

FOR CONSIDERATION By the Committee on Appropriations

576-02447-25

20257026pb

1 A bill to be entitled
2 An act relating to information technology; creating s.
3 20.70, F.S.; creating the Agency for State Systems and
4 Enterprise Technology (ASSET); providing that the
5 Governor and Cabinet are the head of the agency;
6 establishing divisions and offices of the agency;
7 providing for an executive director of the agency;
8 providing that the executive director also serves as
9 the state chief information officer; providing for the
10 appointment and removal of such executive director;
11 prohibiting the state chief information officer from
12 having financial, personal, or business conflicts of
13 interest related to certain vendors, contractors, and
14 service providers of the state; requiring that the
15 state chief information officer selection committee
16 within ASSET be appointed and provide a specified
17 number of nominees upon a vacancy of such officer;
18 providing the composition of such committee; providing
19 the qualifications for the state chief information
20 officer; providing that persons who currently serve,
21 or have served, as state agency heads are ineligible
22 to serve as the state chief information officer;
23 transferring the state chief information officer of
24 the Department of Management Services to ASSET until
25 the Governor and the Cabinet appoint a permanent
26 officer; requiring that such appointment occur by a
27 specified date; amending s. 97.0525, F.S.; requiring
28 that the Division of Elections comprehensive risk
29 assessment comply with the risk assessment methodology

576-02447-25

20257026pb

30 developed by ASSET; amending s. 112.22, F.S.; defining
31 the term "ASSET"; deleting the term "department";
32 revising the definition of the term "prohibited
33 application"; authorizing public employers to request
34 a certain waiver from ASSET; requiring ASSET to take
35 specified actions; deleting obsolete language;
36 requiring ASSET to adopt rules; amending s. 119.0725,
37 F.S.; providing that confidential and exempt
38 information must be made available to ASSET; amending
39 s. 216.023, F.S.; requiring agencies and the judicial
40 branch to include a cumulative inventory and a certain
41 status report of specified projects with their
42 legislative budget requests; defining the term
43 "technology-related project"; deleting a provision
44 requiring state agencies and the judicial branch to
45 include a cumulative inventory and a certain status
46 report of specified projects as part of a budget
47 request; conforming a cross-reference; amending s.
48 282.0041, F.S.; deleting and revising definitions;
49 defining the terms "ASSET" and "technical debt";
50 amending s. 282.0051, F.S.; deleting obsolete
51 language; revising the powers, duties, and functions
52 of the Department of Management Services, through the
53 Florida Digital Service; deleting a requirement that
54 the state chief information officer, in consultation
55 with the Secretary of Management Services, designate a
56 state chief data officer; deleting requirements of the
57 department, acting through the Florida Digital
58 Service, relating to the use of appropriated funds for

576-02447-25

20257026pb

59 certain actions; deleting provisions related to
60 information technology projects that have a total
61 project cost in excess of \$10 million; providing for
62 the future repeal of the section; deleting a
63 requirement to adopt rules; repealing s. 282.00515,
64 F.S., relating to duties of Cabinet agencies; creating
65 s. 282.006, F.S.; requiring ASSET to operate as the
66 state enterprise organization for information
67 technology governance and as the lead entity
68 responsible for understanding needs and environments,
69 creating standards and strategy, supporting state
70 agency technology efforts, and reporting on the state
71 of information technology in this state; providing
72 legislative intent; requiring ASSET to establish the
73 strategic direction of information technology in the
74 state; requiring ASSET to develop and publish
75 information technology policy for a specified purpose;
76 requiring that such policy be updated as necessary to
77 meet certain requirements and advancements in
78 technology; requiring ASSET to take specified actions
79 related to oversight of the state's technology
80 enterprise; requiring ASSET to produce specified
81 reports, recommendations, and analyses and provide
82 such reports, recommendations, and analyses to the
83 Governor, the Commissioner of Agriculture, the Chief
84 Executive Officer, the Attorney General, and the
85 Legislature by specified dates and at specified
86 intervals; providing requirements for such reports;
87 requiring ASSET to conduct a market analysis at a

576-02447-25

20257026pb

88 certain interval beginning on a specified date;
89 providing requirements for the market analysis;
90 requiring that each market analysis be used to prepare
91 a strategic plan for specified purposes; requiring
92 that copies of the market analysis and strategic plan
93 be submitted by a specified date; authorizing ASSET to
94 adopt rules; creating s. 282.0061, F.S.; providing
95 legislative intent; requiring ASSET to complete a
96 certain full baseline needs assessment of state
97 agencies, develop a specified plan to conduct such
98 assessments, and submit such plan to the Governor, the
99 Commissioner of Agriculture, the Chief Financial
100 Officer, the Attorney General, and the Legislature
101 within a specified timeframe; requiring ASSET to
102 support state agency strategic planning efforts and
103 assist such agencies with a certain phased roadmap;
104 providing requirements for such roadmaps; requiring
105 ASSET to make recommendations for standardizing data
106 across state agencies for a specified purpose and
107 identify any opportunities for standardization and
108 consolidation of information technology services
109 across state agencies and support specified functions;
110 requiring ASSET to develop standards for use by state
111 agencies and enforce consistent standards and promote
112 best practices across all state agencies; requiring
113 ASSET to provide a certain report to the Governor, the
114 Commissioner of Agriculture, the Chief Financial
115 Officer, the Attorney General, and the Legislature by
116 a specified date; providing requirements of the

576-02447-25

20257026pb

117 report; providing the duties and responsibilities of
118 ASSET related to state agency technology projects;
119 requiring ASSET, in consultation with state agencies,
120 to create a methodology, approach, and applicable
121 templates and formats for identifying and collecting
122 information technology expenditure data at the state
123 agency level; requiring ASSET to obtain, review, and
124 maintain records of the appropriations, expenditures,
125 and revenues for information technology for each state
126 agency; requiring ASSET to prescribe the format for
127 state agencies to provide financial information to
128 ASSET for inclusion in a certain annual report;
129 requiring state agencies to submit such information by
130 a specified date annually; requiring that such
131 information be reported to ASSET to determine all
132 costs and expenditures of information technology
133 assets and resources provided to state agencies;
134 requiring ASSET to work with state agencies to provide
135 alternative standards, policies, or requirements under
136 specified circumstances; creating s. 282.0062, F.S.;
137 establishing workgroups within ASSET to facilitate
138 coordination with state agencies; providing for the
139 membership and duties of such workgroups; creating s.
140 282.0063, F.S.; requiring ASSET to perform specified
141 actions to develop and manage career paths,
142 progressions, and training programs for the benefit of
143 state agency personnel; creating s. 282.0064, F.S.;
144 requiring ASSET, in coordination with the Department
145 of Management Services, to establish a policy for all

576-02447-25

20257026pb

146 information technology-related solicitations,
147 contracts, and procurements; providing requirements
148 for the policy related to state term contracts, all
149 contracts, and information technology projects that
150 require oversight; prohibiting entities providing
151 independent verification and validation from having
152 certain interests, responsibilities, or other
153 participation in the project; providing the primary
154 objective of independent verification and validation;
155 requiring the entity performing such verification and
156 validation to provide specified regular reports and
157 assessments; requiring the Division of State
158 Purchasing within the Department of Management
159 Services to coordinate with ASSET on state term
160 contract solicitations and invitations to negotiate;
161 requiring ASSET to evaluate vendor responses and
162 answer vendor questions on such solicitations and
163 invitations; creating s. 282.0065, F.S.; requiring
164 ASSET to establish, maintain, and manage a certain
165 test laboratory, beginning at a specified time;
166 providing the purpose of the laboratory; requiring
167 ASSET to take specified actions relating to the
168 laboratory; creating s. 282.0066, F.S.; requiring
169 ASSET to develop, implement, and maintain a certain
170 library; providing requirements for the library;
171 requiring ASSET to establish procedures that ensure
172 the integrity, security, and availability of the
173 library; requiring ASSET to regularly update documents
174 and materials in the library to reflect current state

576-02447-25

20257026pb

175 and federal requirements, industry best practices, and
176 emerging technologies; requiring state agencies to
177 reference and adhere to the policies, standards, and
178 guidelines of the library in specified tasks;
179 requiring ASSET to create mechanisms for state
180 agencies to submit feedback, request clarifications,
181 and recommend updates; authorizing state agencies to
182 request exemptions to specific policies, standards, or
183 guidelines under specified circumstances; providing
184 the mechanism for a state agency to request such
185 exemption; requiring ASSET to review the request and
186 make a recommendation to the state chief information
187 officer; requiring the state chief information officer
188 to present the exemption to the chief information
189 officer workgroup; requiring that approval of the
190 exemption be by majority vote; requiring that state
191 agencies granted an exemption be reviewed periodically
192 to determine whether such exemption is necessary or if
193 compliance can be achieved; amending s. 282.318, F.S.;
194 revising the duties of the Department of Management
195 Services, acting through the Florida Digital Service,
196 relating to cybersecurity; requiring state agencies to
197 report all ransomware incidents to the state chief
198 information security officer instead of the
199 Cybersecurity Operations Center; requiring the state
200 chief information security officer, instead of the
201 Cybersecurity Operations Center, to notify the
202 Legislature of certain incidents; requiring state
203 agencies to notify the state chief information

576-02447-25

20257026pb

204 security officer within specified timeframes after the
205 discovery of a specified cybersecurity incident or
206 ransomware incident; requiring the state chief
207 information security officer, instead of the
208 Cybersecurity Operations Center, to provide a certain
209 report on a quarterly basis to the Legislature;
210 revising the actions that state agency heads are
211 required to perform relating to cybersecurity;
212 reducing the timeframe that the state agency strategic
213 cybersecurity plan must cover; requiring that a
214 specified comprehensive risk assessment be done
215 biennially; providing requirements for such
216 assessment; revising the definition of the term "state
217 agency"; providing that ASSET is the lead entity
218 responsible for establishing enterprise technology and
219 cybersecurity standards and processes and security
220 measures that comply with specified standards;
221 requiring ASSET to adopt specified rules; requiring
222 that ASSET take specified actions; revising the
223 responsibilities of the state chief information
224 security officer; requiring that ASSET develop and
225 publish a specified framework that includes certain
226 guidelines and processes for use by state agencies;
227 requiring that ASSET, in consultation with the state
228 chief information technology procurement officer,
229 establish specified procedures for procuring
230 information technology commodities and services;
231 requiring ASSET, through the state chief information
232 security officer and the Division of Enterprise

576-02447-25

20257026pb

233 Information Technology Workforce Development, to
234 provide a certain annual training to specified
235 persons; conforming provisions to changes made by the
236 act; amending s. 282.3185, F.S.; requiring the state
237 chief information security officer to perform
238 specified actions relating to cybersecurity training
239 for state employees; requiring local governments to
240 notify the state chief information security officer of
241 compliance with specified provisions as soon as
242 possible; requiring local governments to notify the
243 state chief information security officer, instead of
244 the Cybersecurity Operations Center, of cybersecurity
245 or ransomware incidents; revising the timeframes in
246 which such notifications must be made; requiring the
247 state chief information security officer to notify the
248 state chief information officer, the Governor, the
249 Commissioner of Agriculture, the Chief Financial
250 Officer, the Attorney General, and the Legislature of
251 certain incidents within a specified timeframe;
252 authorizing local governments to report certain
253 cybersecurity incidents to the state chief information
254 security officer instead of the Cybersecurity
255 Operations Center; requiring the state chief
256 information security officer to provide a certain
257 consolidated incident report within a specified
258 timeframe to the Governor, the Commissioner of
259 Agriculture, the Chief Financial Officer, the Attorney
260 General, and the Legislature; conforming provisions to
261 changes made by the act; requiring the state chief

576-02447-25

20257026pb

262 information security officer to establish certain
263 guidelines and processes by a specified date;
264 conforming cross-references; repealing s. 282.319,
265 F.S., relating to the Florida Cybersecurity Advisory
266 Council; establishing positions within ASSET;
267 establishing the Division of Enterprise Information
268 Technology Services and the Division of Enterprise
269 Information Technology Purchasing and associated
270 bureaus; providing the responsibilities of the
271 bureaus; establishing the chief information officer
272 policy workgroup; providing the membership, purpose,
273 chair, and duties of the workgroup; providing for the
274 expiration of the workgroup upon completion of its
275 duties; amending s. 282.201, F.S.; revising
276 requirements of the state data center; abrogating the
277 scheduled repeal of the Division of Emergency
278 Management's exemption from using the state data
279 center; deleting Department of Management Services
280 responsibilities related to the state data center;
281 deleting provisions relating to contracting with the
282 Northwest Regional Data Center; transferring,
283 renumbering, and amending s. 1004.649, F.S.; requiring
284 the Northwest Regional Data Center, by a specified
285 date annually, to provide the projected costs of
286 providing data center services for the following
287 fiscal year to the Office of Policy and Budget in the
288 Executive Office of the Governor and to the chairs of
289 the legislative appropriations committees; deleting a
290 requirement that the data center prepare and submit

576-02447-25

20257026pb

291 certain invoices to the Department of Management
292 Services for approval; conforming a cross-reference;
293 amending s. 20.22, F.S.; deleting the Florida Digital
294 Service from the list of divisions, programs, and
295 services of the Department of Management Services;
296 amending s. 282.802, F.S.; providing that the
297 Government Technology Modernization Council is located
298 within ASSET; providing that the state chief
299 information officer, or his or her designee, is the ex
300 officio executive director of the council; conforming
301 provisions to changes made by the act; requiring the
302 council annually to submit to the Commissioner of
303 Agriculture, the Chief Financial Officer, and the
304 Attorney General certain legislative recommendations;
305 amending s. 282.604, F.S.; requiring ASSET, with input
306 from stakeholders, to adopt rules; amending s.
307 287.0591, F.S.; requiring the state chief information
308 officer, instead of the Florida Digital Service, to
309 participate in certain solicitations; amending s.
310 288.012, F.S.; conforming a cross-reference; amending
311 s. 443.1113, F.S.; requiring the Department of
312 Commerce to seek input on recommended enhancements
313 from ASSET instead of the Florida Digital Service;
314 amending s. 943.0415, F.S.; authorizing the Cybercrime
315 Office to consult with the state chief information
316 security officer of ASSET instead of the Florida
317 Digital Service; amending s. 1004.444, F.S.;
318 authorizing the Florida Center for Cybersecurity to
319 conduct, consult, or assist state agencies upon

576-02447-25

20257026pb

320 receiving a request for assistance from such agencies;
321 providing effective dates.

