

1                   A bill to be entitled  
2           An act relating to technology innovation; amending s.  
3           20.22, F.S.; renaming the Division of State Technology  
4           within the Department of Management Services; adding  
5           the Florida Digital Service to the department;  
6           amending s. 282.0041, F.S.; providing definitions;  
7           amending s. 282.0051, F.S.; establishing the Florida  
8           Digital Service within the department; transferring  
9           specified powers, duties, and functions; providing  
10          appointments and duties of the state chief information  
11          officer and chief data officer of the Florida Digital  
12          Service; requiring the Florida Digital Service to  
13          develop a comprehensive enterprise architecture;  
14          providing requirements for such enterprise  
15          architecture; providing powers and duties of the  
16          Florida Digital Service; providing powers and duties  
17          of the department under certain circumstances;  
18          providing requirements for the procurement terms of  
19          contract under certain circumstances; prohibiting  
20          costs to the enterprise and law enforcement for using  
21          services provided by credential service providers  
22          under certain circumstances; providing requirements  
23          for agreements between the department and credential  
24          service providers, electronic credential providers,  
25          and qualified entities under certain circumstances;

26 providing disposition of revenues generated from such  
 27 agreements under certain circumstances; providing  
 28 report requirements; providing rulemaking authority;  
 29 amending s. 282.00515, F.S.; deleting provisions  
 30 relating to specified duties and powers of the  
 31 Department of Legal Affairs, the Department of  
 32 Financial Services, and the Department of Agriculture  
 33 and Consumer Services; establishing the Enterprise  
 34 Architecture Advisory Council; requiring the council  
 35 to comply with specified requirements; providing  
 36 membership and meeting requirements and duties of the  
 37 council; amending ss. 282.318, 287.0591, 365.171,  
 38 365.172, 365.173, and 943.0415, F.S.; conforming  
 39 provisions to changes made by the act; creating s.  
 40 560.214, F.S.; providing a short title; creating the  
 41 Financial Technology Sandbox; providing definitions;  
 42 providing certain waivers of requirements to specified  
 43 persons under certain circumstances; requiring an  
 44 application for the program for persons who want to  
 45 make innovative financial products or services  
 46 available to consumers; providing application  
 47 requirements; providing standards for application  
 48 approval or refusal; requiring the Office of Financial  
 49 Regulation to perform certain actions upon approval of  
 50 an application; providing operation of the sandbox;

51 providing limitations on the number of consumers of  
52 innovative financial products or services; authorizing  
53 the office to enter into agreement with certain  
54 regulatory agencies for specified purposes; providing  
55 recordkeeping requirements; providing rulemaking  
56 authority; authorizing the office to examine specified  
57 records; providing extension and conclusion of the  
58 sandbox period; requiring written notification to  
59 consumers at the end of an extension or conclusion of  
60 the sandbox period; providing acts that persons who  
61 make innovative financial products or services  
62 available to consumers may and may not engage in at  
63 the end of an extension or conclusion of the sandbox  
64 period; requiring such persons to submit a report;  
65 providing construction; providing that such persons  
66 are not immune from civil damages and are subject to  
67 criminal and consumer protection laws; providing  
68 penalties; providing service of process; requiring the  
69 Financial Services Commission to adopt rules;  
70 authorizing the office to issue certain orders and to  
71 enforce them under ch. 120, F.S., or in court;  
72 authorizing the office to issue and enforce orders for  
73 payment of restitution; providing an appropriation;  
74 providing effective dates.

75

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

77

78 Section 1. Subsection (2) of section 20.22, Florida  
79 Statutes, is amended to read:

80 20.22 Department of Management Services.—There is created  
81 a Department of Management Services.

82 (2) ~~The following divisions and programs within the~~  
83 Department of Management Services shall consist of the following  
84 ~~are established:~~

85 (a) The Facilities Program.

86 (b) The Division of Telecommunications State Technology,  
87 ~~the director of which is appointed by the secretary of the~~  
88 ~~department and shall serve as the state chief information~~  
89 ~~officer. The state chief information officer must be a proven,~~  
90 ~~effective administrator who must have at least 10 years of~~  
91 ~~executive-level experience in the public or private sector,~~  
92 ~~preferably with experience in the development of information~~  
93 ~~technology strategic planning and the development and~~  
94 ~~implementation of fiscal and substantive information technology~~  
95 ~~policy and standards.~~

96 (c) The Workforce Program.

97 (d)1. The Support Program.

98 2. The Federal Property Assistance Program.

99 (e) The Administration Program.

100 (f) The Division of Administrative Hearings.

- 101 (g) The Division of Retirement.
- 102 (h) The Division of State Group Insurance.
- 103 (i) The Florida Digital Service.

104 Section 2. Section 282.0041, Florida Statutes, is amended  
 105 to read:

106 282.0041 Definitions.—As used in this chapter, the term:

107 (1) "Agency assessment" means the amount each customer  
 108 entity must pay annually for services from the Department of  
 109 Management Services and includes administrative and data center  
 110 services costs.

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

113 (3) "Breach" has the same meaning as provided in s.  
 114 501.171.

115 (4) "Business continuity plan" means a collection of  
 116 procedures and information designed to keep an agency's critical  
 117 operations running during a period of displacement or  
 118 interruption of normal operations.

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

122 (6) "Computing facility" or "agency computing facility"  
 123 means agency space containing fewer than a total of 10 physical  
 124 or logical servers, but excluding single, logical-server  
 125 installations that exclusively perform a utility function such

126 as file and print servers.

127 (7) "Credential service provider" means a provider  
128 competitively procured by the department to supply secure  
129 identity management and verification services based on open  
130 standards to qualified entities.

131 (8)~~(7)~~ "Customer entity" means an entity that obtains  
132 services from the Department of Management Services.

133 (9)~~(8)~~ "Data" means a subset of structured information in  
134 a format that allows such information to be electronically  
135 retrieved and transmitted.

136 (10) "Data-call" means an electronic transaction with the  
137 credential service provider that verifies the authenticity of a  
138 digital identity by querying enterprise data.

139 (11)~~(9)~~ "Department" means the Department of Management  
140 Services.

141 (12)~~(10)~~ "Disaster recovery" means the process, policies,  
142 procedures, and infrastructure related to preparing for and  
143 implementing recovery or continuation of an agency's vital  
144 technology infrastructure after a natural or human-induced  
145 disaster.

