and exempt from s. 119.07(1), except that such information shall  
691 be available to the Auditor General, the Cybercrime Office of  
692 the Department of Law Enforcement, the Florida Digital Service  
693 ~~Division of State Technology~~ within the department, and, for  
694 state agencies under the jurisdiction of the Governor, the Chief  
695 Inspector General.

696 (g) Ensure that periodic internal audits and evaluations of



576-04569-20

20201870c3

697 the agency's information technology security program for the  
698 data, information, and information technology resources of the  
699 agency are conducted. The results of such audits and evaluations  
700 are confidential information and exempt from s. 119.07(1),  
701 except that such information shall be available to the Auditor  
702 General, the Cybercrime Office of the Department of Law  
703 Enforcement, the Florida Digital Service ~~Division of State~~  
704 ~~Technology~~ within the department, and, for agencies under the  
705 jurisdiction of the Governor, the Chief Inspector General.

706 (j) Develop a process for detecting, reporting, and  
707 responding to threats, breaches, or information technology  
708 security incidents which is consistent with the security rules,  
709 guidelines, and processes established by the department ~~Agency~~  
710 ~~for State Technology~~.

711 1. All information technology security incidents and  
712 breaches must be reported to the Florida Digital Service  
713 ~~Division of State Technology~~ within the department and the  
714 Cybercrime Office of the Department of Law Enforcement and must  
715 comply with the notification procedures and reporting timeframes  
716 established pursuant to paragraph (3)(c).

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

719 3. Records held by a state agency which identify detection,  
720 investigation, or response practices for suspected or confirmed  
721 information technology security incidents, including suspected  
722 or confirmed breaches, are confidential and exempt from s.  
723 119.07(1) and s. 24(a), Art. I of the State Constitution, if the  
724 disclosure of such records would facilitate unauthorized access  
725 to or the unauthorized modification, disclosure, or destruction

576-04569-20

20201870c3

726 of:

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

728 b. Information technology resources, which includes:

729 (I) Information relating to the security of the agency's  
730 technologies, processes, and practices designed to protect  
731 networks, computers, data processing software, and data from  
732 attack, damage, or unauthorized access; or

733 (II) Security information, whether physical or virtual,  
734 which relates to the agency's existing or proposed information  
735 technology systems.

736

737 Such records shall be available to the Auditor General, the  
738 Florida Digital Service ~~Division of State Technology~~ within the  
739 department, the Cybercrime Office of the Department of Law  
740 Enforcement, and, for state agencies under the jurisdiction of  
741 the Governor, the Chief Inspector General. Such records may be  
742 made available to a local government, another state agency, or a  
743 federal agency for information technology security purposes or  
744 in furtherance of the state agency's official duties. This  
745 exemption applies to such records held by a state agency before,  
746 on, or after the effective date of this exemption. This  
747 subparagraph is subject to the Open Government Sunset Review Act  
748 in accordance with s. 119.15 and shall stand repealed on October  
749 2, 2021, unless reviewed and saved from repeal through  
750 reenactment by the Legislature.

751 (5) The portions of risk assessments, evaluations, external  
752 audits, and other reports of a state agency's information  
753 technology security program for the data, information, and  
754 information technology resources of the state agency which are

576-04569-20

20201870c3

755 held by a state agency are confidential and exempt from s.  
756 119.07(1) and s. 24(a), Art. I of the State Constitution if the  
757 disclosure of such portions of records would facilitate  
758 unauthorized access to or the unauthorized modification,  
759 disclosure, or destruction of:

- 760 (a) Data or information, whether physical or virtual; or
- 761 (b) Information technology resources, which include:
  - 762 1. Information relating to the security of the agency's  
763 technologies, processes, and practices designed to protect  
764 networks, computers, data processing software, and data from  
765 attack, damage, or unauthorized access; or
  - 766 2. Security information, whether physical or virtual, which  
767 relates to the agency's existing or proposed information  
768 technology systems.