322

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

324

325 Section 1. Section 20.70, Florida Statutes, is created to
326 read:

327 20.70 Agency for State Systems and Enterprise Technology.—

328 There is created the Agency for State Systems and Enterprise
329 Technology. The head of the agency is the Governor and Cabinet.

330 (1) DIVISIONS AND OFFICES.—The following divisions and
331 offices of the Agency for State Systems and Enterprise
332 Technology are established:

333 (a) The Division of Administrative Services.

334 (b) The Office of Information Technology.

335 (c) Beginning July 1, 2026:

336 1. The Division of Enterprise Data and Interoperability.

337 2. The Division of Enterprise Security.

338 3. The Division of Enterprise Information Technology
339 Services.

340 4. The Division of Enterprise Information Technology
341 Purchasing.

342 5. The Division of Enterprise Information Technology
343 Workforce Development.

344 (2) EXECUTIVE DIRECTOR.—The executive director of the
345 Agency for State Systems and Enterprise Technology also serves
346 as the state chief information officer. The Governor and Cabinet
347 shall appoint a state chief information officer from nominees of
348 the state chief information officer selection committee. The

576-02447-25

20257026pb

349 appointment must be made by a majority vote of the Governor and
350 Cabinet and is subject to confirmation by the Senate. Removal of
351 the state chief information officer is subject to a majority
352 vote of the Governor and Cabinet. The state chief information
353 officer is prohibited from having any financial, personal, or
354 business conflicts of interest related to technology vendors,
355 contractors, or other information technology service providers
356 doing business with the state.

357 (3) STATE CHIEF INFORMATION OFFICER SELECTION COMMITTEE.—

358 (a) Upon a vacancy or anticipated vacancy, the state chief
359 information officer selection committee within the Agency for
360 State Systems and Enterprise Technology shall be appointed to
361 nominate up to three qualified appointees for the position of
362 state chief information officer to the Governor and Cabinet for
363 appointment.

364 (b) The selection committee shall be composed of the
365 following members:

366 1. A state agency chief information officer of an executive
367 agency, appointed by the Governor and who shall serve as chair
368 of the committee.

369 2. The chief information officer of the Department of
370 Agriculture and Consumer Services, appointed by the Commissioner
371 of Agriculture.

372 3. The chief information officer of the Department of
373 Financial Services, appointed by the Chief Financial Officer.

374 4. The chief information officer of the Department of Legal
375 Affairs, appointed by the Attorney General.

376 (4) QUALIFICATIONS FOR THE STATE CHIEF INFORMATION
377 OFFICER.—

576-02447-25

20257026pb

378 (a) Education requirements.—The state chief information
379 officer must meet one of the following criteria:

380 1. Hold a bachelor's degree from an accredited institution
381 in information technology, computer science, business
382 administration, public administration, or a related field; or

383 2. Hold a master's degree in any of the fields listed
384 above, which may be substituted for a portion of the experience
385 requirement, as determined by the selection committee.

386 (b) Professional experience requirements.—The state chief
387 information officer must have at least 10 years of progressively
388 responsible experience in information technology management,
389 digital transformation, cybersecurity, or information technology
390 governance, including:

391 1. A minimum of 5 years in an executive or senior
392 leadership role, overseeing information technology strategy,
393 operations, or enterprise technology management in either the
394 public or private sector;

395 2. Managing large-scale information technology projects,
396 enterprise infrastructure, and implementation of emerging
397 technologies;

398 3. Budget planning, procurement oversight, and financial
399 management of information technology investments; and

400 4. Working with state and federal information technology
401 regulations, digital services, and cybersecurity compliance
402 frameworks.

403 (c) Technical and policy expertise.—The state chief
404 information officer must have demonstrated expertise in:

405 1. Cybersecurity and data protection by demonstrating
406 knowledge of cybersecurity risk management, compliance with

576-02447-25

20257026pb

407 NIST, ISO 27001, and applicable federal and state security
408 regulations;

409 2. Cloud and digital services with experience with cloud
410 computing, enterprise systems modernization, digital
411 transformation, and emerging information technology trends;

412 3. Information technology governance and policy development
413 by demonstrating an understanding of statewide information
414 technology governance structures, digital services, and
415 information technology procurement policies; and

416 4. Public sector information technology management by
417 demonstrating familiarity with government information technology
418 funding models, procurement requirements, and legislative
419 processes affecting information technology strategy.

420 (d) Leadership and administrative competencies.—The state
421 chief information officer must demonstrate:

422 1. Strategic vision and innovation by possessing the
423 capability to modernize information technology systems, drive
424 digital transformation, and align information technology
425 initiatives with state goals;

426 2. Collaboration and engagement with stakeholders by
427 working with legislators, state agency heads, local governments,
428 and private sector partners to implement information technology
429 initiatives;

430 3. Crisis management and cyber resilience by possessing the
431 capability to develop and lead cyber incident response, disaster
432 recovery, and information technology continuity plans; and

433 4. Fiscal management and budget expertise managing multi-
434 million-dollar information technology budgets, cost-control
435 strategies, and financial oversight of information technology

576-02447-25

20257026pb

436 projects.

437 (e) Previous appointment or service.—A person who is
438 currently serving or has previously served as the head of a
439 state agency in the state is ineligible for nomination,
440 appointment, or service as the state chief information officer.

441 Section 2. Until a state chief information officer is
442 appointed pursuant to s. 20.70, Florida Statutes, the current
443 state chief information officer of the Department of Management
444 Services shall be transferred to the Agency for State Systems
445 and Enterprise Technology and serve as interim state chief
446 information officer. A state chief information officer for the
447 Agency for State Systems and Enterprise Technology must be
448 appointed by the Governor and Cabinet by January 2, 2026.
449 Appointments to the state chief information officer selection
450 committee must be made by August 1, 2025.

451 Section 3. Effective July 1, 2026, paragraph (b) of
452 subsection (3) of section 97.0525, Florida Statutes, is amended
453 to read:

454 97.0525 Online voter registration.—

455 (3)

456 (b) The division shall conduct a comprehensive risk
457 assessment of the online voter registration system every 2
458 years. The comprehensive risk assessment must comply with the
459 risk assessment methodology developed by the Agency for State
460 Systems and Enterprise Technology ~~Department of Management~~
461 ~~Services~~ for identifying security risks, determining the
462 magnitude of such risks, and identifying areas that require
463 safeguards. In addition, the comprehensive risk assessment must
464 incorporate all of the following:

576-02447-25

20257026pb

465 1. Load testing and stress testing to ensure that the
466 online voter registration system has sufficient capacity to
467 accommodate foreseeable use, including during periods of high
468 volume of website users in the week immediately preceding the
469 book-closing deadline for an election.

470 2. Screening of computers and networks used to support the
471 online voter registration system for malware and other
472 vulnerabilities.

473 3. Evaluation of database infrastructure, including
474 software and operating systems, in order to fortify defenses
475 against cyberattacks.

476 4. Identification of any anticipated threats to the
477 security and integrity of data collected, maintained, received,
478 or transmitted by the online voter registration system.

479 Section 4. Effective July 1, 2026, paragraphs (a) and (f)
480 of subsection (1), paragraphs (b) and (c) of subsection (2), and
481 subsections (3) and (4) of section 112.22, Florida Statutes, are
482 amended to read:

483 112.22 Use of applications from foreign countries of
484 concern prohibited.—

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

486 (a) "ASSET" means the Agency for State Systems and
487 Enterprise Technology ~~"Department" means the Department of~~
488 ~~Management Services.~~

489 (f) "Prohibited application" means an application that
490 meets the following criteria:

491 1. Any Internet application that is created, maintained, or
492 owned by a foreign principal and that participates in activities
493 that include, but are not limited to:

576-02447-25

20257026pb

- 494 a. Collecting keystrokes or sensitive personal, financial,
495 proprietary, or other business data;
- 496 b. Compromising e-mail and acting as a vector for
497 ransomware deployment;
- 498 c. Conducting cyber-espionage against a public employer;
- 499 d. Conducting surveillance and tracking of individual
500 users; or
- 501 e. Using algorithmic modifications to conduct
502 disinformation or misinformation campaigns; or
- 503 2. Any Internet application ASSET ~~the department~~ deems to
504 present a security risk in the form of unauthorized access to or
505 temporary unavailability of the public employer's records,
506 digital assets, systems, networks, servers, or information.
- 507 (2)
- 508 (b) A person, including an employee or officer of a public
509 employer, may not download or access any prohibited application
510 on any government-issued device.
- 511 1. This paragraph does not apply to a law enforcement
512 officer as defined in s. 943.10(1) if the use of the prohibited
513 application is necessary to protect the public safety or conduct
514 an investigation within the scope of his or her employment.
- 515 2. A public employer may request a waiver from ASSET ~~the~~
516 ~~department~~ to allow designated employees or officers to download
517 or access a prohibited application on a government-issued
518 device.
- 519 (c) Within 15 calendar days after ASSET ~~the department~~
520 issues or updates its list of prohibited applications pursuant
521 to paragraph (3)(a), an employee or officer of a public employer
522 who uses a government-issued device must remove, delete, or

576-02447-25

20257026pb

523 uninstall any prohibited applications from his or her
524 government-issued device.

525 (3) ASSET ~~The department~~ shall do all of the following:

526 (a) Compile and maintain a list of prohibited applications
527 and publish the list on its website. ASSET ~~The department~~ shall
528 update this list quarterly and shall provide notice of any
529 update to public employers.

530 (b) Establish procedures for granting or denying requests
531 for waivers pursuant to subparagraph (2) (b)2. The request for a
532 waiver must include all of the following:

533 1. A description of the activity to be conducted and the
534 state interest furthered by the activity.

535 2. The maximum number of government-issued devices and
536 employees or officers to which the waiver will apply.

537 3. The length of time necessary for the waiver. Any waiver
538 granted pursuant to subparagraph (2) (b)2. must be limited to a
539 timeframe of no more than 1 year, but ASSET ~~the department~~ may
540 approve an extension.

541 4. Risk mitigation actions that will be taken to prevent
542 access to sensitive data, including methods to ensure that the
543 activity does not connect to a state system, network, or server.

544 5. A description of the circumstances under which the
545 waiver applies.

546 (4) ~~(a) Notwithstanding s. 120.74(4) and (5), the department~~
547 ~~is authorized, and all conditions are deemed met, to adopt~~
548 ~~emergency rules pursuant to s. 120.54(4) and to implement~~
549 ~~paragraph (3) (a). Such rulemaking must occur initially by filing~~
550 ~~emergency rules within 30 days after July 1, 2023.~~

551 ~~(b)~~ ASSET ~~The department~~ shall adopt rules necessary to

576-02447-25

20257026pb

552 administer this section.

553 Section 5. Effective July 1, 2026, paragraph (a) of
554 subsection (5) of section 119.0725, Florida Statutes, is amended
555 to read:

556 119.0725 Agency cybersecurity information; public records
557 exemption; public meetings exemption.—

558 (5) (a) Information made confidential and exempt pursuant to
559 this section must ~~shall~~ be made available to a law enforcement
560 agency, the Auditor General, the Cybercrime Office of the
561 Department of Law Enforcement, the Agency for State Systems and
562 Enterprise Technology Florida Digital Service within the
563 Department of Management Services, and, for agencies under the
564 jurisdiction of the Governor, the Chief Inspector General.

565 Section 6. Subsection (7) of section 216.023, Florida
566 Statutes, is amended to read:

567 216.023 Legislative budget requests to be furnished to
568 Legislature by agencies.—

569 (7) As part of the legislative budget request, each state
570 agency and the judicial branch shall include a cumulative an
571 inventory and status report of all ~~ongoing~~ technology-related
572 projects ongoing during the prior fiscal year or undertaken in
573 the prior fiscal year. For the purposes of this subsection, the
574 term "technology-related project" means a project that has been
575 funded or has had or is expected to have expenditures in more
576 than one fiscal year; has ~~that have~~ a cumulative estimated or
577 realized cost of more than \$1 million; and does not include the
578 continuance of existing hardware and software maintenance
579 agreements, renewal of existing software licensing agreements,
580 or the replacement of desktop units with new technology that is

576-02447-25

20257026pb

581 substantially similar to the technology being replaced. The
582 inventory must, at a minimum, contain all of the following
583 information:

584 (a) The name of the technology system.