146 (13) "Electronic" means technology having electrical,  
147 digital, magnetic, wireless, optical, electromagnetic, or  
148 similar capabilities.

149 (14) "Electronic credential" means an electronic  
150 representation of a physical driver license or identification

151 card that is viewable in an electronic format and is capable of  
152 being verified and authenticated.

153 (15) "Electronic credential provider" means a qualified  
154 entity contracted with the department to provide electronic  
155 credentials to eligible driver license or identification card  
156 holders.

157 (16) "Enterprise" means the collection of state agencies.  
158 The term includes the Department of Legal Affairs, the  
159 Department of Agriculture and Consumer Services, the Department  
160 of Financial Services, and the judicial branch.

161 (17) "Enterprise architecture" means a comprehensive  
162 operational framework that contemplates the needs and assets of  
163 the enterprise to support interoperability across state  
164 government.

165 (18)~~(11)~~ "Enterprise information technology service" means  
166 an information technology service that is used in all agencies  
167 or a subset of agencies and is established in law to be  
168 designed, delivered, and managed at the enterprise level.

169 (19)~~(12)~~ "Event" means an observable occurrence in a  
170 system or network.

171 (20)~~(13)~~ "Incident" means a violation or imminent threat  
172 of violation, whether such violation is accidental or  
173 deliberate, of information technology resources, security,  
174 policies, or practices. An imminent threat of violation refers  
175 to a situation in which the state agency has a factual basis for

176 believing that a specific incident is about to occur.

177 (21)~~(14)~~ "Information technology" means equipment,  
178 hardware, software, firmware, programs, systems, networks,  
179 infrastructure, media, and related material used to  
180 automatically, electronically, and wirelessly collect, receive,  
181 access, transmit, display, store, record, retrieve, analyze,  
182 evaluate, process, classify, manipulate, manage, assimilate,  
183 control, communicate, exchange, convert, converge, interface,  
184 switch, or disseminate information of any kind or form.

185 (22)~~(15)~~ "Information technology policy" means a definite  
186 course or method of action selected from among one or more  
187 alternatives that guide and determine present and future  
188 decisions.

189 (23)~~(16)~~ "Information technology resources" has the same  
190 meaning as provided in s. 119.011.

191 (24)~~(17)~~ "Information technology security" means the  
192 protection afforded to an automated information system in order  
193 to attain the applicable objectives of preserving the integrity,  
194 availability, and confidentiality of data, information, and  
195 information technology resources.

196 (25) "Interoperability" means the technical ability to  
197 share and use data across and throughout the enterprise.

198 (26)~~(18)~~ "Open data" means data collected or created by a  
199 state agency and structured in a way that enables the data to be  
200 fully discoverable and usable by the public. The term does not



201 include data that are restricted from public distribution based  
202 on federal or state privacy, confidentiality, and security laws  
203 and regulations or data for which a state agency is statutorily  
204 authorized to assess a fee for its distribution.

205 (27)~~(19)~~ "Performance metrics" means the measures of an  
206 organization's activities and performance.

207 (28)~~(20)~~ "Project" means an endeavor that has a defined  
208 start and end point; is undertaken to create or modify a unique  
209 product, service, or result; and has specific objectives that,  
210 when attained, signify completion.

211 (29)~~(21)~~ "Project oversight" means an independent review  
212 and analysis of an information technology project that provides  
213 information on the project's scope, completion timeframes, and  
214 budget and that identifies and quantifies issues or risks  
215 affecting the successful and timely completion of the project.

216 (30) "Qualified entity" means a public or private entity  
217 or individual that enters into a binding agreement with the  
218 department, meets usage criteria, agrees to terms and  
219 conditions, and is subsequently and prescriptively authorized by  
220 the department to access data under the terms of that agreement.

221 (31)~~(22)~~ "Risk assessment" means the process of  
222 identifying security risks, determining their magnitude, and  
223 identifying areas needing safeguards.

224 (32)~~(23)~~ "Service level" means the key performance  
225 indicators (KPI) of an organization or service which must be

226 regularly performed, monitored, and achieved.

227 (33)~~(24)~~ "Service-level agreement" means a written  
 228 contract between the Department of Management Services and a  
 229 customer entity which specifies the scope of services provided,  
 230 service level, the duration of the agreement, the responsible  
 231 parties, and service costs. A service-level agreement is not a  
 232 rule pursuant to chapter 120.

233 (34)~~(25)~~ "Stakeholder" means a person, group,  
 234 organization, or state agency involved in or affected by a  
 235 course of action.

236 (35)~~(26)~~ "Standards" means required practices, controls,  
 237 components, or configurations established by an authority.

238 (36)~~(27)~~ "State agency" means any official, officer,  
 239 commission, board, authority, council, committee, or department  
 240 of the executive branch of state government; the Justice  
 241 Administrative Commission; and the Public Service Commission.  
 242 The term does not include university boards of trustees or state  
 243 universities. As used in part I of this chapter, except as  
 244 otherwise specifically provided, the term does not include the  
 245 Department of Legal Affairs, the Department of Agriculture and  
 246 Consumer Services, or the Department of Financial Services.

247 (37)~~(28)~~ "SUNCOM Network" means the state enterprise  
 248 telecommunications system that provides all methods of  
 249 electronic or optical telecommunications beyond a single  
 250 building or contiguous building complex and used by entities

251 authorized as network users under this part.

252 (38)~~(29)~~ "Telecommunications" means the science and  
 253 technology of communication at a distance, including electronic  
 254 systems used in the transmission or reception of information.

255 (39)~~(30)~~ "Threat" means any circumstance or event that has  
 256 the potential to adversely impact a state agency's operations or  
 257 assets through an information system via unauthorized access,  
 258 destruction, disclosure, or modification of information or  
 259 denial of service.

260 (40)~~(31)~~ "Variance" means a calculated value that  
 261 illustrates how far positive or negative a projection has  
 262 deviated when measured against documented estimates within a  
 263 project plan.

264 Section 3. Section 282.0051, Florida Statutes, is amended  
 265 to read:

266 282.0051 Florida Digital Service ~~Department of Management~~  
 267 ~~Services; powers, duties, and functions.~~ There is established  
 268 the Florida Digital Service within the department to create  
 269 innovative solutions that securely modernize state government,  
 270 achieve value through digital transformation and  
 271 interoperability, and fully support the cloud-first policy as  
 272 specified in s. 282.206.