769

770 Such portions of records shall be available to the Auditor  
771 General, the Cybercrime Office of the Department of Law  
772 Enforcement, the Florida Digital Service ~~Division of State~~  
773 ~~Technology~~ within the department, and, for agencies under the  
774 jurisdiction of the Governor, the Chief Inspector General. Such  
775 portions of records may be made available to a local government,  
776 another state agency, or a federal agency for information  
777 technology security purposes or in furtherance of the state  
778 agency's official duties. For purposes of this subsection,  
779 "external audit" means an audit that is conducted by an entity  
780 other than the state agency that is the subject of the audit.  
781 This exemption applies to such records held by a state agency  
782 before, on, or after the effective date of this exemption. This  
783 subsection is subject to the Open Government Sunset Review Act

576-04569-20

20201870c3

784 in accordance with s. 119.15 and shall stand repealed on October  
785 2, 2021, unless reviewed and saved from repeal through  
786 reenactment by the Legislature.

787 Section 7. Subsection (4) of section 287.0591, Florida  
788 Statutes, is amended to read:

789 287.0591 Information technology.—

790 (4) If the department issues a competitive solicitation for  
791 information technology commodities, consultant services, or  
792 staff augmentation contractual services, the Florida Digital  
793 Service Division of State Technology within the department shall  
794 participate in such solicitations.

795 Section 8. Paragraph (a) of subsection (3) of section  
796 365.171, Florida Statutes, is amended to read:

797 365.171 Emergency communications number E911 state plan.—

798 (3) DEFINITIONS.—As used in this section, the term:

799 (a) "Office" means the Division of Telecommunications ~~State~~  
800 ~~Technology~~ within the Department of Management Services, as  
801 designated by the secretary of the department.

802 Section 9. Paragraph (s) of subsection (3) of section  
803 365.172, Florida Statutes, is amended to read:

804 365.172 Emergency communications number "E911."—

805 (3) DEFINITIONS.—Only as used in this section and ss.  
806 365.171, 365.173, 365.174, and 365.177, the term:

807 (s) "Office" means the Division of Telecommunications ~~State~~  
808 ~~Technology~~ within the Department of Management Services, as  
809 designated by the secretary of the department.

810 Section 10. Paragraph (a) of subsection (1) of section  
811 365.173, Florida Statutes, is amended to read:

812 365.173 Communications Number E911 System Fund.—

576-04569-20

20201870c3

813 (1) REVENUES.—

814 (a) Revenues derived from the fee levied on subscribers  
815 under s. 365.172(8) must be paid by the board into the State  
816 Treasury on or before the 15th day of each month. Such moneys  
817 must be accounted for in a special fund to be designated as the  
818 Emergency Communications Number E911 System Fund, a fund created  
819 in the Division of Telecommunications ~~State Technology~~, or other  
820 office as designated by the Secretary of Management Services.

821 Section 11. Subsection (5) of section 943.0415, Florida  
822 Statutes, is amended to read:

823 943.0415 Cybercrime Office.—There is created within the  
824 Department of Law Enforcement the Cybercrime Office. The office  
825 may:

826 (5) Consult with the Florida Digital Service ~~Division of~~  
827 ~~State Technology~~ within the Department of Management Services in  
828 the adoption of rules relating to the information technology  
829 security provisions in s. 282.318.

830 Section 12. Effective January 1, 2021, section 559.952,  
831 Florida Statutes, is created to read:

832 559.952 Financial Technology Sandbox.—

833 (1) SHORT TITLE.—This section may be cited as the  
834 “Financial Technology Sandbox.”

835 (2) CREATION OF THE FINANCIAL TECHNOLOGY SANDBOX.—There is  
836 created the Financial Technology Sandbox within the Office of  
837 Financial Regulation to allow financial technology innovators to  
838 test new products and services in a supervised, flexible  
839 regulatory sandbox using exceptions to specified general law and  
840 waivers of the corresponding rule requirements under defined  
841 conditions. The creation of a supervised, flexible regulatory

576-04569-20

20201870c3

842 sandbox provides a welcoming business environment for technology  
843 innovators and may lead to significant business growth.