585 (b) A brief description of the purpose and function of the
586 system.

587 (c) A brief description of the goals of the project.

588 (d) The initiation date of the project.

589 (e) The key performance indicators for the project.

590 (f) Any other metrics for the project evaluating the health
591 and status of the project.

592 (g) The original and current baseline estimated end dates
593 of the project.

594 (h) The original and current estimated costs of the
595 project.

596 (i) Total funds appropriated or allocated to the project
597 and the current realized cost for the project by fiscal year.

598
599 ~~For purposes of this subsection, an ongoing technology-related~~
600 ~~project is one which has been funded or has had or is expected~~
601 ~~to have expenditures in more than one fiscal year. An ongoing~~
602 ~~technology-related project does not include the continuance of~~
603 ~~existing hardware and software maintenance agreements, the~~
604 ~~renewal of existing software licensing agreements, or the~~
605 ~~replacement of desktop units with new technology that is~~
606 ~~substantially similar to the technology being replaced. This~~
607 ~~subsection expires July 1, 2025.~~

608 Section 7. Effective July 1, 2026, paragraph (a) of
609 subsection (4) and subsection (7) of section 216.023, Florida

576-02447-25

20257026pb

610 Statutes, are amended to read:

611 216.023 Legislative budget requests to be furnished to
612 Legislature by agencies.—

613 (4) (a) The legislative budget request for each program must
614 contain:

615 1. The constitutional or statutory authority for a program,
616 a brief purpose statement, and approved program components.

617 2. Information on expenditures for 3 fiscal years (actual
618 prior-year expenditures, current-year estimated expenditures,
619 and agency budget requested expenditures for the next fiscal
620 year) by appropriation category.

621 3. Details on trust funds and fees.

622 4. The total number of positions (authorized, fixed, and
623 requested).

624 5. An issue narrative describing and justifying changes in
625 amounts and positions requested for current and proposed
626 programs for the next fiscal year.

627 6. Information resource requests.

628 7. Supporting information, including applicable cost-
629 benefit analyses, business case analyses, performance
630 contracting procedures, service comparisons, and impacts on
631 performance standards for any request to outsource or privatize
632 state agency functions. The cost-benefit and business case
633 analyses must include an assessment of the impact on each
634 affected activity from those identified in accordance with
635 paragraph (b). Performance standards must include standards for
636 each affected activity and be expressed in terms of the
637 associated unit of activity.

638 8. An evaluation of major outsourcing and privatization

576-02447-25

20257026pb

639 initiatives undertaken during the last 5 fiscal years having
640 aggregate expenditures exceeding \$10 million during the term of
641 the contract. The evaluation must include an assessment of
642 contractor performance, a comparison of anticipated service
643 levels to actual service levels, and a comparison of estimated
644 savings to actual savings achieved. Consolidated reports issued
645 by the Department of Management Services may be used to satisfy
646 this requirement.

647 9. Supporting information for any proposed consolidated
648 financing of deferred-payment commodity contracts including
649 guaranteed energy performance savings contracts. Supporting
650 information must also include narrative describing and
651 justifying the need, baseline for current costs, estimated cost
652 savings, projected equipment purchases, estimated contract
653 costs, and return on investment calculation.

654 10. For projects that exceed \$10 million in total cost, the
655 statutory reference of the existing policy or the proposed
656 substantive policy that establishes and defines the project's
657 governance structure, planned scope, main business objectives
658 that must be achieved, and estimated completion timeframes. The
659 governance structure for information technology-related projects
660 must incorporate the applicable project management and oversight
661 standards established pursuant to s. 282.0061 ~~s. 282.0051~~.

662 Information technology budget requests for the continuance of
663 existing hardware and software maintenance agreements, renewal
664 of existing software licensing agreements, or the replacement of
665 desktop units with new technology that is similar to the
666 technology currently in use are exempt from this requirement.

667 ~~(7) As part of the legislative budget request, each state~~

576-02447-25

20257026pb

668 ~~agency and the judicial branch shall include a cumulative~~
669 ~~inventory and status report of all technology-related projects~~
670 ~~ongoing during the prior fiscal year or undertaken in the prior~~
671 ~~fiscal year. For the purposes of this subsection, the term~~
672 ~~"technology-related project" means a project that has been~~
673 ~~funded or has had or is expected to have expenditures in more~~
674 ~~than one fiscal year; has a cumulative estimated or realized~~
675 ~~cost of more than \$1 million; and does not include the~~
676 ~~continuance of existing hardware and software maintenance~~
677 ~~agreements, renewal of existing software licensing agreements,~~
678 ~~or the replacement of desktop units with new technology that is~~
679 ~~substantially similar to the technology being replaced. The~~
680 ~~inventory must, at a minimum, contain all of the following~~
681 ~~information:~~

682 ~~(a) The name of the technology system.~~

683 ~~(b) A brief description of the purpose and function of the~~
684 ~~system.~~

685 ~~(c) A brief description of the goals of the project.~~

686 ~~(d) The initiation date of the project.~~

687 ~~(e) The key performance indicators for the project.~~

688 ~~(f) Any other metrics for the project evaluating the health~~
689 ~~and status of the project.~~

690 ~~(g) The original and current baseline estimated end dates~~
691 ~~of the project.~~

692 ~~(h) The original and current estimated costs of the~~
693 ~~project.~~

694 ~~(i) Total funds appropriated or allocated to the project~~
695 ~~and the current realized cost for the project by fiscal year.~~

696 Section 8. Present subsections (36), (37), and (38) of

576-02447-25

20257026pb

697 section 282.0041, Florida Statutes, are redesignated as
698 subsections (37), (38), and (39), respectively, and a new
699 subsection (36) is added to that section, and subsections (1)
700 and (34) of that section are amended, to read:

701 282.0041 Definitions.—As used in this chapter, the term:

702 (1) “ASSET” means the Agency for State Systems and
703 Enterprise Technology ~~“Agency assessment” means the amount each~~
704 ~~customer entity must pay annually for services from the~~
705 ~~Department of Management Services and includes administrative~~
706 ~~and data center services costs.~~

707 (34) “State agency” means any official, officer,
708 commission, board, authority, council, committee, or department
709 of the executive branch of state government; the Justice
710 Administrative Commission; the Northwest Regional Data Center;
711 and the Public Service Commission. The term does not include
712 university boards of trustees or state universities. As used in
713 part I of this chapter, except as otherwise specifically
714 provided, the term includes ~~does not include~~ the Department of
715 Legal Affairs, the Department of Agriculture and Consumer
716 Services, and ~~or~~ the Department of Financial Services.

717 (36) “Technical debt” means the accumulated cost and
718 operational impact resulting from the use of suboptimal,
719 expedient, or outdated technology solutions that require future
720 remediation, refactoring, or replacement to ensure
721 maintainability, security, efficiency, and compliance with
722 enterprise architecture standards.

723 Section 9. Section 282.0051, Florida Statutes, is amended
724 to read:

725 282.0051 Department of Management Services; Florida Digital

576-02447-25

20257026pb

726 Service; powers, duties, and functions.—

727 ~~(1) The Florida Digital Service has been created within the~~
728 ~~department to propose innovative solutions that securely~~
729 ~~modernize state government, including technology and information~~
730 ~~services, to achieve value through digital transformation and~~
731 ~~interoperability, and to fully support the cloud-first policy as~~
732 ~~specified in s. 282.206. The department, through the Florida~~
733 ~~Digital Service, shall have the following powers, duties, and~~
734 ~~functions:~~

735 (a) Assign and document state agency technical debt and
736 security risks. All results of the assessments and all
737 documentation, including source documents, meeting notes, and
738 internal work products, must be provided in native electronic
739 and paper formats to ASSET no later than June 15, 2026.

740 (b) Facilitate the transfer of existing cybersecurity tools
741 and services, provided to state agencies by the department
742 through the Florida Digital Service, directly to the respective
743 state agencies, accompanied by the necessary training, no later
744 than September 15, 2025.

745 (c) Direct the state chief information security officer to
746 provide a consolidated cybersecurity incident report by the 30th
747 day after the end of each quarter to the interim state chief
748 information officer, the Executive Office of the Governor, the
749 Commissioner of Agriculture, the Chief Financial Officer, the
750 Attorney General, the President of the Senate, and the Speaker
751 of the House of Representatives ~~Develop and publish information~~
752 ~~technology policy for the management of the state's information~~
753 ~~technology resources.~~

754 ~~(b) Develop an enterprise architecture that:~~

576-02447-25

20257026pb

755 ~~1. Acknowledges the unique needs of the entities within the~~
756 ~~enterprise in the development and publication of standards and~~
757 ~~terminologies to facilitate digital interoperability;~~

758 ~~2. Supports the cloud-first policy as specified in s.~~
759 ~~282.206; and~~

760 ~~3. Addresses how information technology infrastructure may~~
761 ~~be modernized to achieve cloud-first objectives.~~

762 ~~(c) Establish project management and oversight standards~~
763 ~~with which state agencies must comply when implementing~~
764 ~~information technology projects. The department, acting through~~
765 ~~the Florida Digital Service, shall provide training~~
766 ~~opportunities to state agencies to assist in the adoption of the~~
767 ~~project management and oversight standards. To support data-~~
768 ~~driven decisionmaking, the standards must include, but are not~~
769 ~~limited to:~~

770 ~~1. Performance measurements and metrics that objectively~~
771 ~~reflect the status of an information technology project based on~~
772 ~~a defined and documented project scope, cost, and schedule.~~

773 ~~2. Methodologies for calculating acceptable variances in~~
774 ~~the projected versus actual scope, schedule, or cost of an~~
775 ~~information technology project.~~

776 ~~3. Reporting requirements, including requirements designed~~
777 ~~to alert all defined stakeholders that an information technology~~
778 ~~project has exceeded acceptable variances defined and documented~~
779 ~~in a project plan.~~

780 ~~4. Content, format, and frequency of project updates.~~

781 ~~5. Technical standards to ensure an information technology~~
782 ~~project complies with the enterprise architecture.~~

783 ~~(d) Perform project oversight on all state agency~~

576-02447-25

20257026pb

784 ~~information technology projects that have total project costs of~~
785 ~~\$10 million or more and that are funded in the General~~
786 ~~Appropriations Act or any other law. The department, acting~~
787 ~~through the Florida Digital Service, shall report at least~~
788 ~~quarterly to the Executive Office of the Governor, the President~~
789 ~~of the Senate, and the Speaker of the House of Representatives~~
790 ~~on any information technology project that the department~~
791 ~~identifies as high-risk due to the project exceeding acceptable~~
792 ~~variance ranges defined and documented in a project plan. The~~
793 ~~report must include a risk assessment, including fiscal risks,~~
794 ~~associated with proceeding to the next stage of the project, and~~
795 ~~a recommendation for corrective actions required, including~~
796 ~~suspension or termination of the project.~~

797 ~~(e) Identify opportunities for standardization and~~
798 ~~consolidation of information technology services that support~~
799 ~~interoperability and the cloud-first policy, as specified in s.~~
800 ~~282.206, and business functions and operations, including~~
801 ~~administrative functions such as purchasing, accounting and~~
802 ~~reporting, cash management, and personnel, and that are common~~
803 ~~across state agencies. The department, acting through the~~
804 ~~Florida Digital Service, shall biennially on January 1 of each~~
805 ~~even-numbered year provide recommendations for standardization~~
806 ~~and consolidation to the Executive Office of the Governor, the~~
807 ~~President of the Senate, and the Speaker of the House of~~
808 ~~Representatives.~~

809 ~~(f) Establish best practices for the procurement of~~
810 ~~information technology products and cloud-computing services in~~
811 ~~order to reduce costs, increase the quality of data center~~
812 ~~services, or improve government services.~~

576-02447-25

20257026pb

813 ~~(g) Develop standards for information technology reports~~
814 ~~and updates, including, but not limited to, operational work~~
815 ~~plans, project spend plans, and project status reports, for use~~
816 ~~by state agencies.~~

817 ~~(h) Upon request, assist state agencies in the development~~
818 ~~of information technology related legislative budget requests.~~

819 ~~(i) Conduct annual assessments of state agencies to~~
820 ~~determine compliance with all information technology standards~~
821 ~~and guidelines developed and published by the department and~~
822 ~~provide results of the assessments to the Executive Office of~~
823 ~~the Governor, the President of the Senate, and the Speaker of~~
824 ~~the House of Representatives.~~