273 (1) The Florida Digital Service ~~department~~ shall have the  
 274 following powers, duties, and functions:

275 (a)~~(1)~~ Develop and publish information technology policy

276 | for the management of the state's information technology  
277 | resources.

278 |        (b)-(2) Establish and publish information technology  
279 | architecture standards to provide for the most efficient use of  
280 | ~~the state's~~ information technology resources and to ensure  
281 | compatibility and alignment with the needs of state agencies.  
282 | The Florida Digital Service ~~department~~ shall assist state  
283 | agencies in complying with the standards.

284 |        (c)-(3) Establish project management and oversight  
285 | standards with which state agencies must comply when  
286 | implementing projects that have an information technology  
287 | component ~~projects~~. The Florida Digital Service ~~department~~ shall  
288 | provide training opportunities to state agencies to assist in  
289 | the adoption of the project management and oversight standards.  
290 | To support data-driven decisionmaking, the standards must  
291 | include, but are not limited to:

292 |        1.(a) Performance measurements and metrics that  
293 | objectively reflect the status of a project with an information  
294 | technology component ~~project~~ based on a defined and documented  
295 | project scope, cost, and schedule.

296 |        2.(b) Methodologies for calculating acceptable variances  
297 | in the projected versus actual scope, schedule, or cost of a  
298 | project with an information technology component ~~project~~.

299 |        3.(c) Reporting requirements, including requirements  
300 | designed to alert all defined stakeholders that a project with

301 an information technology component ~~project~~ has exceeded  
 302 acceptable variances defined and documented in a project plan.  
 303 4.~~(d)~~ Content, format, and frequency of project updates.  
 304 (d)~~(4)~~ Perform project oversight on all state agency  
 305 ~~information technology~~ projects that have an information  
 306 technology component with a total project cost ~~costs~~ of \$10  
 307 million or more and that are funded in the General  
 308 Appropriations Act or any other law. The Florida Digital Service  
 309 ~~department~~ shall report at least quarterly to the Executive  
 310 Office of the Governor, the President of the Senate, and the  
 311 Speaker of the House of Representatives on any project with an  
 312 information technology component ~~project~~ that the Florida  
 313 Digital Service ~~department~~ identifies as high-risk due to the  
 314 project exceeding acceptable variance ranges defined and  
 315 documented in a project plan. The report must include a risk  
 316 assessment, including fiscal risks, associated with proceeding  
 317 to the next stage of the project, and a recommendation for  
 318 corrective actions required, including suspension or termination  
 319 of the project.  
 320 (e)~~(5)~~ Identify opportunities for standardization and  
 321 consolidation of information technology services that support  
 322 interoperability and the cloud-first policy as specified in s.  
 323 282.206, business functions and operations, including  
 324 administrative functions such as purchasing, accounting and  
 325 reporting, cash management, and personnel, and that are common

326 across state agencies. The Florida Digital Service ~~department~~  
327 shall biennially on April 1 provide recommendations for  
328 standardization and consolidation to the Executive Office of the  
329 Governor, the President of the Senate, and the Speaker of the  
330 House of Representatives.

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

335 (g) ~~(7)~~ Develop standards for information technology  
336 reports and updates, including, but not limited to, operational  
337 work plans, project spend plans, and project status reports, for  
338 use by state agencies.

339 (h) ~~(8)~~ Upon request, assist state agencies in the  
340 development of information technology-related legislative budget  
341 requests.

342 (i) ~~(9)~~ Conduct annual assessments of state agencies to  
343 determine compliance with all information technology standards  
344 and guidelines developed and published by the Florida Digital  
345 Service ~~department~~ and provide results of the assessments to the  
346 Executive Office of the Governor, the President of the Senate,  
347 and the Speaker of the House of Representatives.

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

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

354        ~~2.(b)~~ Developing and implementing cost-recovery or other  
355 payment mechanisms that recover the full direct and indirect  
356 cost of services through charges to applicable customer  
357 entities. Such cost-recovery or other payment mechanisms must  
358 comply with applicable state and federal regulations concerning  
359 distribution and use of funds and must ensure that, for any  
360 fiscal year, no service or customer entity subsidizes another  
361 service or customer entity.

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

369        ~~a.1.~~ Implementing a consolidated administrative support  
370 structure responsible for providing financial management,  
371 procurement, transactions involving real or personal property,  
372 human resources, and operational support.

373        ~~b.2.~~ Implementing an annual reconciliation process to  
374 ensure that each customer entity is paying for the full direct  
375 and indirect cost of each service as determined by the customer

376 entity's use of each service.

377 ~~c.3.~~ Providing rebates that may be credited against future  
378 billings to customer entities when revenues exceed costs.

379 ~~d.4.~~ Requiring customer entities to validate that  
380 sufficient funds exist in the appropriate data processing  
381 appropriation category or will be transferred into the  
382 appropriate data processing appropriation category before  
383 implementation of a customer entity's request for a change in  
384 the type or level of service provided, if such change results in  
385 a net increase to the customer entity's cost for that fiscal  
386 year.

387 ~~e.5.~~ By November 15 of each year, providing to the Office  
388 of Policy and Budget in the Executive Office of the Governor and  
389 to the chairs of the legislative appropriations committees the  
390 projected costs of providing data center services for the  
391 following fiscal year.

392 ~~f.6.~~ Providing a plan for consideration by the Legislative  
393 Budget Commission if the cost of a service is increased for a  
394 reason other than a customer entity's request made pursuant to  
395 sub-subparagraph d. ~~subparagraph 4.~~ Such a plan is required only  
396 if the service cost increase results in a net increase to a  
397 customer entity for that fiscal year.

398 ~~g.7.~~ Standardizing and consolidating procurement and  
399 contracting practices.

400 ~~4.(d)~~ In collaboration with the Department of Law



401 Enforcement, developing and implementing a process for  
402 detecting, reporting, and responding to information technology  
403 security incidents, breaches, and threats.

404 5.~~(e)~~ Adopting rules relating to the operation of the  
405 state data center, including, but not limited to, budgeting and  
406 accounting procedures, cost-recovery or other payment  
407 methodologies, and operating procedures.