844 (3) DEFINITIONS.—As used in this section, the term:

845 (a) "Business entity" means a domestic corporation or other  
846 organized domestic entity with a physical presence, other than  
847 that of a registered office or agent or virtual mailbox, in this  
848 state.

849 (b) "Commission" means the Financial Services Commission.

850 (c) "Consumer" means a person in this state, whether a  
851 natural person or a business organization, who purchases, uses,  
852 receives, or enters into an agreement to purchase, use, or  
853 receive an innovative financial product or service made  
854 available through the Financial Technology Sandbox.

855 (d) "Control person" means an individual, a partnership, a  
856 corporation, a trust, or other organization that possesses the  
857 power, directly or indirectly, to direct the management or  
858 policies of a company, whether through ownership of securities,  
859 by contract, or through other means. A person is presumed to  
860 control a company if, with respect to a particular company, that  
861 person:

862 1. Is a director, a general partner, or an officer  
863 exercising executive responsibility or having similar status or  
864 functions;

865 2. Directly or indirectly may vote 10 percent or more of a  
866 class of a voting security or sell or direct the sale of 10  
867 percent or more of a class of voting securities; or

868 3. In the case of a partnership, may receive upon  
869 dissolution or has contributed 10 percent or more of the  
870 capital.

576-04569-20

20201870c3

871 (e) "Corresponding rule requirements" means the commission  
872 rules, or portions thereof, which implement the general laws  
873 enumerated in paragraph (4) (a).

874 (f) "Financial product or service" means a product or  
875 service related to a consumer finance loan, as defined in s.  
876 516.01, or a money transmitter or payment instrument seller, as  
877 those terms are defined in s. 560.103, including mediums of  
878 exchange that are in electronic or digital form, which is  
879 subject to the general laws enumerated in paragraph (4) (a) and  
880 corresponding rule requirements and which is under the  
881 jurisdiction of the office.

882 (g) "Financial Technology Sandbox" means the program  
883 created by this section which allows a licensee to make an  
884 innovative financial product or service available to consumers  
885 during a sandbox period through exceptions to general laws and  
886 waivers of corresponding rule requirements.

887 (h) "Innovative" means new or emerging technology, or new  
888 uses of existing technology, which provide a product, service,  
889 business model, or delivery mechanism to the public and which  
890 are not known to have a comparable offering in this state  
891 outside the Financial Technology Sandbox.

892 (i) "Licensee" means a business entity that has been  
893 approved by the office to participate in the Financial  
894 Technology Sandbox.

895 (j) "Office" means, unless the context clearly indicates  
896 otherwise, the Office of Financial Regulation.

897 (k) "Sandbox period" means the initial 24-month period in  
898 which the office has authorized a licensee to make an innovative  
899 financial product or service available to consumers, and any

576-04569-20

20201870c3

900 extension granted pursuant to subsection (7).

901 (4) EXCEPTIONS TO GENERAL LAW AND WAIVERS OF RULE  
902 REQUIREMENTS.—

903 (a) Notwithstanding any other law, upon approval of a  
904 Financial Technology Sandbox application, the following  
905 provisions and corresponding rule requirements are not  
906 applicable to the licensee during the sandbox period:

907 1. Section 516.03(1), except for the application fee, the  
908 investigation fee, the requirement to provide the social  
909 security numbers of control persons, evidence of liquid assets  
910 of at least \$25,000, and the office's authority to investigate  
911 the applicant's background. The office may prorate the license  
912 renewal fee for an extension granted under subsection (7).

913 2. Section 516.05(1) and (2), except that the office shall  
914 investigate the applicant's background.

915 3. Section 560.109, only to the extent that the section  
916 requires the office to examine a licensee at least once every 5  
917 years.

918 4. Section 560.118(2).