825 ~~(j) Conduct a market analysis not less frequently than~~
826 ~~every 3 years beginning in 2021 to determine whether the~~
827 ~~information technology resources within the enterprise are~~
828 ~~utilized in the most cost-effective and cost-efficient manner,~~
829 ~~while recognizing that the replacement of certain legacy~~
830 ~~information technology systems within the enterprise may be cost~~
831 ~~prohibitive or cost inefficient due to the remaining useful life~~
832 ~~of those resources; whether the enterprise is complying with the~~
833 ~~cloud first policy specified in s. 282.206; and whether the~~
834 ~~enterprise is utilizing best practices with respect to~~
835 ~~information technology, information services, and the~~
836 ~~acquisition of emerging technologies and information services.~~
837 ~~Each market analysis shall be used to prepare a strategic plan~~
838 ~~for continued and future information technology and information~~
839 ~~services for the enterprise, including, but not limited to,~~
840 ~~proposed acquisition of new services or technologies and~~
841 ~~approaches to the implementation of any new services or~~

576-02447-25

20257026pb

842 ~~technologies. Copies of each market analysis and accompanying~~
843 ~~strategic plan must be submitted to the Executive Office of the~~
844 ~~Governor, the President of the Senate, and the Speaker of the~~
845 ~~House of Representatives not later than December 31 of each year~~
846 ~~that a market analysis is conducted.~~

847 ~~(k) Recommend other information technology services that~~
848 ~~should be designed, delivered, and managed as enterprise~~
849 ~~information technology services. Recommendations must include~~
850 ~~the identification of existing information technology resources~~
851 ~~associated with the services, if existing services must be~~
852 ~~transferred as a result of being delivered and managed as~~
853 ~~enterprise information technology services.~~

854 ~~(l) In consultation with state agencies, propose a~~
855 ~~methodology and approach for identifying and collecting both~~
856 ~~current and planned information technology expenditure data at~~
857 ~~the state agency level.~~

858 ~~(m)1. Notwithstanding any other law, provide project~~
859 ~~oversight on any information technology project of the~~
860 ~~Department of Financial Services, the Department of Legal~~
861 ~~Affairs, and the Department of Agriculture and Consumer Services~~
862 ~~which has a total project cost of \$20 million or more. Such~~
863 ~~information technology projects must also comply with the~~
864 ~~applicable information technology architecture, project~~
865 ~~management and oversight, and reporting standards established by~~
866 ~~the department, acting through the Florida Digital Service.~~

867 ~~2. When performing the project oversight function specified~~
868 ~~in subparagraph 1., report at least quarterly to the Executive~~
869 ~~Office of the Governor, the President of the Senate, and the~~
870 ~~Speaker of the House of Representatives on any information~~

576-02447-25

20257026pb

871 ~~technology project that the department, acting through the~~
872 ~~Florida Digital Service, identifies as high risk due to the~~
873 ~~project exceeding acceptable variance ranges defined and~~
874 ~~documented in the project plan. The report shall include a risk~~
875 ~~assessment, including fiscal risks, associated with proceeding~~
876 ~~to the next stage of the project and a recommendation for~~
877 ~~corrective actions required, including suspension or termination~~
878 ~~of the project.~~

879 ~~(n) If an information technology project implemented by a~~
880 ~~state agency must be connected to or otherwise accommodated by~~
881 ~~an information technology system administered by the Department~~
882 ~~of Financial Services, the Department of Legal Affairs, or the~~
883 ~~Department of Agriculture and Consumer Services, consult with~~
884 ~~these departments regarding the risks and other effects of such~~
885 ~~projects on their information technology systems and work~~
886 ~~cooperatively with these departments regarding the connections,~~
887 ~~interfaces, timing, or accommodations required to implement such~~
888 ~~projects.~~

889 ~~(o) If adherence to standards or policies adopted by or~~
890 ~~established pursuant to this section causes conflict with~~
891 ~~federal regulations or requirements imposed on an entity within~~
892 ~~the enterprise and results in adverse action against an entity~~
893 ~~or federal funding, work with the entity to provide alternative~~
894 ~~standards, policies, or requirements that do not conflict with~~
895 ~~the federal regulation or requirement. The department, acting~~
896 ~~through the Florida Digital Service, shall annually report such~~
897 ~~alternative standards to the Executive Office of the Governor,~~
898 ~~the President of the Senate, and the Speaker of the House of~~
899 ~~Representatives.~~

576-02447-25

20257026pb

900 ~~(p)1. Establish an information technology policy for all~~
901 ~~information technology-related state contracts, including state~~
902 ~~term contracts for information technology commodities,~~
903 ~~consultant services, and staff augmentation services. The~~
904 ~~information technology policy must include:~~

905 ~~a. Identification of the information technology product and~~
906 ~~service categories to be included in state term contracts.~~

907 ~~b. Requirements to be included in solicitations for state~~
908 ~~term contracts.~~

909 ~~c. Evaluation criteria for the award of information~~
910 ~~technology-related state term contracts.~~

911 ~~d. The term of each information technology-related state~~
912 ~~term contract.~~

913 ~~e. The maximum number of vendors authorized on each state~~
914 ~~term contract.~~

915 ~~f. At a minimum, a requirement that any contract for~~
916 ~~information technology commodities or services meet the National~~
917 ~~Institute of Standards and Technology Cybersecurity Framework.~~

918 ~~g. For an information technology project wherein project~~
919 ~~oversight is required pursuant to paragraph (d) or paragraph~~
920 ~~(m), a requirement that independent verification and validation~~
921 ~~be employed throughout the project life cycle with the primary~~
922 ~~objective of independent verification and validation being to~~
923 ~~provide an objective assessment of products and processes~~
924 ~~throughout the project life cycle. An entity providing~~
925 ~~independent verification and validation may not have technical,~~
926 ~~managerial, or financial interest in the project and may not~~
927 ~~have responsibility for, or participate in, any other aspect of~~
928 ~~the project.~~

576-02447-25

20257026pb

929 ~~2. Evaluate vendor responses for information technology-~~
930 ~~related state term contract solicitations and invitations to~~
931 ~~negotiate.~~

932 ~~3. Answer vendor questions on information technology-~~
933 ~~related state term contract solicitations.~~

934 ~~4. Ensure that the information technology policy~~
935 ~~established pursuant to subparagraph 1. is included in all~~
936 ~~solicitations and contracts that are administratively executed~~
937 ~~by the department.~~

938 ~~(q) Recommend potential methods for standardizing data~~
939 ~~across state agencies which will promote interoperability and~~
940 ~~reduce the collection of duplicative data.~~

941 ~~(r) Recommend open data technical standards and~~
942 ~~terminologies for use by the enterprise.~~

943 ~~(s) Ensure that enterprise information technology solutions~~
944 ~~are capable of utilizing an electronic credential and comply~~
945 ~~with the enterprise architecture standards.~~

946 ~~(2)(a) The Secretary of Management Services shall designate~~
947 ~~a state chief information officer, who shall administer the~~
948 ~~Florida Digital Service. The state chief information officer,~~
949 ~~prior to appointment, must have at least 5 years of experience~~
950 ~~in the development of information system strategic planning and~~
951 ~~development or information technology policy, and, preferably,~~
952 ~~have leadership-level experience in the design, development, and~~
953 ~~deployment of interoperable software and data solutions.~~

954 ~~(b) The state chief information officer, in consultation~~
955 ~~with the Secretary of Management Services, shall designate a~~
956 ~~state chief data officer. The chief data officer must be a~~
957 ~~proven and effective administrator who must have significant and~~

576-02447-25

20257026pb

958 ~~substantive experience in data management, data governance,~~
959 ~~interoperability, and security.~~

960 ~~(3) The department, acting through the Florida Digital~~
961 ~~Service and from funds appropriated to the Florida Digital~~
962 ~~Service, shall:~~

963 ~~(a) Create, not later than December 1, 2022, and maintain a~~
964 ~~comprehensive indexed data catalog in collaboration with the~~
965 ~~enterprise that lists the data elements housed within the~~
966 ~~enterprise and the legacy system or application in which these~~
967 ~~data elements are located. The data catalog must, at a minimum,~~
968 ~~specifically identify all data that is restricted from public~~
969 ~~disclosure based on federal or state laws and regulations and~~
970 ~~require that all such information be protected in accordance~~
971 ~~with s. 282.318.~~

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

976 ~~(c) Adopt, by rule, standards that support the creation and~~
977 ~~deployment of an application programming interface to facilitate~~
978 ~~integration throughout the enterprise.~~

979 ~~(d) Adopt, by rule, standards necessary to facilitate a~~
980 ~~secure ecosystem of data interoperability that is compliant with~~
981 ~~the enterprise architecture.~~

982 ~~(e) Adopt, by rule, standards that facilitate the~~
983 ~~deployment of applications or solutions to the existing~~
984 ~~enterprise system in a controlled and phased approach.~~

985 ~~(f) After submission of documented use cases developed in~~
986 ~~conjunction with the affected agencies, assist the affected~~

576-02447-25

20257026pb

987 ~~agencies with the deployment, contingent upon a specific~~
988 ~~appropriation therefor, of new interoperable applications and~~
989 ~~solutions:~~

990 ~~1. For the Department of Health, the Agency for Health Care~~
991 ~~Administration, the Agency for Persons with Disabilities, the~~
992 ~~Department of Education, the Department of Elderly Affairs, and~~
993 ~~the Department of Children and Families.~~

994 ~~2. To support military members, veterans, and their~~
995 ~~families.~~

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

998 ~~(a) State agencies must provide the Florida Digital Service~~
999 ~~with written notice of any planned procurement of an information~~
1000 ~~technology project.~~

1001 ~~(b) The Florida Digital Service must participate in the~~
1002 ~~development of specifications and recommend modifications to any~~
1003 ~~planned procurement of an information technology project by~~
1004 ~~state agencies so that the procurement complies with the~~
1005 ~~enterprise architecture.~~

1006 ~~(c) The Florida Digital Service must participate in post-~~
1007 ~~award contract monitoring.~~

1008 ~~(2)(5)~~ The department, acting through the Florida Digital
1009 Service, may not retrieve or disclose any data without a shared-
1010 data agreement in place between the department and the
1011 enterprise entity that has primary custodial responsibility of,
1012 or data-sharing responsibility for, that data.

1013 (3) This section is repealed July 1, 2026.

1014 ~~(6) The department, acting through the Florida Digital~~
1015 ~~Service, shall adopt rules to administer this section.~~

576-02447-25

20257026pb

1016 Section 10. Section 282.00515, Florida Statutes, is
1017 repealed.

1018 Section 11. Effective July 1, 2026, section 282.006,
1019 Florida Statutes, is created to read:

1020 282.006 Agency for State Systems and Enterprise Technology;
1021 duties; enterprise responsibilities; reporting.—

1022 (1) The Agency for State Systems and Enterprise Technology
1023 established in s. 20.70 shall operate as the state enterprise
1024 organization for information technology governance and is the
1025 lead entity responsible for understanding the unique state
1026 agency information technology needs and environments, creating
1027 enterprise technology standards and strategy, supporting state
1028 agency technology efforts, and reporting on the status of
1029 technology for the enterprise.

1030 (2) The Legislature intends for ASSET policy, standards,
1031 guidance, and oversight to allow for adaptability to emerging
1032 technology and organizational needs while maintaining compliance
1033 with industry best practices. All policies, standards, and
1034 guidelines established pursuant to this chapter must be
1035 technology-agnostic and may not prescribe specific tools,
1036 platforms, or vendors.

1037 (3) ASSET shall establish the strategic direction of
1038 information technology in the state. ASSET shall develop and
1039 publish information technology policy that aligns with industry
1040 best practices for the management of the state's information
1041 technology resources. The policy must be updated as necessary to
1042 meet the requirements of this chapter and advancements in
1043 technology.

1044 (4) Related to its oversight of the state's technology

576-02447-25

20257026pb

1045 enterprise, ASSET shall:

1046 (a) In coordination with state agency technology subject
1047 matter experts, develop, publish, and maintain an enterprise
1048 architecture that:

1049 1. Acknowledges the unique needs of the entities within the
1050 enterprise in the development and publication of standards and
1051 terminologies to facilitate digital interoperability;

1052 2. Supports the cloud-first policy as specified in s.
1053 282.206;

1054 3. Addresses how information technology infrastructure may
1055 be modernized to achieve security, scalability, maintainability,
1056 interoperability, and improved cost-efficiency goals; and

1057 4. Includes, at a minimum, best practices, guidelines, and
1058 standards for:

1059 a. Data models and taxonomies.

1060 b. Master data management.

1061 c. Data integration and interoperability.

1062 d. Data security and encryption.

1063 e. Bot prevention and data protection.

1064 f. Data backup and recovery.

1065 g. Application portfolio and catalog requirements.

1066 h. Application architectural patterns and principles.

1067 i. Technology and platform standards.

1068 j. Secure coding practices.

1069 k. Performance and scalability.

1070 l. Cloud infrastructure and architecture.

1071 m. Networking, connectivity, and security protocols.

1072 n. Authentication, authorization, and access controls.

1073 o. Disaster recovery.

576-02447-25

20257026pb

1074 p. Quality assurance.

1075 q. Testing methodologies and measurements.

1076 r. Logging and log retention.

1077 s. Application and use of artificial intelligence.

1078 (b) Recommend open data technical standards and
1079 terminologies for use by the state's technology enterprise.

1080 (c) Develop enterprise technology testing and quality
1081 assurance best practices and standards to ensure the
1082 reliability, security, and performance of information technology
1083 systems. Such best practices and standards must include:

1084 1. Functional testing to ensure software or systems meet
1085 required specifications.