408 ~~(f) Conducting an annual market analysis to determine~~  
409 ~~whether the state's approach to the provision of data center~~  
410 ~~services is the most effective and cost-efficient manner by~~  
411 ~~which its customer entities can acquire such services, based on~~  
412 ~~federal, state, and local government trends; best practices in~~  
413 ~~service provision; and the acquisition of new and emerging~~  
414 ~~technologies. The results of the market analysis shall assist~~  
415 ~~the state data center in making adjustments to its data center~~  
416 ~~service offerings.~~

417 (k)~~(11)~~ Recommend other information technology services  
418 that should be designed, delivered, and managed as enterprise  
419 information technology services. Recommendations must include  
420 the identification of existing information technology resources  
421 associated with the services, if existing services must be  
422 transferred as a result of being delivered and managed as  
423 enterprise information technology services.

424 (l)~~(12)~~ In consultation with state agencies, propose a  
425 methodology and approach for identifying and collecting both

426 current and planned information technology expenditure data at  
427 the state agency level.

428 (m) 1. (13) (a) Notwithstanding any other law, provide  
429 project oversight on any project with an information technology  
430 component ~~project~~ of the Department of Financial Services, the  
431 Department of Legal Affairs, and the Department of Agriculture  
432 and Consumer Services which has a total project cost of \$25  
433 million or more and which impacts one or more other agencies.  
434 Such projects with an information technology component ~~projects~~  
435 must also comply with the applicable information technology  
436 architecture, project management and oversight, and reporting  
437 standards established by the Florida Digital Service ~~department~~.

438 2. (b) When performing the project oversight function  
439 specified in subparagraph 1. paragraph (a), report at least  
440 quarterly to the Executive Office of the Governor, the President  
441 of the Senate, and the Speaker of the House of Representatives  
442 on any project with an information technology component ~~project~~  
443 that the Florida Digital Service ~~department~~ identifies as high-  
444 risk due to the project exceeding acceptable variance ranges  
445 defined and documented in the project plan. The report shall  
446 include a risk assessment, including fiscal risks, associated  
447 with proceeding to the next stage of the project and a  
448 recommendation for corrective actions required, including  
449 suspension or termination of the project.

450 (n) (14) If a project with an information technology

451 component ~~project~~ implemented by a state agency must be  
452 connected to or otherwise accommodated by an information  
453 technology system administered by the Department of Financial  
454 Services, the Department of Legal Affairs, or the Department of  
455 Agriculture and Consumer Services, consult with these  
456 departments regarding the risks and other effects of such  
457 projects on their information technology systems and work  
458 cooperatively with these departments regarding the connections,  
459 interfaces, timing, or accommodations required to implement such  
460 projects.

461 (o) ~~(15)~~ If adherence to standards or policies adopted by  
462 or established pursuant to this section causes conflict with  
463 federal regulations or requirements imposed on a state agency  
464 and results in adverse action against the state agency or  
465 federal funding, work with the state agency to provide  
466 alternative standards, policies, or requirements that do not  
467 conflict with the federal regulation or requirement. The Florida  
468 Digital Service ~~department~~ shall annually report such  
469 alternative standards to the Governor, the President of the  
470 Senate, and the Speaker of the House of Representatives.

471 (p) 1. ~~(16)~~ (a) Establish an information technology policy  
472 for all information technology-related state contracts,  
473 including state term contracts for information technology  
474 commodities, consultant services, and staff augmentation  
475 services. The information technology policy must include:

476        a.1. Identification of the information technology product  
477 and service categories to be included in state term contracts.

478        b.2. Requirements to be included in solicitations for  
479 state term contracts.

480        c.3. Evaluation criteria for the award of information  
481 technology-related state term contracts.

482        d.4. The term of each information technology-related state  
483 term contract.

484        e.5. The maximum number of vendors authorized on each  
485 state term contract.

486        2.(b) Evaluate vendor responses for information  
487 technology-related state term contract solicitations and  
488 invitations to negotiate.

489        3.(e) Answer vendor questions on information technology-  
490 related state term contract solicitations.

491        4.(d) Ensure that the information technology policy  
492 established pursuant to subparagraph 1. ~~paragraph (a)~~ is  
493 included in all solicitations and contracts that are  
494 administratively executed by the department.

495        (q) (17) Recommend potential methods for standardizing data  
496 across state agencies which will promote interoperability and  
497 reduce the collection of duplicative data.

498        (r) (18) Recommend open data technical standards and  
499 terminologies for use by state agencies.

500        (2) (a) The Secretary of Management Services shall appoint

501 a state chief information officer, who shall administer the  
502 Florida Digital Service and is included in the Senior Management  
503 Service.

504 (b) The state chief information officer shall appoint a  
505 chief data officer, who shall report to the state chief  
506 information officer and is included in the Senior Management  
507 Service.

508 (3) The Florida Digital Service shall develop a  
509 comprehensive enterprise architecture that:

510 (a) Recognizes the unique needs of those included within  
511 the enterprise that results in the publication of standards,  
512 terminologies, and procurement guidelines to facilitate digital  
513 interoperability.

514 (b) Supports the cloud-first policy as specified in s.  
515 282.206.

516 (c) Addresses how information technology infrastructure  
517 may be modernized to achieve cloud-first objectives.

518 (4) The Florida Digital Service shall, pursuant to  
519 legislative appropriation:

520 (a) Create and maintain a comprehensive indexed data  
521 catalog that lists what data elements are housed within the  
522 enterprise and in which legacy system or application these data  
523 elements are located.

524 (b) Develop and publish, in collaboration with the  
525 enterprise, a data dictionary for each agency that reflects the

526 nomenclature in the comprehensive indexed data catalog.

527 (c) Review and document use cases across the enterprise  
528 architecture.

529 (d) Develop, publish, and manage an application  
530 programming interface to facilitate integration throughout the  
531 enterprise.

532 (e) Facilitate collaborative analysis of enterprise  
533 architecture data to improve service delivery.

534 (f) Provide a testing environment in which any newly  
535 developed solution can be tested for compliance within the  
536 enterprise architecture and for functionality assurance before  
537 deployment.

538 (g) Create the functionality necessary for a secure  
539 ecosystem of data interoperability that is compliant with the  
540 enterprise architecture and allows for a qualified entity to  
541 access the stored data under the terms of the agreement with the  
542 department.

543 (h) Develop and deploy applications or solutions to  
544 existing enterprise obligations in a controlled and phased  
545 approach, including, but not limited to:

546 1. Digital licenses, including full identification  
547 management.