919 5. Section 560.125(1), only to the extent that subsection  
920 would prohibit a licensee from engaging in the business of a  
921 money transmitter or payment instrument seller during the  
922 sandbox period.

923 6. Section 560.125(2), only to the extent that subsection  
924 would prohibit a licensee from appointing an authorized vendor  
925 during the sandbox period. Any authorized vendor of such a  
926 licensee during the sandbox period remains liable to the holder  
927 or remitter.

928 7. Section 560.128.



576-04569-20

20201870c3

929 8. Section 560.141, except for s. 560.141(1)(a)1., 3., 7.-  
930 10. and (b), (c), and (d).

931 9. Section 560.142(1) and (2), except that the office may  
932 prorate, but may not entirely eliminate, the license renewal  
933 fees in s. 560.143 for an extension granted under subsection  
934 (7).

935 10. Section 560.143(2), only to the extent necessary for  
936 proration of the renewal fee under subparagraph 9.

937 11. Section 560.204(1), only to the extent that subsection  
938 would prohibit a licensee from engaging in, or advertising that  
939 it engages in, the selling or issuing of payment instruments or  
940 in the activity of a money transmitter during the sandbox  
941 period.

942 12. Section 560.205(2).

943 13. Section 560.208(2).

944 14. Section 560.209, only to the extent that the office may  
945 modify, but may not entirely eliminate, the net worth, corporate  
946 surety bond, and collateral deposit amounts required under that  
947 section. The modified amounts must be in such lower amounts that  
948 the office determines to be commensurate with the factors under  
949 paragraph (5)(c) and the maximum number of consumers authorized  
950 to receive the financial product or service under this section.

951 (b) The office may approve a Financial Technology Sandbox  
952 application if one or more of the general laws enumerated in  
953 paragraph (a) currently prevent the innovative financial product  
954 or service from being made available to consumers and if all  
955 other requirements of this section are met.

956 (c) A licensee may conduct business through electronic  
957 means, including through the Internet or a software application.

576-04569-20

20201870c3

958 (5) FINANCIAL TECHNOLOGY SANDBOX APPLICATION; STANDARDS FOR  
959 APPROVAL.—

960 (a) Before filing an application for licensure under this  
961 section, a substantially affected person may seek a declaratory  
962 statement pursuant to s. 120.565 regarding the applicability of  
963 a statute, a rule, or an agency order to the petitioner's  
964 particular set of circumstances or a variance or waiver of a  
965 rule pursuant to s. 120.542.

966 (b) Before making an innovative financial product or  
967 service available to consumers in the Financial Technology  
968 Sandbox, a business entity must file with the office an  
969 application for licensure under the Financial Technology  
970 Sandbox. The commission shall, by rule, prescribe the form and  
971 manner of the application and how the office will evaluate and  
972 apply each of the factors specified in paragraph (c).

973 1. The application must specify each general law enumerated  
974 in paragraph (4) (a) which currently prevents the innovative  
975 financial product or service from being made available to  
976 consumers and the reasons why those provisions of general law  
977 prevent the innovative financial product or service from being  
978 made available to consumers.

979 2. The application must contain sufficient information for  
980 the office to evaluate the factors specified in paragraph (c).

981 3. An application submitted on behalf of a business entity  
982 must include evidence that the business entity has authorized  
983 the person to submit the application on behalf of the business  
984 entity intending to make an innovative financial product or  
985 service available to consumers.

986 4. The application must specify the maximum number of

576-04569-20

20201870c3

987 consumers, which may not exceed the number of consumers  
988 specified in paragraph (f), to whom the applicant proposes to  
989 provide the innovative financial product or service.

990 5. The application must include a proposed draft of the  
991 statement or statements meeting the requirements of paragraph  
992 (6) (b) which the applicant proposes to provide to consumers.