1086 2. Performance and load testing to ensure software and
1087 systems operate efficiently under various conditions.

1088 3. Security testing to protect software and systems from
1089 vulnerabilities and cyber threats.

1090 4. Compatibility and interoperability testing to ensure
1091 software and systems operate seamlessly across environments.

1092 (5) ASSET shall produce the following reports and provide
1093 them to the Governor, the Commissioner of Agriculture, the Chief
1094 Financial Officer, the Attorney General, the President of the
1095 Senate, and the Speaker of the House of Representatives:

1096 (a) Annually by December 15, an enterprise analysis report
1097 that includes all of the following:

1098 1. Results of the state agency needs assessments, including
1099 any plan to address technical debt as required by s. 282.0061
1100 pursuant to the schedule adopted.

1101 2. Alternative standards related to federal funding adopted
1102 pursuant to s. 282.0061.

576-02447-25

20257026pb

- 1103 3. Information technology financial data for each state
1104 agency for the previous fiscal year. This portion of the annual
1105 report must include, at a minimum, the following recurring and
1106 nonrecurring information:
- 1107 a. Total number of full-time equivalent positions.
1108 b. Total amount of salary.
1109 c. Total amount of benefits.
1110 d. Total number of comparable full-time equivalent
1111 positions and total amount of expenditures for information
1112 technology staff augmentation.
- 1113 e. Total number of contracts and purchase orders and total
1114 amount of associated expenditures for information technology
1115 managed services.
- 1116 f. Total amount of expenditures by state term contract as
1117 defined in s. 287.012, contracts procured using alternative
1118 purchasing methods as authorized pursuant to s. 287.042(16), and
1119 state agency procurements through request for proposal,
1120 invitation to negotiate, invitation to bid, single source, and
1121 emergency purchases.
- 1122 g. Total amount of expenditures for hardware.
1123 h. Total amount of expenditures for non-cloud software.
1124 i. Total amount of expenditures for cloud software licenses
1125 and services with a separate amount for expenditures for state
1126 data center services.
- 1127 j. Total amount of expenditures for cloud data center
1128 services with a separate amount for expenditures for state data
1129 center services.
- 1130 k. Total amount of expenditures for administrative costs.
1131 4. Consolidated information for the previous fiscal year

576-02447-25

20257026pb

1132 about state information technology projects, which must include,
1133 at a minimum, the following information:

1134 a. Anticipated funding requirements for information
1135 technology support over the next 5 years.

1136 b. An inventory of current information technology assets
1137 and major projects. The term "major project" includes projects
1138 costing more than \$500,000 to implement.

1139 c. Significant unmet needs for information technology
1140 resources over the next 5 fiscal years, ranked in priority order
1141 according to their urgency.

1142 5. A review and summary of whether the information
1143 technology contract policy established pursuant to s. 282.0064
1144 is included in all solicitations and contracts.

1145 6. Information related to the information technology test
1146 laboratory created in s. 282.0065, including usage statistics
1147 and key findings, and recommendations for improving the state's
1148 information technology procurement processes.

1149 (b) Biennially by December 15 of even-numbered years, a
1150 report on the strategic direction of information technology in
1151 the state which includes all of the following:

1152 1. Recommendations for standardization and consolidation of
1153 information technology services that are identified as common
1154 across state agencies as required in s. 282.0061.

1155 2. Recommendations for information technology services that
1156 should be designed, delivered, and managed as enterprise
1157 information technology services. Recommendations must include
1158 the identification of existing information technology resources
1159 associated with the services, if existing services must be
1160 transferred as a result of being delivered and managed as

576-02447-25

20257026pb

1161 enterprise information technology services, and which entity is
1162 best suited to manage the service.

1163 (c)1. When conducted as provided in this paragraph, a
1164 market analysis and accompanying strategic plan submitted by
1165 December 31 of each year that the market analysis is conducted.

1166 2. No less frequently than every 3 years, ASSET shall
1167 conduct market analysis to determine whether the:

1168 a. Information technology resources within the enterprise
1169 are used in the most cost-effective and cost-efficient manner,
1170 while recognizing that the replacement of certain legacy
1171 information technology systems within the enterprise may be cost
1172 prohibitive or cost inefficient due to the remaining useful life
1173 of those resources; and

1174 b. Enterprise is using best practices with respect to
1175 information technology, information services, and the
1176 acquisition of emerging technologies and information services.

1177 3. Each market analysis must be used to prepare a strategic
1178 plan for continued and future information technology and
1179 information services for the enterprise, including, but not
1180 limited to, proposed acquisition of new services or technologies
1181 and approaches to the implementation of any new services or
1182 technologies.

1183 (6) ASSET may adopt rules to implement this chapter.

1184 Section 12. Effective July 1, 2026, section 282.0061,
1185 Florida Statutes, is created to read:

1186 282.0061 ASSET support of state agencies; information
1187 technology procurement and projects.-

1188 (1) LEGISLATIVE INTENT.-The Legislature intends for ASSET
1189 to support state agencies in their information technology

576-02447-25

20257026pb

1190 efforts through the adoption of policies, standards, and
1191 guidance and by providing oversight that recognizes unique state
1192 agency information technology needs, environments, and goals.
1193 ASSET assistance and support must allow for adaptability to
1194 emerging technologies and organizational needs while maintaining
1195 compliance with industry best practices. ASSET may not prescribe
1196 specific tools, platforms, or vendors.

1197 (2) NEEDS ASSESSMENTS.—

1198 (a) By January 1, 2028, ASSET shall conduct full baseline
1199 needs assessments of state agencies to document their distinct
1200 technical environments, existing technical debt, security risks,
1201 and compliance with all information technology standards and
1202 guidelines developed and published by ASSET. The needs
1203 assessment must use the Capability Maturity Model to evaluate
1204 each state agency's information technology capabilities,
1205 providing a maturity level rating for each assessed domain.
1206 After completion of the full baseline needs assessments, such
1207 assessments must be maintained and updated on a regular schedule
1208 adopted by ASSET.

1209 (b) In assessing the existing technical debt portion of the
1210 needs assessment, ASSET shall analyze the state's legacy
1211 information technology systems and develop a plan to document
1212 the needs and costs for replacement systems. The plan must
1213 include an inventory of legacy applications and infrastructure;
1214 the required capabilities not available with the legacy system;
1215 the estimated process, timeline, and cost to migrate from legacy
1216 environments; and any other information necessary for fiscal or
1217 technology planning. The plan must determine and document the
1218 estimated timeframe during which the state agency can continue

576-02447-25

20257026pb

1219 to efficiently use legacy information technology systems,
1220 resources, security, and data management to support operations.
1221 State agencies shall provide all necessary documentation to
1222 enable accurate reporting on legacy systems.

1223 (c) ASSET shall develop a plan and schedule to conduct the
1224 initial full baseline needs assessments. By October 1, 2026,
1225 ASSET shall submit the plan to the Governor, the Commissioner of
1226 Agriculture, the Chief Financial Officer, the Attorney General,
1227 the President of the Senate, and the Speaker of the House of
1228 Representatives.

1229 (d) ASSET shall support state agency strategic planning
1230 efforts and assist state agencies with the production of a
1231 phased roadmap to address known technology gaps and deficiencies
1232 as identified in the needs assessments. The roadmaps must
1233 include specific strategies and initiatives aimed at advancing
1234 the state agency's maturity level in accordance with the
1235 Capability Maturity Model. State agencies shall create,
1236 maintain, and submit the roadmap on an annual basis with their
1237 legislative budget requests required under s. 216.023.

1238 (3) STANDARDIZATION.—ASSET shall:

1239 (a) Recommend in its annual enterprise analysis required
1240 under s. 282.006 any potential methods for standardizing data
1241 across state agencies which will promote interoperability and
1242 reduce the collection of duplicative data.

1243 (b) Identify any opportunities in its annual enterprise
1244 analysis required under s. 282.006 for standardization and
1245 consolidation of information technology services that are common
1246 across all state agencies and that support:

1247 1. Improved interoperability, security, scalability,

576-02447-25

20257026pb

1248 maintainability, and cost efficiency; and

1249 2. Business functions and operations, including
1250 administrative functions such as purchasing, accounting and
1251 reporting, cash management, and personnel.

1252 (4) DATA MANAGEMENT.—

1253 (a) ASSET shall develop standards for use by state agencies
1254 which support best practices for master data management at the
1255 state agency level to facilitate enterprise data sharing and
1256 interoperability.

1257 (b) ASSET shall establish a methodology and strategy for
1258 implementing statewide master data management and submit a
1259 report to the Governor, the Commissioner of Agriculture, the
1260 Chief Financial Officer, the Attorney General, the President of
1261 the Senate, and the Speaker of the House of Representatives by
1262 December 1, 2028. The report must include the vision, goals, and
1263 benefits of implementing a statewide master data management
1264 initiative, an analysis of the current state of data management,
1265 and the recommended strategy, methodology, and estimated
1266 timeline and resources needed at a state agency and enterprise
1267 level to accomplish the initiative.

1268 (5) INFORMATION TECHNOLOGY PROJECTS.—ASSET has the
1269 following duties and responsibilities related to state agency
1270 technology projects:

1271 (a) Provide procurement advisory and review services for
1272 information technology projects to all state agencies, including
1273 procurement and contract development assistance to meet the
1274 information technology contract policy established pursuant to
1275 s. 282.0064.

1276 (b) Establish best practices and enterprise procurement

576-02447-25

20257026pb

1277 processes and develop metrics to support these processes for the
1278 procurement of information technology products and services in
1279 order to reduce costs or improve the provision of government
1280 services.

1281 (c) Upon request, assist state agencies in the development
1282 of information technology-related legislative budget requests.

1283 (d) Develop standards and accountability measures for
1284 information technology projects, including criteria for
1285 effective project management and oversight. State agencies must
1286 satisfy these standards and measures when implementing
1287 information technology projects. To support data-driven
1288 decisionmaking, the standards and measures must include, but are
1289 not limited to:

1290 1. Performance measurements and metrics that objectively
1291 reflect the status of an information technology project based on
1292 a defined and documented project scope, to include the volume of
1293 impacted stakeholders, cost, and schedule.

1294 2. Methodologies for calculating and defining acceptable
1295 variances in the projected versus actual scope, schedule, or
1296 cost of an information technology project.

1297 3. Reporting requirements designed to alert all defined
1298 stakeholders that an information technology project has exceeded
1299 acceptable variances defined and documented in a project plan as
1300 well as any variances that represent a schedule delay of 1 month
1301 or more or a cost increase of \$1 million or more.

1302 4. Technical standards to ensure an information technology
1303 project complies with the enterprise architecture standards.

1304 (e) Develop information technology project reports for use
1305 by state agencies, including, but not limited to, operational

576-02447-25

20257026pb

1306 work plans, project spending plans, and project status reports.
1307 Reporting standards must include content, format, and frequency
1308 of project updates.

1309 (f) Provide training opportunities to state agencies to
1310 assist in the adoption of the project management and oversight
1311 standards.

1312 (g) Perform project oversight on all state agency
1313 information technology projects that have total project costs of
1314 \$10 million or more. ASSET shall report by the 30th day after
1315 the end of each quarter to the Executive Office of the Governor,
1316 the Commissioner of Agriculture, the Chief Financial Officer,
1317 the Attorney General, the President of the Senate, and the
1318 Speaker of the House of Representatives on any information
1319 technology project that ASSET identifies as high-risk. The
1320 report must include a risk assessment, including fiscal risks,
1321 associated with proceeding to the next stage of the project, and
1322 a recommendation for corrective actions required, including
1323 suspension or termination of the project.

1324 (6) INFORMATION TECHNOLOGY FINANCIAL DATA.-

1325 (a) In consultation with state agencies, ASSET shall create
1326 a methodology, an approach, and applicable templates and formats
1327 for identifying and collecting both current and planned
1328 information technology expenditure data at the state agency
1329 level. ASSET shall continuously obtain, review, and maintain
1330 records of the appropriations, expenditures, and revenues for
1331 information technology for each state agency.

1332 (b) ASSET shall prescribe the format for state agencies to
1333 provide all necessary financial information to ASSET for
1334 inclusion in the annual report required under s. 282.006. State

576-02447-25

20257026pb

1335 agencies must provide the information to ASSET by October 1 for
1336 the previous fiscal year. The information must be reported by
1337 ASSET in order to determine all costs and expenditures for
1338 information technology assets and resources provided by the
1339 state agencies or through contracts or grants.

1340 (7) FEDERAL CONFLICTS.—ASSET shall work with state agencies
1341 to provide alternative standards, policies, or requirements that
1342 do not conflict with federal regulations or requirements, if
1343 adherence to standards or policies adopted by or established
1344 pursuant to this section conflict with federal regulations or
1345 requirements imposed on an entity within the enterprise and
1346 results in, or is expected to result in, adverse action against
1347 the state agencies or loss of federal funding.