548 2. Interoperability that enables supervisors of elections  
549 to authenticate voter eligibility in real time at the point of  
550 service.

551 3. The criminal justice database.

552 4. Motor vehicle insurance cancellation integration  
553 between insurers and the Department of Highway Safety and Motor  
554 Vehicles.

555 5. Interoperability solutions between agencies, including,  
556 but not limited to, the Department of Health, the Agency for  
557 Health Care Administration, the Agency for Persons with  
558 Disabilities, the Department of Education, the Department of  
559 Elderly Affairs, and the Department of Children and Families.

560 6. Interoperability solutions to support military members,  
561 veterans, and their families.

562 (5) Pursuant to legislative authorization and subject to  
563 appropriation:

564 (a) The department may procure a credential service  
565 provider through a competitive process pursuant to s. 287.057.  
566 The terms of the contract developed from such procurement must  
567 pay for the value on a per-data-call or subscription basis, and  
568 there shall be no cost to the enterprise or law enforcement for  
569 using the services provided by the credential service provider.

570 (b) The department may enter into agreements with  
571 electronic credential providers that have the technological  
572 capabilities necessary to integrate with the credential service  
573 provider; ensure secure validation and authentication of data;  
574 meet usage criteria; and agree to terms and conditions, privacy  
575 policies, and uniform remittance terms relating to the

576 consumption of an electronic credential. These agreements must  
577 include clear, enforceable, and significant penalties for  
578 violations of the agreements.

579 (c) The department may enter into agreements with  
580 qualified entities that meet usage criteria and agree to the  
581 enterprise architecture terms of service and privacy policies.  
582 These agreements must include clear, enforceable, and  
583 significant penalties for violations of the agreements.

584 (d) The terms of the agreements between the department and  
585 the credential service provider, the electronic credential  
586 providers, and the qualified entities shall be based on the per-  
587 data-call or subscription charges to validate and authenticate  
588 an electronic credential and allow the department to recover any  
589 state costs for implementing and administering an electronic  
590 credential solution. Credential service provider, electronic  
591 credential provider, and qualifying entity revenues may not be  
592 derived from any other transactions that generate revenue for  
593 the enterprise outside of the per-data-call or subscription  
594 charges.

595 (e) All revenues generated from the agreements with the  
596 credential service provider, electronic credential providers,  
597 and qualified entities shall be remitted to the department, and  
598 the department shall deposit these revenues into the Department  
599 of Management Services Operating Trust Fund for distribution  
600 pursuant to a legislative appropriation and department



601 agreements with the credential service provider, electronic  
602 credential providers, and qualified entities.

603 (f) Upon the signing of the agreement and the enterprise  
604 architecture terms of service and privacy policies with a  
605 qualified entity or an electronic credential provider, the  
606 department shall provide to the qualified entity or the  
607 electronic credential provider, as applicable, appropriate  
608 access to the stored data to facilitate authorized integrations  
609 to collaboratively solve enterprise use cases.

610 (6) The Florida Digital Service may develop a process to:

611 (a) Receive written notice from the state agencies within  
612 the enterprise of any planned or existing procurement of an  
613 information technology project that is subject to governance by  
614 the enterprise architecture.

615 (b) Intervene in any planned procurement by a state agency  
616 so that the procurement complies with the enterprise  
617 architecture.

618 (c) Report to the Governor, the President of the Senate,  
619 and the Speaker of the House of Representatives on any  
620 information technology project within the judicial branch that  
621 does not comply with the enterprise architecture.

622 (7) ~~(19)~~ The Florida Digital Service may adopt rules to  
623 administer this section.

624 Section 4. Section 282.00515, Florida Statutes, is amended  
625 to read:

626           282.00515 Enterprise Architecture Advisory Council ~~Duties~~  
627 ~~of Cabinet Agencies. The Department of Legal Affairs, the~~  
628 ~~Department of Financial Services, and the Department of~~  
629 ~~Agriculture and Consumer Services shall adopt the standards~~  
630 ~~established in s. 282.0051(2), (3), and (7) or adopt alternative~~  
631 ~~standards based on best practices and industry standards, and~~  
632 ~~may contract with the department to provide or perform any of~~  
633 ~~the services and functions described in s. 282.0051 for the~~  
634 ~~Department of Legal Affairs, the Department of Financial~~  
635 ~~Services, or the Department of Agriculture and Consumer~~  
636 ~~Services.~~

637           (1) (a) The Enterprise Architecture Advisory Council, an  
638 advisory council as defined in s. 20.03(7), is established  
639 within the Department of Management Services. The council shall  
640 comply with the requirements of s. 20.052, except as otherwise  
641 provided in this section.

642           (b) The council shall consist of the following members:

643           1. Four members appointed by the Governor.

644           2. One member appointed by the President of the Senate.

645           3. One member appointed by the Speaker of the House of  
646 Representatives.

647           4. One member appointed by the Chief Justice of the  
648 Supreme Court.

649           5. The director of the Office of Policy and Budget in the  
650 Executive Office of the Governor, or the person acting in the

651 director's capacity should the position be vacant.

652 6. The Secretary of Management Services, or the person  
653 acting in the secretary's capacity should the position be  
654 vacant.

655 7. The state chief information officer, or the person  
656 acting in the state chief information officer's capacity should  
657 the position be vacant.

658 8. The chief information officer of the Department of  
659 Financial Services, or the person acting in the chief  
660 information officer's capacity should the position be vacant.

661 9. The chief information officer of the Department of  
662 Legal Affairs, or the person acting in the chief information  
663 officer's capacity should the position be vacant.

664 10. The chief information officer of the Department of  
665 Agriculture and Consumer Services, or the person acting in the  
666 chief information officer's capacity should the position be  
667 vacant.

668 (2) (a) The appointments made by the Governor, the  
669 President of the Senate, the Speaker of the House of  
670 Representatives, and the Chief Justice of the Supreme Court are  
671 for terms of 4 years. However, for the purpose of providing  
672 staggered terms:

673 1. The appointments made by the Governor, the President of  
674 the Senate, and the Speaker of the House of Representatives are  
675 for initial terms of 2 years.

676 2. The appointment made by the Chief Justice is for an  
677 initial term of 3 years.