993 (c) The office shall approve or deny in writing a Financial  
994 Technology Sandbox application within 60 days after receiving  
995 the completed application. The office and the applicant may  
996 jointly agree to extend the time beyond 60 days. Consistent with  
997 this section, the office may impose conditions on any approval.  
998 In deciding whether to approve or deny an application for  
999 licensure, the office must consider each of the following:

1000 1. The nature of the innovative financial product or  
1001 service proposed to be made available to consumers in the  
1002 Financial Technology Sandbox, including all relevant technical  
1003 details.

1004 2. The potential risk to consumers and the methods that  
1005 will be used to protect consumers and resolve complaints during  
1006 the sandbox period.

1007 3. The business plan proposed by the applicant, including  
1008 company information, market analysis, and financial projections  
1009 or pro forma financial statements, and evidence of the financial  
1010 viability of the applicant.

1011 4. Whether the applicant has the necessary personnel,  
1012 adequate financial and technical expertise, and a sufficient  
1013 plan to test, monitor, and assess the innovative financial  
1014 product or service.

1015 5. Whether any control person of the applicant, regardless

576-04569-20

20201870c3

1016 of adjudication, has pled no contest to, has been convicted or  
1017 found guilty of, or is currently under investigation for fraud,  
1018 a state or federal securities violation, a property-based  
1019 offense, or a crime involving moral turpitude or dishonest  
1020 dealing, in which case the application to the Financial  
1021 Technology Sandbox must be denied.

1022 6. A copy of the disclosures that will be provided to  
1023 consumers under paragraph (6) (b).

1024 7. The financial responsibility of the applicant and any  
1025 control person, including whether the applicant or any control  
1026 person has a history of unpaid liens, unpaid judgments, or other  
1027 general history of nonpayment of legal debts, including, but not  
1028 limited to, having been the subject of a petition for bankruptcy  
1029 under the United States Bankruptcy Code within the past 7  
1030 calendar years.

1031 8. Any other factor that the office determines to be  
1032 relevant.

1033 (d) The office may not approve an application if:

1034 1. The applicant had a prior Financial Technology Sandbox  
1035 application that was approved and that related to a  
1036 substantially similar financial product or service;

1037 2. Any control person of the applicant was substantially  
1038 involved in the development, operation, or management with  
1039 another Financial Technology Sandbox applicant whose application  
1040 was approved and whose application related to a substantially  
1041 similar financial product or service; or

1042 3. The applicant or any control person has failed to  
1043 affirmatively demonstrate financial responsibility.

1044 (e) Upon approval of an application, the office shall

576-04569-20

20201870c3

1045 notify the licensee that the licensee is exempt from the  
1046 provisions of general law enumerated in paragraph (4)(a) and the  
1047 corresponding rule requirements during the sandbox period. The  
1048 office shall post on its website notice of the approval of the  
1049 application, a summary of the innovative financial product or  
1050 service, and the contact information of the licensee.

1051 (f) The office, on a case-by-case basis, shall specify the  
1052 maximum number of consumers authorized to receive an innovative  
1053 financial product or service, after consultation with the  
1054 Financial Technology Sandbox applicant. The office may not  
1055 authorize more than 15,000 consumers to receive the financial  
1056 product or service until the licensee has filed the first report  
1057 required under subsection (8). After the filing of that report,  
1058 if the licensee demonstrates adequate financial capitalization,  
1059 risk management processes, and management oversight, the office  
1060 may authorize up to 25,000 consumers to receive the financial  
1061 product or service.

1062 (g) A licensee has a continuing obligation to promptly  
1063 inform the office of any material change to the information  
1064 provided under paragraph (b).

1065 (6) OPERATION OF THE FINANCIAL TECHNOLOGY SANDBOX.—

1066 (a) A licensee may make an innovative financial product or  
1067 service available to consumers during the sandbox period.

1068 (b)1. Before a consumer purchases, uses, receives, or  
1069 enters into an agreement to purchase, use, or receive an  
1070 innovative financial product or service through the Financial  
1071 Technology Sandbox, the licensee must provide a written  
1072 statement of all of the following to the consumer:

1073 a. The name and contact information of the licensee.