1348 Section 13. Effective July 1, 2026, section 282.0062,
1349 Florida Statutes, is created to read:

1350 282.0062 ASSET workgroups.—The following workgroups are
1351 established within ASSET to facilitate coordination with state
1352 agencies:

1353 (1) CHIEF INFORMATION OFFICER WORKGROUP.—

1354 (a) The chief information officer workgroup, composed of
1355 all state agency chief information officers, shall consider and
1356 make recommendations to the state chief information officer and
1357 the state chief information architect on such matters as
1358 enterprise information technology policies, standards, services,
1359 and architecture. The workgroup may also identify and recommend
1360 opportunities for the establishment of public-private
1361 partnerships when considering technology infrastructure and
1362 services in order to accelerate project delivery and provide a
1363 source of new or increased project funding.

576-02447-25

20257026pb

1364 (b) At a minimum, the state chief information officer shall
1365 consult with the workgroup on a quarterly basis with regard to
1366 executing the duties and responsibilities of the state agencies
1367 related to statewide information technology strategic planning
1368 and policy.

1369 (2) ENTERPRISE DATA AND INTEROPERABILITY WORKGROUP.—

1370 (a) The enterprise data and interoperability workgroup,
1371 composed of chief data officer representatives from all state
1372 agencies, shall consider and make recommendations to the state
1373 chief data officer on such matters as enterprise data policies,
1374 standards, services, and architecture that promote data
1375 consistency, accessibility, and seamless integration across the
1376 enterprise.

1377 (b) At a minimum, the state chief data officer shall
1378 consult with the workgroup on a quarterly basis with regard to
1379 executing the duties and responsibilities of the state agencies
1380 related to statewide data governance planning and policy.

1381 (3) ENTERPRISE SECURITY WORKGROUP.—

1382 (a) The enterprise security workgroup, composed of chief
1383 security officer representatives from all state agencies, shall
1384 consider and make recommendations to the state chief security
1385 officer on such matters as cybersecurity policies, standards,
1386 services, and architecture that promote the protection of state
1387 assets.

1388 (b) At a minimum, the state chief security officer shall
1389 consult with the workgroup on a quarterly basis with regard to
1390 executing the duties and responsibilities of the state agencies
1391 related to cybersecurity governance and policy development.

1392 (4) ENTERPRISE INFORMATION TECHNOLOGY OPERATIONS

576-02447-25

20257026pb

1393 WORKGROUP.—

1394 (a) The enterprise information technology operations
1395 workgroup, composed of information technology business analyst
1396 representatives from all state agencies, shall consider and make
1397 recommendations to the state chief technology officer on such
1398 matters as information technology needs assessments policies,
1399 standards, and services that promote the strategic alignment of
1400 technology with operational needs and the evaluation of
1401 solutions across the enterprise.

1402 (b) At a minimum, the state chief technology officer shall
1403 consult with the workgroup on a quarterly basis with regard to
1404 executing the duties and responsibilities of the state agencies
1405 related to statewide process improvement and optimization.

1406 (5) ENTERPRISE INFORMATION TECHNOLOGY QUALITY ASSURANCE
1407 WORKGROUP.—

1408 (a) The enterprise information technology quality assurance
1409 workgroup, composed of testing and quality assurance
1410 representatives from all state agencies, shall consider and make
1411 recommendations to the state chief technology officer on such
1412 matters as testing methodologies, tools, and best practices to
1413 reduce risks related to software defects, cybersecurity threats,
1414 and operational failures.

1415 (b) At a minimum, the state chief technology officer shall
1416 consult with the workgroup on a quarterly basis with regard to
1417 executing the duties and responsibilities of the state agencies
1418 related to enterprise software testing and quality assurance
1419 standards.

1420 (6) ENTERPRISE INFORMATION TECHNOLOGY PROJECT MANAGEMENT
1421 WORKGROUP.—

576-02447-25

20257026pb

1422 (a) The enterprise information technology project
1423 management workgroup, composed of information technology project
1424 manager representatives from all state agencies, shall consider
1425 and make recommendations to the state chief technology officer
1426 on such matters as information technology project management
1427 policies, standards, accountability measures, and services that
1428 promote project governance and standardization across the
1429 enterprise.

1430 (b) At a minimum, the state chief technology officer shall
1431 consult with the workgroup on a quarterly basis with regard to
1432 executing the duties and responsibilities of the state agencies
1433 related to project management and oversight.

1434 (7) ENTERPRISE INFORMATION TECHNOLOGY CONTRACT MANAGEMENT
1435 WORKGROUP.—

1436 (a) The enterprise information technology contract
1437 management workgroup, composed of information technology
1438 contract manager representatives from all state agencies, shall
1439 consider and make recommendations to the state chief technology
1440 officer on such matters as information technology contract
1441 management policies and standards that promote best practices
1442 for vendor oversight, risk management and compliance, and
1443 performance monitoring and reporting across the enterprise.

1444 (b) At a minimum, the state chief technology officer shall
1445 consult with the workgroup on a quarterly basis with regard to
1446 executing the duties and responsibilities of the state agencies
1447 related to contract management and vendor accountability.

1448 (8) ENTERPRISE INFORMATION TECHNOLOGY PURCHASING
1449 WORKGROUP.—

1450 (a) The enterprise information technology purchasing

576-02447-25

20257026pb

1451 workgroup, composed of information technology procurement
1452 representatives from all state agencies, shall consider and make
1453 recommendations to the state chief technology procurement
1454 officer on such matters as information technology procurement
1455 policies, standards, and purchasing strategy and optimization
1456 that promote best practices for contract negotiation,
1457 consolidation, and effective service-level agreement
1458 implementation across the enterprise.

1459 (b) At a minimum, the state chief technology procurement
1460 officer shall consult with the workgroup on a quarterly basis
1461 with regard to executing the duties and responsibilities of the
1462 state agencies related to technology evaluation, purchasing, and
1463 cost savings.

1464 Section 14. Effective July 1, 2026, section 282.0063,
1465 Florida Statutes, is created to read:

1466 282.0063 State information technology professionals career
1467 paths and training.-

1468 (1) ASSET shall develop standardized frameworks for, and
1469 career paths, progressions, and training programs for, the
1470 benefit of state agency information technology personnel. To
1471 meet that goal, ASSET shall:

1472 (a) Assess current and future information technology
1473 workforce needs across state agencies, identifying skill gaps
1474 and developing strategies to address them.

1475 (b) Develop and establish a training program for state
1476 agencies to support the understanding and implementation of each
1477 element of the enterprise architecture.

1478 (c) Establish training programs, certifications, and
1479 continuing education opportunities to enhance information

576-02447-25

20257026pb

1480 technology competencies, including cybersecurity, cloud
1481 computing, and emerging technologies.

1482 (d) Support initiatives to upskill existing employees in
1483 emerging technologies and automation, ensuring state agencies
1484 remain competitive and innovative.

1485 (e) Develop strategies to recruit and retain information
1486 technology professionals, including internship programs,
1487 partnerships with educational institutions, scholarships for
1488 service, and initiatives to attract diverse talent.

1489 (2) ASSET shall consult with CareerSource Florida, Inc.,
1490 the Department of Commerce, and the Department of Education in
1491 the implementation of this section.

1492 (3) Specifically, in consultation with the Division of
1493 State Human Resource Management in the Department of Management
1494 Services, ASSET shall:

1495 (a) Define career progression frameworks for information
1496 technology personnel, for supporting leadership development, and
1497 for providing mentorship programs.

1498 (b) Establish guidelines and best practices for information
1499 technology professional development and performance management
1500 across state agencies.

1501 Section 15. Effective July 1, 2026, section 282.0064,
1502 Florida Statutes, is created to read:

1503 282.0064 Information technology contract policy.-

1504 (1) In coordination with the Department of Management
1505 Services, ASSET shall establish a policy for all information
1506 technology-related solicitations and contracts, including state
1507 term contracts; contracts sourced using alternative purchasing
1508 methods as authorized pursuant to s. 287.042(16); sole source

576-02447-25

20257026pb

1509 and emergency procurements; and contracts for commodities,
1510 consultant services, and staff augmentation services.

1511 (2) Related to state term contracts, the information
1512 technology policy must include:

1513 (a) Identification of the information technology product
1514 and service categories to be included in state term contracts.

1515 (b) The term of each information technology-related state
1516 term contract.

1517 (c) The maximum number of vendors authorized on each state
1518 term contract.

1519 (3) For all contracts, the information technology policy
1520 must include:

1521 (a) Evaluation criteria for the award of information
1522 technology-related contracts.

1523 (b) Requirements to be included in solicitations.

1524 (c) At a minimum, a requirement that any contract for
1525 information technology commodities or services must meet the
1526 requirements of the enterprise architecture and National
1527 Institute of Standards and Technology Cybersecurity Framework.

1528 (4) The policy must include the following requirements for
1529 any information technology project that requires project
1530 oversight through independent verification and validation:

1531 (a) An entity providing independent verification and
1532 validation may not have any:

1533 1. Technical, managerial, or financial interest in the
1534 project; or

1535 2. Responsibility for or participation in any other aspect
1536 of the project.

1537 (b) The primary objective of independent verification and

576-02447-25

20257026pb

1538 validation must be to provide an objective assessment throughout
1539 the entire project life cycle, reporting directly to all
1540 relevant stakeholders. An independent verification and
1541 validation entity shall independently verify and validate
1542 whether:

1543 1. The project is being built and implemented in accordance
1544 with defined technical architecture, specifications, and
1545 requirements.

1546 2. The project is adhering to established project
1547 management processes.

1548 3. The procurement of products, tools, and services and
1549 resulting contracts align with current statutory and regulatory
1550 requirements.

1551 4. The value of services delivered is commensurate with
1552 project costs.

1553 5. The completed project meets the actual needs of the
1554 intended users.

1555 (c) The entity performing independent verification and
1556 validation shall provide regular reports and assessments
1557 directly to the designated oversight body, identifying risks,
1558 deficiencies, and recommendations for corrective actions to
1559 ensure project success and compliance with statutory
1560 requirements.

1561 (5) The Division of State Purchasing in the Department of
1562 Management Services shall coordinate with ASSET on state term
1563 contract solicitations and invitations to negotiate related to
1564 information technology. ASSET shall evaluate vendor responses
1565 and answer vendor questions on such solicitations or invitations
1566 to negotiate.

576-02447-25

20257026pb

1567 Section 16. Effective July 1, 2026, section 282.0065,
1568 Florida Statutes, is created to read:

1569 282.0065 ASSET information technology test laboratory.-

1570 (1) Beginning July 1, 2027, or after all elements of the
1571 enterprise architecture are published, whichever is later, and
1572 subject to specific appropriation, ASSET shall establish,
1573 maintain, and manage an information technology test laboratory
1574 to support state agencies in evaluating information technology
1575 services, software, and tools before procurement and
1576 implementation.

1577 (2) The purpose of the information technology test
1578 laboratory is to:

1579 (a) Serve as an independent environment for state agencies
1580 to develop, test, and refine proofs of concept for information
1581 technology solutions to assess functionality, security,
1582 interoperability, and performance; and

1583 (b) Assist state agencies in defining and improving
1584 procurement requirements based on real-world testing and
1585 evaluation.

1586 (3) ASSET shall:

1587 (a) Operate and maintain the test laboratory and ensure
1588 that it remains fully operational with the necessary
1589 infrastructure, resources, and security controls to support
1590 state agency testing activities.

1591 (b) Facilitate proofs of concept for state agencies by
1592 providing the agencies with controlled environments to assess
1593 emerging technologies, validate vendor claims, and conduct
1594 comparative evaluations of information technology solutions.

1595 (c) Support the development of requirements for state

576-02447-25

20257026pb

1596 agency information technology projects by assisting state
1597 agencies in refining technical specifications, performance
1598 benchmarks, and security requirements prior to issuing
1599 procurement solicitations.

1600 (d) Ensure the security and compliance of the test
1601 laboratory by implementing safeguards to protect sensitive data,
1602 ensure compliance with applicable laws, and prevent unauthorized
1603 access to testing environments.

1604 (e) Provide access to emerging technologies by partnering
1605 with industry and research institutions to ensure that state
1606 agencies have the opportunity to evaluate the latest information
1607 technology innovations relevant to government operations.

1608 (f) Enter into partnerships with public and private
1609 entities to support the information technology test laboratory's
1610 operations, provided that such partnerships comply with
1611 conflict-of-interest policies and procurement regulations.

1612 (g) Establish policies, procedures, and eligibility
1613 criteria for state agencies to access and use the lab.

1614 Section 17. Section 282.0066, Florida Statutes, is created
1615 to read:

1616 282.0066 Enterprise Information Technology Library.—

1617 (1) ASSET shall develop, implement, and maintain a library
1618 to serve as the official repository for all enterprise
1619 information technology policies, standards, guidelines, and best
1620 practices applicable to state agencies. The library must be
1621 online and accessible by all state agencies through a secure
1622 authentication system.

1623 (2) In developing the library, ASSET shall create a
1624 structured index and search functionality to facilitate

576-02447-25

20257026pb

1625 efficient retrieval of information and maintain version control
1626 and revision history for all published documents.

1627 (3) The library must include standardized checklists
1628 organized by technical subject areas to assist state agencies in
1629 measuring compliance with the information technology policies,
1630 standards, guidelines, and best practices.