678 (b) A vacancy on the council among members appointed under  
679 subparagraph (1)(b)1., subparagraph (1)(b)2., subparagraph  
680 (1)(b)3., or subparagraph (1)(b)4. shall be filled in the same  
681 manner as the original appointment for the remainder of the  
682 unexpired term.

683 (c) The council shall elect a chair from among its  
684 members.

685 (d) The council shall meet at least semiannually,  
686 beginning October 1, 2020, to discuss implementation,  
687 management, and coordination of the enterprise architecture as  
688 defined in s. 282.0041; identify potential issues and threats  
689 with specific use cases; and recommend proactive solutions. The  
690 council may conduct its meetings through teleconferences or  
691 other similar means.

692 Section 5. Paragraph (a) of subsection (3) of section  
693 282.318, Florida Statutes, is amended to read:

694 282.318 Security of data and information technology.—

695 (3) The department is responsible for establishing  
696 standards and processes consistent with generally accepted best  
697 practices for information technology security, to include  
698 cybersecurity, and adopting rules that safeguard an agency's  
699 data, information, and information technology resources to  
700 ensure availability, confidentiality, and integrity and to

701 mitigate risks. The department shall also:

702 (a) Designate a state chief information security officer  
703 who shall report to the state chief information officer of the  
704 Florida Digital Service and is in the Senior Management Service.  
705 The state chief information security officer must have  
706 experience and expertise in security and risk management for  
707 communications and information technology resources.

708 Section 6. Subsection (4) of section 287.0591, Florida  
709 Statutes, is amended to read:

710 287.0591 Information technology.—

711 (4) If the department issues a competitive solicitation  
712 for information technology commodities, consultant services, or  
713 staff augmentation contractual services, the Florida Digital  
714 Service ~~Division of State Technology~~ within the department shall  
715 participate in such solicitations.

716 Section 7. Paragraph (a) of subsection (3) of section  
717 365.171, Florida Statutes, is amended to read:

718 365.171 Emergency communications number E911 state plan.—

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

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

723 Section 8. Paragraph (s) of subsection (3) of section  
724 365.172, Florida Statutes, is amended to read:

725 365.172 Emergency communications number "E911."—

726 (3) DEFINITIONS.—Only as used in this section and ss.  
727 365.171, 365.173, 365.174, and 365.177, the term:

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

731 Section 9. Paragraph (a) of subsection (1) of section  
732 365.173, Florida Statutes, is amended to read:

733 365.173 Communications Number E911 System Fund.—

734 (1) REVENUES.—

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

742 Section 10. Subsection (5) of section 943.0415, Florida  
743 Statutes, is amended to read:

744 943.0415 Cybercrime Office.—There is created within the  
745 Department of Law Enforcement the Cybercrime Office. The office  
746 may:

747 (5) Consult with the Florida Digital Service ~~Division of~~  
748 ~~State Technology~~ within the Department of Management Services in  
749 the adoption of rules relating to the information technology  
750 security provisions in s. 282.318.

751 Section 11. Section 560.214, Florida Statutes, is created  
752 to read:

753 560.214 Financial Technology Sandbox.-

754 (1) SHORT TITLE.-This section may be cited as the  
755 "Financial Technology Sandbox."

756 (2) CREATION OF THE FINANCIAL TECHNOLOGY SANDBOX.-There is  
757 created the Financial Technology Sandbox within the office to  
758 allow financial technology innovators to test new products and  
759 services in a supervised, flexible regulatory sandbox, using  
760 waivers of specified general law and corresponding rule  
761 requirements under defined conditions. The creation of a  
762 supervised, flexible regulatory sandbox provides a welcoming  
763 business environment for technology innovators and may lead to  
764 significant business growth.

765 (3) DEFINITIONS.-As used in this section, the term:

766 (a) "Consumer" means a person in this state, whether a  
767 natural person or a business entity, who purchases, uses,  
768 receives, or enters into an agreement to purchase, use, or  
769 receive an innovative financial product or service made  
770 available through the Financial Technology Sandbox.

771 (b) "Financial product or service" means a product or  
772 service related to money transmitters and payment instrument  
773 sellers, as defined in s. 560.103, including mediums of exchange  
774 that are in electronic or digital form, which is subject to  
775 general law or corresponding rule requirements in the sections

776 enumerated in paragraph (4) (a) and which is under the  
777 jurisdiction of the office.

778 (c) "Financial Technology Sandbox" means the program  
779 created in this section which allows a person to make an  
780 innovative financial product or service available to consumers  
781 as a money transmitter or payment instrument seller, as defined  
782 in s. 560.103, during a sandbox period through a waiver of  
783 general laws or rule requirements, or portions thereof, as  
784 specified in this section.

785 (d) "Innovative" means new or emerging technology, or new  
786 uses of existing technology, which provides a product, service,  
787 business model, or delivery mechanism to the public.

788 (e) "Office" means, unless the context clearly indicates  
789 otherwise, the Office of Financial Regulation.

790 (f) "Sandbox period" means the period, initially not  
791 longer than 24 months, in which the office has:

792 1. Authorized an innovative financial product or service  
793 to be made available to consumers.

794 2. Granted the person who makes the innovative financial  
795 product or service available a waiver of general law or  
796 corresponding rule requirements, as determined by the office, so  
797 that the authorization under subparagraph 1. is possible.

798 (4) WAIVERS OF GENERAL LAW AND RULE REQUIREMENTS.—

799 (a) If all the conditions in this section are met, the  
800 office may approve the application and grant the applicant a



801 waiver of a requirement, or a portion thereof, which is imposed  
802 by a general law or corresponding rule in any of the following  
803 sections:

- 804 1. Section 560.1105.
- 805 2. Section 560.118.
- 806 3. Section 560.125, except for s. 560.125(2).
- 807 4. Section 560.128.
- 808 5. Section 560.1401, except for s. 560.1401(2)-(4).
- 809 6. Section 560.141, except for s. 560.141(1)(b)-(d).
- 810 7. Section 560.142, except that the office may prorate,  
811 but may not entirely waive, the license renewal fees provided in  
812 ss. 560.142 and 560.143 for an extension granted under  
813 subsection (7).
- 814 8. Section 560.143(2) to the extent necessary for  
815 proration of the renewal fee under subparagraph 7.
- 816 9. Section 560.205, except for s. 560.205(1) and (3).
- 817 10. Section 560.208, except for s. 560.208(3)-(6).
- 818 11. Section 560.209, except that the office may modify,  
819 but may not entirely waive, the net worth, corporate surety  
820 bond, and collateral deposit amounts required under s. 560.209.  
821 The modified amounts must be in such lower amounts that the  
822 office determines to be commensurate with the considerations  
823 under paragraph (5)(e) and the maximum number of consumers  
824 authorized to receive the financial product or service under  
825 this section.