576-04569-20

20201870c3

1074 b. That the financial product or service has been  
1075 authorized to be made available to consumers for a temporary  
1076 period by the office, under the laws of this state.

1077 c. That the state does not endorse the financial product or  
1078 service.

1079 d. That the financial product or service is undergoing  
1080 testing, may not function as intended, and may entail financial  
1081 risk.

1082 e. That the licensee is not immune from civil liability for  
1083 any losses or damages caused by the financial product or  
1084 service.

1085 f. The expected end date of the sandbox period.

1086 g. The contact information for the office and notification  
1087 that suspected legal violations, complaints, or other comments  
1088 related to the financial product or service may be submitted to  
1089 the office.

1090 h. Any other statements or disclosures required by rule of  
1091 the commission which are necessary to further the purposes of  
1092 this section.

1093 2. The written statement under subparagraph 1. must contain  
1094 an acknowledgment from the consumer, which must be retained for  
1095 the duration of the sandbox period by the licensee.

1096 (c) The office may enter into an agreement with a state,  
1097 federal, or foreign regulatory agency to allow licensees under  
1098 the Financial Technology Sandbox to make their products or  
1099 services available in other jurisdictions. The commission shall  
1100 adopt rules to implement this paragraph.

1101 (d) The office may examine the records of a licensee at any  
1102 time, with or without prior notice.

576-04569-20

20201870c3

1103 (7) EXTENSIONS AND CONCLUSION OF SANDBOX PERIOD.—

1104 (a) A licensee may apply for one extension of the initial  
1105 24-month sandbox period for 12 additional months for a purpose  
1106 specified in subparagraph (b)1. or subparagraph (b)2. A complete  
1107 application for an extension must be filed with the office at  
1108 least 90 days before the conclusion of the initial sandbox  
1109 period. The office shall approve or deny the application for  
1110 extension in writing at least 35 days before the conclusion of  
1111 the initial sandbox period. In determining whether to approve or  
1112 deny an application for extension of the sandbox period, the  
1113 office must, at a minimum, consider the current status of the  
1114 factors previously considered under paragraph (5)(c).

1115 (b) An application for an extension under paragraph (a)  
1116 must cite one of the following reasons as the basis for the  
1117 application and must provide all relevant supporting  
1118 information:

1119 1. Amendments to general law or rules are necessary to  
1120 offer the innovative financial product or service in this state  
1121 permanently.

1122 2. An application for a license that is required in order  
1123 to offer the innovative financial product or service in this  
1124 state permanently has been filed with the office and approval is  
1125 pending.

1126 (c) At least 30 days before the conclusion of the initial  
1127 24-month sandbox period or the extension, whichever is later, a  
1128 licensee shall provide written notification to consumers  
1129 regarding the conclusion of the initial sandbox period or the  
1130 extension and may not make the financial product or service  
1131 available to any new consumers after the conclusion of the

576-04569-20

20201870c3

1132 initial sandbox period or the extension, whichever is later,  
1133 until legal authority outside of the Financial Technology  
1134 Sandbox exists for the licensee to make the financial product or  
1135 service available to consumers. After the conclusion of the  
1136 sandbox period or the extension, whichever is later, the  
1137 business entity formerly licensed under the Financial Technology  
1138 Sandbox may:

1139 1. Collect and receive money owed to the business entity or  
1140 pay money owed by the business entity, based on agreements with  
1141 consumers made before the conclusion of the sandbox period or  
1142 the extension.

1143 2. Take necessary legal action.

1144 3. Take other actions authorized by commission rule which  
1145 are not inconsistent with this section.

1146 (8) REPORT.—A licensee shall submit a report to the office  
1147 twice a year as prescribed by commission rule. The report must,  
1148 at a minimum, include financial reports and the number of  
1149 consumers who have received the financial product or service.