1631 (4) ASSET shall establish procedures to ensure the
1632 integrity, security, and availability of the library, including
1633 appropriate access controls, encryption, and disaster recovery
1634 measures. ASSET must regularly update documents and materials of
1635 the library to reflect current state and federal requirements,
1636 industry best practices, and emerging technologies.

1637 (5) (a) All state agencies shall reference and adhere to the
1638 policies, standards, guidelines, and best practices contained in
1639 the online library in information technology planning,
1640 procurement, implementation, and operations. ASSET shall create
1641 mechanisms for state agencies to submit feedback, request
1642 clarifications, and recommend updates.

1643 (b)1. A state agency may request an exemption to a specific
1644 policy, standard, or guideline when compliance is not
1645 technically feasible, would cause undue hardship, or conflicts
1646 with agency specific statutory requirements. The state agency
1647 requesting an exception must submit a formal justification to
1648 ASSET detailing all of the following:

1649 a. The specific requirement for which an exemption is
1650 sought.

1651 b. The reason compliance is not feasible or practical.

1652 c. Any compensating controls or alternative measures the
1653 state agency will implement to mitigate associated risks.

576-02447-25

20257026pb

1654 d. The anticipated duration of the exemption.

1655 2. ASSET shall review all exemption requests and provide a
1656 recommendation to the state chief information officer who shall
1657 present the compliance exemption requests to the chief
1658 information officer workgroup. Approval of exemption requests
1659 must be made by a majority vote of the workgroup. Approved
1660 exemptions must be documented, including conditions and
1661 expiration dates.

1662 3. A state agency with an approved exemption must undergo
1663 periodic review to determine whether the exemption remains
1664 necessary or if compliance can be achieved.

1665 Section 18. Paragraphs (b), (c), (g), (h), and (i) of
1666 subsection (3) and paragraphs (b), (c), (d), and (j) of
1667 subsection (4) of section 282.318, Florida Statutes, are amended
1668 to read:

1669 282.318 Cybersecurity.—

1670 (3) The department, acting through the Florida Digital
1671 Service, is the lead entity responsible for establishing
1672 standards and processes for assessing state agency cybersecurity
1673 risks and determining appropriate security measures. Such
1674 standards and processes must be consistent with generally
1675 accepted technology best practices, including the National
1676 Institute for Standards and Technology Cybersecurity Framework,
1677 for cybersecurity. The department, acting through the Florida
1678 Digital Service, shall adopt rules that mitigate risks;
1679 safeguard state agency digital assets, data, information, and
1680 information technology resources to ensure availability,
1681 confidentiality, and integrity; and support a security
1682 governance framework. The department, acting through the Florida

576-02447-25

20257026pb

1683 Digital Service, shall also:

1684 (b) ~~Develop, and annually update by February 1, a statewide~~
1685 ~~cybersecurity strategic plan that includes security goals and~~
1686 ~~objectives for cybersecurity, including the identification and~~
1687 ~~mitigation of risk, proactive protections against threats,~~
1688 ~~tactical risk detection, threat reporting, and response and~~
1689 ~~recovery protocols for a cyber incident.~~

1690 (c) ~~Develop and publish for use by state agencies a~~
1691 ~~cybersecurity governance framework that, at a minimum, includes~~
1692 ~~guidelines and processes for:~~

1693 1. ~~Establishing asset management procedures to ensure that~~
1694 ~~an agency's information technology resources are identified and~~
1695 ~~managed consistent with their relative importance to the~~
1696 ~~agency's business objectives.~~

1697 2. ~~Using a standard risk assessment methodology that~~
1698 ~~includes the identification of an agency's priorities,~~
1699 ~~constraints, risk tolerances, and assumptions necessary to~~
1700 ~~support operational risk decisions.~~

1701 3. ~~Completing comprehensive risk assessments and~~
1702 ~~cybersecurity audits, which may be completed by a private sector~~
1703 ~~vendor, and submitting completed assessments and audits to the~~
1704 ~~department.~~

1705 4. ~~Identifying protection procedures to manage the~~
1706 ~~protection of an agency's information, data, and information~~
1707 ~~technology resources.~~

1708 5. ~~Establishing procedures for accessing information and~~
1709 ~~data to ensure the confidentiality, integrity, and availability~~
1710 ~~of such information and data.~~

1711 6. ~~Detecting threats through proactive monitoring of~~

576-02447-25

20257026pb

1712 ~~events, continuous security monitoring, and defined detection~~
1713 ~~processes.~~

1714 ~~7. Establishing agency cybersecurity incident response~~
1715 ~~teams and describing their responsibilities for responding to~~
1716 ~~cybersecurity incidents, including breaches of personal~~
1717 ~~information containing confidential or exempt data.~~

1718 ~~8. Recovering information and data in response to a~~
1719 ~~cybersecurity incident. The recovery may include recommended~~
1720 ~~improvements to the agency processes, policies, or guidelines.~~

1721 ~~9. Establishing a cybersecurity incident reporting process~~
1722 ~~that includes procedures for notifying the department and the~~
1723 ~~Department of Law Enforcement of cybersecurity incidents.~~

1724 a. The level of severity of the cybersecurity incident is
1725 defined by the National Cyber Incident Response Plan of the
1726 United States Department of Homeland Security as follows:

1727 (I) Level 5 is an emergency-level incident within the
1728 specified jurisdiction that poses an imminent threat to the
1729 provision of wide-scale critical infrastructure services;
1730 national, state, or local government security; or the lives of
1731 the country's, state's, or local government's residents.

1732 (II) Level 4 is a severe-level incident that is likely to
1733 result in a significant impact in the affected jurisdiction to
1734 public health or safety; national, state, or local security;
1735 economic security; or civil liberties.

1736 (III) Level 3 is a high-level incident that is likely to
1737 result in a demonstrable impact in the affected jurisdiction to
1738 public health or safety; national, state, or local security;
1739 economic security; civil liberties; or public confidence.

1740 (IV) Level 2 is a medium-level incident that may impact

576-02447-25

20257026pb

1741 public health or safety; national, state, or local security;
1742 economic security; civil liberties; or public confidence.

1743 (V) Level 1 is a low-level incident that is unlikely to
1744 impact public health or safety; national, state, or local
1745 security; economic security; civil liberties; or public
1746 confidence.

1747 b. The cybersecurity incident reporting process must
1748 specify the information that must be reported by a state agency
1749 following a cybersecurity incident or ransomware incident,
1750 which, at a minimum, must include the following:

1751 (I) A summary of the facts surrounding the cybersecurity
1752 incident or ransomware incident.

1753 (II) The date on which the state agency most recently
1754 backed up its data; the physical location of the backup, if the
1755 backup was affected; and if the backup was created using cloud
1756 computing.

1757 (III) The types of data compromised by the cybersecurity
1758 incident or ransomware incident.

1759 (IV) The estimated fiscal impact of the cybersecurity
1760 incident or ransomware incident.

1761 (V) In the case of a ransomware incident, the details of
1762 the ransom demanded.

1763 c.(I) A state agency shall report all ransomware incidents
1764 and any cybersecurity incident determined by the state agency to
1765 be of severity level 3, 4, or 5 to the state chief information
1766 security officer ~~Cybersecurity Operations Center~~ and the
1767 Cybercrime Office of the Department of Law Enforcement as soon
1768 as possible but no later than 48 hours after discovery of the
1769 cybersecurity incident and no later than 12 hours after

576-02447-25

20257026pb

1770 discovery of the ransomware incident. The report must contain
1771 the information required in sub-subparagraph b.

1772 (II) The state chief information security officer
1773 ~~Cybersecurity Operations Center~~ shall notify the President of
1774 the Senate and the Speaker of the House of Representatives of
1775 any severity level 3, 4, or 5 incident as soon as possible but
1776 no later than 12 hours after receiving a state agency's incident
1777 report. The notification must include a high-level description
1778 of the incident and the likely effects.

1779 d. A state agency shall report a cybersecurity incident
1780 determined by the state agency to be of severity level 1 or 2 to
1781 the state chief information security officer ~~Cybersecurity~~
1782 ~~Operations Center~~ and the Cybercrime Office of the Department of
1783 Law Enforcement as soon as possible, but no later than 96 hours
1784 after the discovery of the cybersecurity incident and no later
1785 than 72 hours after the discovery of the ransomware incident.
1786 The report must contain the information required in sub-
1787 subparagraph b.

1788 e. The state chief information security officer
1789 ~~Cybersecurity Operations Center~~ shall provide a consolidated
1790 incident report on a quarterly basis to the President of the
1791 Senate and, the Speaker of the House of Representatives, ~~and the~~
1792 ~~Florida Cybersecurity Advisory Council. The report provided to~~
1793 ~~the Florida Cybersecurity Advisory Council may not contain the~~
1794 ~~name of any agency, network information, or system identifying~~
1795 ~~information but must contain sufficient relevant information to~~
1796 ~~allow the Florida Cybersecurity Advisory Council to fulfill its~~
1797 ~~responsibilities as required in s. 282.319(9).~~

1798 2.10. Incorporating information obtained through detection

576-02447-25

20257026pb

1799 and response activities into the agency's cybersecurity incident
1800 response plans.

1801 3.11. Developing agency strategic and operational
1802 cybersecurity plans required pursuant to this section.

1803 4.12. Establishing the managerial, operational, and
1804 technical safeguards for protecting state government data and
1805 information technology resources that align with the state
1806 agency risk management strategy and that protect the
1807 confidentiality, integrity, and availability of information and
1808 data.

1809 ~~13. Establishing procedures for procuring information
1810 technology commodities and services that require the commodity
1811 or service to meet the National Institute of Standards and
1812 Technology Cybersecurity Framework.~~

1813 5.14. Submitting after-action reports following a
1814 cybersecurity incident or ransomware incident. Such guidelines
1815 and processes for submitting after-action reports must be
1816 developed and published by December 1, 2022.

1817 (f)(g) Annually provide cybersecurity training to all state
1818 agency technology professionals and employees with access to
1819 highly sensitive information which develops, assesses, and
1820 documents competencies by role and skill level. The
1821 cybersecurity training curriculum must include training on the
1822 identification of each cybersecurity incident severity level
1823 referenced in sub-subparagraph (b)1.a. ~~(e)9.a.~~ The training may
1824 be provided in collaboration with the Cybercrime Office of the
1825 Department of Law Enforcement, a private sector entity, or an
1826 institution of the State University System.

1827 ~~(h) Operate and maintain a Cybersecurity Operations Center~~

576-02447-25

20257026pb

1828 ~~led by the state chief information security officer, which must~~
1829 ~~be primarily virtual and staffed with tactical detection and~~
1830 ~~incident response personnel. The Cybersecurity Operations Center~~
1831 ~~shall serve as a clearinghouse for threat information and~~
1832 ~~coordinate with the Department of Law Enforcement to support~~
1833 ~~state agencies and their response to any confirmed or suspected~~
1834 ~~cybersecurity incident.~~

1835 ~~(i) Lead an Emergency Support Function, ESF CYBER, under~~
1836 ~~the state comprehensive emergency management plan as described~~
1837 ~~in s. 252.35.~~

1838 (4) Each state agency head shall, at a minimum:

1839 (b) In consultation with the department, through the
1840 Florida Digital Service, and the Cybercrime Office of the
1841 Department of Law Enforcement, establish an agency cybersecurity
1842 response team to respond to a cybersecurity incident. The agency
1843 cybersecurity response team shall convene upon notification of a
1844 cybersecurity incident and must immediately report all confirmed
1845 or suspected incidents to the state chief information security
1846 officer, or his or her designee, and comply with all applicable
1847 guidelines and processes established pursuant to paragraph

1848 (3) (b) ~~(3) (c)~~.

1849 (c) Submit to the state chief information security officer
1850 ~~department~~ annually by July 31, the state agency's strategic and
1851 operational cybersecurity plans developed pursuant to rules and
1852 guidelines established by the state chief information security
1853 officer ~~department, through the Florida Digital Service.~~

1854 1. The state agency strategic cybersecurity plan must cover
1855 a 2-year ~~3-year~~ period and, at a minimum, define security goals,
1856 intermediate objectives, and projected agency costs for the

576-02447-25

20257026pb

1857 strategic issues of agency information security policy, risk
1858 management, security training, security incident response, and
1859 disaster recovery. The plan must be based on the statewide
1860 cybersecurity strategic plan created by the state chief
1861 information security officer ~~department~~ and include performance
1862 metrics that can be objectively measured to reflect the status
1863 of the state agency's progress in meeting security goals and
1864 objectives identified in the agency's strategic information
1865 security plan.