826 (b) The office may grant, during a sandbox period, a  
827 waiver of a requirement, or a portion thereof, imposed by a  
828 general law or corresponding rule in any section enumerated in  
829 paragraph (a), if all of the following conditions are met:

830 1. The general law or corresponding rule currently  
831 prevents the innovative financial product or service to be made  
832 available to consumers.

833 2. The waiver is not broader than necessary to accomplish  
834 the purposes and standards specified in this section, as  
835 determined by the office.

836 3. No provision relating to the liability of an  
837 incorporator, director, or officer of the applicant is eligible  
838 for a waiver.

839 4. The other requirements of this section are met.

840 (5) FINANCIAL TECHNOLOGY SANDBOX APPLICATION; STANDARDS  
841 FOR APPROVAL.—

842 (a) Before filing an application under this section, a  
843 substantially affected person may seek a declaratory statement  
844 pursuant to s. 120.565 regarding the applicability of a statute,  
845 rule, or agency order to the petitioner's particular set of  
846 circumstances.

847 (b) Before making an innovative financial product or  
848 service available to consumers in the Financial Technology  
849 Sandbox, a person must file an application with the office. The  
850 commission shall, by rule, prescribe the form and manner of the

851 application.

852 1. In the application, the person must specify the general  
853 law or rule requirements for which a waiver is sought, and the  
854 reasons why these requirements prevent the innovative financial  
855 product or service from being made available to consumers.

856 2. The application must also contain the information  
857 specified in paragraph (e).

858 (c) A business entity filing an application under this  
859 section must be a domestic corporation or other organized  
860 domestic entity with a physical presence, other than that of a  
861 registered office or agent or virtual mailbox, in this state.

862 (d) Before a person applies on behalf of a business entity  
863 intending to make an innovative financial product or service  
864 available to consumers, the person must obtain the consent of  
865 the business entity.

866 (e) The office shall approve or deny in writing a  
867 Financial Technology Sandbox application within 60 days after  
868 receiving the completed application. The office and the  
869 applicant may jointly agree to extend the time beyond 60 days.  
870 The office may impose conditions on any approval, consistent  
871 with this section. In deciding to approve or deny an  
872 application, the office must consider each of the following:

873 1. The nature of the innovative financial product or  
874 service proposed to be made available to consumers in the  
875 Financial Technology Sandbox, including all relevant technical

876 details.

877 2. The potential risk to consumers and the methods that  
878 will be used to protect consumers and resolve complaints during  
879 the sandbox period.

880 3. The business plan proposed by the applicant, including  
881 a statement regarding the applicant's current and proposed  
882 capitalization.

883 4. Whether the applicant has the necessary personnel,  
884 adequate financial and technical expertise, and a sufficient  
885 plan to test, monitor, and assess the innovative financial  
886 product or service.

887 5. Whether any person substantially involved in the  
888 development, operation, or management of the applicant's  
889 innovative financial product or service has pled no contest to,  
890 has been convicted or found guilty of, or is currently under  
891 investigation for, fraud, a state or federal securities  
892 violation, a property-based offense, or a crime involving moral  
893 turpitude or dishonest dealing. A plea of no contest, a  
894 conviction, or a finding of guilt must be reported under this  
895 subparagraph regardless of adjudication.

896 6. A copy of the disclosures that will be provided to  
897 consumers under paragraph (6) (c).

898 7. The financial responsibility of any person  
899 substantially involved in the development, operation, or  
900 management of the applicant's innovative financial product or

901 service.

902 8. Any other factor that the office determines to be  
903 relevant.

904 (f) The office may not approve an application if:

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

908 2. Any person substantially involved in the development,  
909 operation, or management of the applicant's innovative financial  
910 product or service was substantially involved in such with  
911 another Financial Technology Sandbox applicant whose application  
912 was approved and whose application related to a substantially  
913 similar financial product or service.

914 (g) Upon approval of an application, the office shall  
915 specify the general law or rule requirements, or portions  
916 thereof, for which a waiver is granted during the sandbox period  
917 and the length of the initial sandbox period, not to exceed 24  
918 months. The office shall post on its website notice of the  
919 approval of the application, a summary of the innovative  
920 financial product or service, and the contact information of the  
921 person making the financial product or service available.

922 (6) OPERATION OF THE FINANCIAL TECHNOLOGY SANDBOX.-

923 (a) A person whose Financial Technology Sandbox  
924 application is approved may make an innovative financial product  
925 or service available to consumers during the sandbox period.

926        (b) The office may, on a case-by-case basis, specify the  
927 maximum number of consumers authorized to receive an innovative  
928 financial product or service, after consultation with the person  
929 who makes the financial product or service available to  
930 consumers. The office may not authorize more than 15,000  
931 consumers to receive the financial product or service until the  
932 person who makes the financial product or service available to  
933 consumers has filed the first report required under subsection  
934 (8). After the filing of the report, if the person demonstrates  
935 adequate financial capitalization, risk management process, and  
936 management oversight, the office may authorize up to 25,000  
937 consumers to receive the financial product or service.

938        (c)1. Before a consumer purchases, uses, receives, or  
939 enters into an agreement to purchase, use, or receive an  
940 innovative financial product or service through the Financial  
941 Technology Sandbox, the person making the financial product or  
942 service available must provide a written statement of all of the  
943 following to the consumer:

944            a. The name and contact information of the person making  
945 the financial product or service available to consumers.

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

949            c. That the state does not endorse the financial product  
950 or service.

951 d. That the financial product or service is undergoing  
952 testing, may not function as intended, and may entail financial  
953 risk.

954 e. That the person making the financial product or service  
955 available to consumers is not immune from civil liability for  
956 any losses or damages caused by the financial product or  
957 service.

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

959 g. The contact information for the office, and  
960 notification that suspected legal violations, complaints, or  
961 other comments related to the financial product or service may  
962 be submitted to the office.

963 h. Any other statements or disclosures required by rule of  
964 the commission which are necessary to further the purposes of  
965 this section.