1150 (9) CONSTRUCTION.—A business entity whose Financial  
1151 Technology Sandbox application is approved under this section:

1152 (a) Is licensed under chapter 516, chapter 560, or both  
1153 chapters 516 and 560, as applicable to the business entity's  
1154 activities.

1155 (b) Is subject to any provision of chapter 516 or chapter  
1156 560 not specifically excepted under paragraph (4) (a), as  
1157 applicable to the business entity's activities, and must comply  
1158 with such provisions.

1159 (c) May not engage in activities authorized under part III  
1160 of chapter 560, notwithstanding s. 560.204(2).



576-04569-20

20201870c3

1161 (10) VIOLATIONS AND PENALTIES.—

1162 (a) A licensee who makes an innovative financial product or  
1163 service available to consumers in the Financial Technology  
1164 Sandbox remains subject to:

1165 1. Civil damages for acts and omissions arising from or  
1166 related to any innovative financial product or services provided  
1167 or made available by the licensee or relating to this section.

1168 2. All criminal and consumer protection laws and any other  
1169 statute not specifically excepted under paragraph (4) (a).

1170 (b)1. The office may, by order, revoke or suspend a  
1171 licensee's approval to participate in the Financial Technology  
1172 Sandbox if:

1173 a. The licensee has violated or refused to comply with this  
1174 section, any statute not specifically excepted under paragraph  
1175 (4) (a), a rule of the commission that has not been waived, an  
1176 order of the office, or a condition placed by the office on the  
1177 approval of the licensee's Financial Technology Sandbox  
1178 application;

1179 b. A fact or condition exists that, if it had existed or  
1180 become known at the time that the Financial Technology Sandbox  
1181 application was pending, would have warranted denial of the  
1182 application or the imposition of material conditions;

1183 c. A material error, false statement, misrepresentation, or  
1184 material omission was made in the Financial Technology Sandbox  
1185 application; or

1186 d. After consultation with the licensee, the office  
1187 determines that continued testing of the innovative financial  
1188 product or service would:

1189 (I) Be likely to harm consumers; or

576-04569-20

20201870c3

1190 (II) No longer serve the purposes of this section because  
1191 of the financial or operational failure of the financial product  
1192 or service.

1193 2. Written notice of a revocation or suspension order made  
1194 under subparagraph 1. must be served using any means authorized  
1195 by law. If the notice relates to a suspension, the notice must  
1196 include any condition or remedial action that the licensee must  
1197 complete before the office lifts the suspension.

1198 (c) The office may refer any suspected violation of law to  
1199 an appropriate state or federal agency for investigation,  
1200 prosecution, civil penalties, and other appropriate enforcement  
1201 action.

1202 (d) If service of process on a licensee is not feasible,  
1203 service on the office is deemed service on the licensee.

1204 (11) RULES AND ORDERS.-

1205 (a) The commission shall adopt rules to administer this  
1206 section before approving any application under this section.

1207 (b) The office may issue all necessary orders to enforce  
1208 this section and may enforce these orders in accordance with  
1209 chapter 120 or in any court of competent jurisdiction. These  
1210 orders include, but are not limited to, orders for payment of  
1211 restitution for harm suffered by consumers as a result of an  
1212 innovative financial product or service.

1213 Section 13. For the 2020-2021 fiscal year, the sum of  
1214 \$50,000 in nonrecurring funds is appropriated from the  
1215 Administrative Trust Fund to the Office of Financial Regulation  
1216 to implement s. 559.952, Florida Statutes, as created by this  
1217 act.

1218 Section 14. The creation of s. 559.952, Florida Statutes,

576-04569-20

20201870c3

1219 and the appropriation to implement s. 559.952, Florida Statutes,  
1220 by this act shall take effect only if SB 1872 or similar  
1221 legislation takes effect and if such legislation is adopted in  
1222 the same legislative session or an extension thereof and becomes  
1223 a law.

1224       Section 15. Except as otherwise expressly provided in this  
1225 act, this act shall take effect July 1, 2020.