966 2. The written statement must contain an acknowledgement  
967 from the consumer, which must be retained for the duration of  
968 the sandbox period by the person making the financial product or  
969 service available.

970 (d) The office may enter into an agreement with a state,  
971 federal, or foreign regulatory agency to allow persons who make  
972 an innovative financial product or service available in this  
973 state through the Financial Technology Sandbox to make their  
974 products or services available in other jurisdictions.

975 (e)1. A person whose Financial Technology Sandbox

976 application is approved by the office shall maintain  
977 comprehensive records relating to the innovative financial  
978 product or service. The person shall keep these records for at  
979 least 5 years after the conclusion of the sandbox period. The  
980 commission may specify by rule additional records requirements.

981 2. The office may examine the records maintained under  
982 subparagraph 1. at any time, with or without notice.

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

984 (a) A person who is authorized to make an innovative  
985 financial product or service available to consumers may apply  
986 for an extension of the initial sandbox period for up to 12  
987 additional months for a purpose specified in subparagraph (b)1.  
988 or subparagraph (b)2. A complete application for an extension  
989 must be filed with the office at least 90 days before the  
990 conclusion of the initial sandbox period. The office shall  
991 approve or deny the application for extension in writing at  
992 least 35 days before the conclusion of the initial sandbox  
993 period. In deciding to approve or deny an application for  
994 extension of the sandbox period, the office must, at a minimum,  
995 consider the current status of the factors previously considered  
996 under paragraph (5) (e).

997 (b) An application for an extension under paragraph (a)  
998 must cite one of the following reasons as the basis for the  
999 application and must provide all relevant supporting information  
1000 that:



1001 1. Amendments to general law or rules are necessary to  
1002 offer the innovative financial product or service in this state  
1003 permanently.

1004 2. An application for a license that is required in order  
1005 to offer the innovative financial product or service in this  
1006 state permanently has been filed with the office, and approval  
1007 is pending.

1008 (c) At least 30 days before the conclusion of the initial  
1009 sandbox period or the extension, whichever is later, a person  
1010 who makes an innovative financial product or service available  
1011 shall provide written notification to consumers regarding the  
1012 conclusion of the initial sandbox period or the extension and  
1013 may not make the financial product or service available to any  
1014 new consumers after the conclusion of the initial sandbox period  
1015 or the extension, whichever is later, until legal authority  
1016 outside of the Financial Technology Sandbox exists to make the  
1017 financial product or service available to consumers. After the  
1018 conclusion of the sandbox period or the extension, whichever is  
1019 later, the person may:

1020 1. Collect and receive money owed to the person or pay  
1021 money owed by the person, based on agreements with consumers  
1022 made before the conclusion of the sandbox period or the  
1023 extension.

1024 2. Take necessary legal action.

1025 3. Take other actions authorized by commission rule which

1026 are not inconsistent with this subsection.

1027 (8) REPORT.—A person authorized to make an innovative  
1028 financial product or service available to consumers under this  
1029 section shall submit a report to the office twice a year as  
1030 prescribed by commission rule. The report must, at a minimum,  
1031 include financial reports and the number of consumers who have  
1032 received the financial product or service.

1033 (9) CONSTRUCTION.—A person whose Financial Technology  
1034 Sandbox application is approved shall be deemed licensed under  
1035 part II of this chapter unless the person's authorization to  
1036 make the financial product or service available to consumers  
1037 under this section has been revoked or suspended.

1038 (10) VIOLATIONS AND PENALTIES.—

1039 (a) A person who makes an innovative financial product or  
1040 service available to consumers in the Financial Technology  
1041 Sandbox is:

1042 1. Not immune from civil damages for acts and omissions  
1043 relating to this section.

1044 2. Subject to all criminal and consumer protection laws.

1045 (b)1. The office may, by order, revoke or suspend  
1046 authorization granted to a person to make an innovative  
1047 financial product or service available to consumers if:

1048 a. The person has violated or refused to comply with this  
1049 section, a rule of the commission, an order of the office, or a  
1050 condition placed by the office on the approval of the person's

1051 Financial Technology Sandbox application;  
1052 b. A fact or condition exists that, if it had existed or  
1053 become known at the time that the Financial Technology Sandbox  
1054 application was pending, would have warranted denial of the  
1055 application or the imposition of material conditions;  
1056 c. A material error, false statement, misrepresentation,  
1057 or material omission was made in the Financial Technology  
1058 Sandbox application; or  
1059 d. After consultation with the person, continued testing  
1060 of the innovative financial product or service would:  
1061 (I) Be likely to harm consumers; or  
1062 (II) No longer serve the purposes of this section because  
1063 of the financial or operational failure of the financial product  
1064 or service.  
1065 2. Written notice of a revocation or suspension order made  
1066 under subparagraph 1. shall be served using any means authorized  
1067 by law. If the notice relates to a suspension, the notice must  
1068 include any condition or remedial action that the person must  
1069 complete before the office lifts the suspension.  
1070 (c) The office may refer any suspected violation of law to  
1071 an appropriate state or federal agency for investigation,  
1072 prosecution, civil penalties, and other appropriate enforcement  
1073 actions.  
1074 (d) If service of process on a person making an innovative  
1075 financial product or service available to consumers in the

1076 Financial Technology Sandbox is not feasible, service on the  
 1077 office shall be deemed service on such person.

1078 (11) RULES AND ORDERS.—

1079 (a) The commission shall adopt rules to administer this  
 1080 section.

1081 (b) The office may issue all necessary orders to enforce  
 1082 this section and may enforce these orders in accordance with  
 1083 chapter 120 or in any court of competent jurisdiction. These  
 1084 orders include, but are not limited to, orders for payment of  
 1085 restitution for harm suffered by consumers as a result of an  
 1086 innovative financial product or service.

1087 Section 12. Effective July 1, 2020, for the 2020-2021  
 1088 fiscal year, the sum of \$50,000 in nonrecurring funds is  
 1089 appropriated from the Administrative Trust Fund to the Office of  
 1090 Financial Regulation to implement s. 560.214, Florida Statutes,  
 1091 as created by this act.

1092 Section 13. Except as otherwise expressly provided in this  
 1093 act and except for this section, which shall take effect upon  
 1094 this act becoming a law, this act shall take effect January 1,  
 1095 2021.