1866 2. The state agency operational cybersecurity plan must
1867 include a set of measures that objectively assesses the
1868 performance of the agency's cybersecurity program in accordance
1869 with its risk management plan ~~progress report that objectively~~
1870 ~~measures progress made towards the prior operational~~
1871 ~~cybersecurity plan and a project plan that includes activities,~~
1872 ~~timelines, and deliverables for security objectives that the~~
1873 ~~state agency will implement during the current fiscal year.~~

1874 (d) Conduct, and update every 2 ~~3~~ years, a comprehensive
1875 risk assessment, which may be completed by a private sector
1876 vendor, to determine the security threats to the data,
1877 information, and information technology resources, including
1878 mobile devices and print environments, of the agency. The risk
1879 assessment must comply with the risk assessment methodology
1880 developed by the state chief information security officer
1881 ~~department~~ and is confidential and exempt from s. 119.07(1),
1882 except that such information shall be available to the Auditor
1883 General, the state chief information security officer ~~Florida~~
1884 ~~Digital Service within the department~~, the Cybercrime Office of
1885 the Department of Law Enforcement, and, for state agencies under

576-02447-25

20257026pb

1886 the jurisdiction of the Governor, the Chief Inspector General.
1887 If a private sector vendor is used to complete a comprehensive
1888 risk assessment, it must attest to the validity of the risk
1889 assessment findings. The comprehensive risk assessment must
1890 include all of the following:

1891 1. The results of vulnerability and penetration tests on
1892 any Internet website or mobile application that processes any
1893 sensitive personal information or confidential information and a
1894 plan to address any vulnerability identified in the tests.

1895 2. A written acknowledgment that the executive director or
1896 the secretary of the agency, the chief financial officer of the
1897 agency, and each executive manager as designated by the state
1898 agency have been made aware of the risks revealed during the
1899 preparation of the agency's operations cybersecurity plan and
1900 the comprehensive risk assessment.

1901 (j) Develop a process for detecting, reporting, and
1902 responding to threats, breaches, or cybersecurity incidents
1903 which is consistent with the security rules, guidelines, and
1904 processes established by the department through the Florida
1905 Digital Service.

1906 1. All cybersecurity incidents and ransomware incidents
1907 must be reported by state agencies. Such reports must comply
1908 with the notification procedures and reporting timeframes
1909 established pursuant to paragraph (3) (b) ~~(3) (e)~~.

1910 2. For cybersecurity breaches, state agencies shall provide
1911 notice in accordance with s. 501.171.

1912 Section 19. Effective July 1, 2026, subsections (2), (3),
1913 (4), (7), and (10) of section 282.318, Florida Statutes, as
1914 amended by this act, are amended to read:

576-02447-25

20257026pb

1915 282.318 Cybersecurity.—

1916 (2) As used in this section, the term "state agency" has
1917 the same meaning as provided in s. 282.0041, ~~except that the~~
1918 ~~term includes the Department of Legal Affairs, the Department of~~
1919 ~~Agriculture and Consumer Services, and the Department of~~
1920 ~~Financial Services.~~

1921 (3) ASSET ~~The department, acting through the Florida~~
1922 ~~Digital Service,~~ is the lead entity responsible for establishing
1923 enterprise technology and cybersecurity standards and processes
1924 for assessing state agency cybersecurity risks and determining
1925 appropriate security measures that comply with all national and
1926 state data compliance security standards. Such standards and
1927 processes must be consistent with generally accepted technology
1928 best practices, including the National Institute for Standards
1929 and Technology Cybersecurity Framework, for cybersecurity. ASSET
1930 ~~The department, acting through the Florida Digital Service,~~
1931 shall adopt rules that mitigate risks; safeguard state agency
1932 digital assets, data, information, and information technology
1933 resources to ensure availability, confidentiality, and
1934 integrity; and support a security governance framework. ASSET
1935 ~~The department, acting through the Florida Digital Service,~~
1936 shall also:

1937 (a) Designate an employee ~~of the Florida Digital Service~~ as
1938 the state chief information security officer. The state chief
1939 information security officer must have experience and expertise
1940 in security and risk management for communications and
1941 information technology resources. The state chief information
1942 security officer is responsible for the development of
1943 enterprise cybersecurity policy, standards, operation, and

576-02447-25

20257026pb

1944 security architecture oversight ~~of cybersecurity~~ for state
1945 technology systems. The state chief information security officer
1946 shall be notified of all confirmed or suspected incidents or
1947 threats of state agency information technology resources and
1948 must report such incidents or threats to the state chief
1949 information officer ~~and the Governor~~.

1950 (b) Develop, and annually update by February 1, a statewide
1951 cybersecurity strategic plan that includes security goals and
1952 objectives for cybersecurity, including the identification and
1953 mitigation of risk, proactive protections against threats,
1954 tactical risk detection, threat reporting, and response and
1955 recovery protocols for a cyber incident.

1956 (c) ~~(b)~~ Develop and publish for use by state agencies a
1957 cybersecurity governance framework that, at a minimum, includes
1958 guidelines and processes for:

1959 1. Establishing asset management procedures to ensure that
1960 an agency's information technology resources are identified and
1961 managed consistently with their relative importance to the
1962 agency's business objectives.

1963 2. Using a standard risk assessment methodology that
1964 includes the identification of an agency's priorities,
1965 constraints, risk tolerances, and assumptions necessary to
1966 support operational risk decisions.

1967 3. Completing comprehensive risk assessments and
1968 cybersecurity audits, which may be completed by a private sector
1969 vendor, and submitting completed assessments and audits to the
1970 department.

1971 4. Identifying protection procedures to manage the
1972 protection of an agency's information, data, and information

576-02447-25

20257026pb

1973 technology resources.

1974 5. Establishing procedures for accessing information and
1975 data to ensure the confidentiality, integrity, and availability
1976 of such information and data.

1977 6. Detecting threats through proactive monitoring of
1978 events, continuous security monitoring, and defined detection
1979 processes.

1980 7. Establishing agency cybersecurity incident response
1981 teams and describing their responsibilities for responding to
1982 cybersecurity incidents, including breaches of personal
1983 information containing confidential or exempt data.

1984 8. Recovering information and data in response to a
1985 cybersecurity incident. The recovery may include recommended
1986 improvements to the agency processes, policies, or guidelines.

1987 9. Establishing a cybersecurity incident reporting process
1988 that includes procedures for notifying ASSET ~~the department~~ and
1989 the Department of Law Enforcement of cybersecurity incidents.

1990 a. The level of severity of the cybersecurity incident is
1991 defined by the National Cyber Incident Response Plan of the
1992 United States Department of Homeland Security as follows:

1993 (I) Level 5 is an emergency-level incident within the
1994 specified jurisdiction that poses an imminent threat to the
1995 provision of wide-scale critical infrastructure services;
1996 national, state, or local government security; or the lives of
1997 the country's, state's, or local government's residents.

1998 (II) Level 4 is a severe-level incident that is likely to
1999 result in a significant impact in the affected jurisdiction to
2000 public health or safety; national, state, or local security;
2001 economic security; or civil liberties.

576-02447-25

20257026pb

2002 (III) Level 3 is a high-level incident that is likely to
2003 result in a demonstrable impact in the affected jurisdiction to
2004 public health or safety; national, state, or local security;
2005 economic security; civil liberties; or public confidence.

2006 (IV) Level 2 is a medium-level incident that may impact
2007 public health or safety; national, state, or local security;
2008 economic security; civil liberties; or public confidence.

2009 (V) Level 1 is a low-level incident that is unlikely to
2010 impact public health or safety; national, state, or local
2011 security; economic security; civil liberties; or public
2012 confidence.

2013 b. The cybersecurity incident reporting process must
2014 specify the information that must be reported by a state agency
2015 following a cybersecurity incident or ransomware incident,
2016 which, at a minimum, must include the following:

2017 (I) A summary of the facts surrounding the cybersecurity
2018 incident or ransomware incident.

2019 (II) The date on which the state agency most recently
2020 backed up its data; the physical location of the backup, if the
2021 backup was affected; and if the backup was created using cloud
2022 computing.

2023 (III) The types of data compromised by the cybersecurity
2024 incident or ransomware incident.

2025 (IV) The estimated fiscal impact of the cybersecurity
2026 incident or ransomware incident.

2027 (V) In the case of a ransomware incident, the details of
2028 the ransom demanded.

2029 c.(I) A state agency shall report all ransomware incidents
2030 and any cybersecurity incident determined by the state agency to

576-02447-25

20257026pb

2031 be of severity level 3, 4, or 5 to the state chief information
2032 security officer and the Cybercrime Office of the Department of
2033 Law Enforcement as soon as possible but no later than 48 hours
2034 after discovery of the cybersecurity incident and no later than
2035 12 hours after discovery of the ransomware incident. The report
2036 must contain the information required in sub-subparagraph b.

2037 (II) The state chief information security officer shall
2038 notify the President of the Senate and the Speaker of the House
2039 of Representatives of any severity level 3, 4, or 5 incident as
2040 soon as possible but no later than 12 hours after receiving a
2041 state agency's incident report. The notification must include a
2042 high-level description of the incident and the likely effects.

2043 d. A state agency shall report a cybersecurity incident
2044 determined by the state agency to be of severity level 1 or 2 to
2045 the state chief information security officer and the Cybercrime
2046 Office of the Department of Law Enforcement as soon as possible,
2047 but no later than 96 hours after the discovery of the
2048 cybersecurity incident and no later than 72 hours after the
2049 discovery of the ransomware incident. The report must contain
2050 the information required in sub-subparagraph b.

2051 e. The state chief information security officer shall
2052 provide a consolidated incident report on a quarterly basis to
2053 the Executive office of the Governor, the Commissioner of
2054 Agriculture, the Chief Financial Officer, the Attorney General,
2055 the President of the Senate, and the Speaker of the House of
2056 Representatives.

2057 10.2- Incorporating information obtained through detection
2058 and response activities into the agency's cybersecurity incident
2059 response plans.

576-02447-25

20257026pb

2060 ~~11.3.~~ Developing agency strategic and operational
2061 cybersecurity plans required pursuant to this section.

2062 ~~12.4.~~ Establishing the managerial, operational, and
2063 technical safeguards for protecting state government data and
2064 information technology resources that align with the state
2065 agency risk management strategy and that protect the
2066 confidentiality, integrity, and availability of information and
2067 data.

2068 13. In coordination with the state chief information
2069 technology procurement officer, establishing procedures for
2070 procuring information technology commodities and services that
2071 require the commodity or service to meet the National Institute
2072 of Standards and Technology Cybersecurity Framework.

2073 ~~14.5.~~ Submitting after-action reports following a
2074 cybersecurity incident or ransomware incident. Such guidelines
2075 and processes for submitting after-action reports must be
2076 developed and published by July 1, 2027 ~~December 1, 2022~~.

2077 ~~(d)-(e)~~ Assist state agencies in complying with this
2078 section.

2079 ~~(e)-(d)~~ In collaboration with the Cybercrime Office of the
2080 Department of Law Enforcement and through the state chief
2081 information security officer and the Division of Enterprise
2082 Information Technology Workforce Development, annually provide
2083 training for state agency information security managers and
2084 computer security incident response team members that contains
2085 training on cybersecurity, including cybersecurity threats,
2086 trends, and best practices.

2087 ~~(f)-(e)~~ Annually review the strategic and operational
2088 cybersecurity plans of state agencies.

576-02447-25

20257026pb

2089 (g) ~~(f)~~ Annually provide cybersecurity training through the
2090 state chief information security officer and the Division of
2091 Enterprise Information Technology Workforce Development to all
2092 state agency technology professionals and employees with access
2093 to highly sensitive information which develops, assesses, and
2094 documents competencies by role and skill level. The
2095 cybersecurity training curriculum must include training on the
2096 identification of each cybersecurity incident severity level
2097 referenced in sub-subparagraph (c)9.a. ~~(b)1.a.~~ The training may
2098 be provided in collaboration with the Cybercrime Office of the
2099 Department of Law Enforcement, a private sector entity, or an
2100 institution of the State University System.

2101 (4) Each state agency head shall, at a minimum:

2102 (a) Designate an information security manager to administer
2103 the cybersecurity program of the state agency. This designation
2104 must be provided annually in writing to ASSET ~~the department~~ by
2105 January 1. A state agency's information security manager, for
2106 purposes of these information security duties, shall report
2107 directly to the agency head.

2108 (b) In consultation with the state chief information
2109 security officer ~~department,~~ ~~through the Florida Digital~~
2110 ~~Service,~~ and the Cybercrime Office of the Department of Law
2111 Enforcement, establish an agency cybersecurity response team to
2112 respond to a cybersecurity incident. The agency cybersecurity
2113 response team shall convene upon notification of a cybersecurity
2114 incident and must immediately report all confirmed or suspected
2115 incidents to the state chief information security officer, or
2116 his or her designee, and comply with all applicable guidelines
2117 and processes established pursuant to paragraph (3)(c) ~~(3)(b)~~.

576-02447-25

20257026pb

2118 (c) Submit to state chief information security officer
2119 annually by July 31 the state agency's strategic and operational
2120 cybersecurity plans developed pursuant to rules and guidelines
2121 established by the state chief information security officer.

2122 1. The state agency strategic cybersecurity plan must cover
2123 a 2-year period and, at a minimum, define security goals,
2124 intermediate objectives, and projected agency costs for the
2125 strategic issues of agency information security policy, risk
2126 management, security training, security incident response, and
2127 disaster recovery. The plan must be based on the statewide
2128 cybersecurity strategic plan created by the state chief
2129 information security officer and include performance metrics
2130 that can be objectively measured to reflect the status of the
2131 state agency's progress in meeting security goals and objectives
2132 identified in the agency's strategic information security plan.

2133 2. The state agency operational cybersecurity plan must
2134 include a set of measures that objectively assess the
2135 performance of the agency's cybersecurity program in accordance
2136 with its risk management plan.

2137 (d) Conduct, and update every 2 years, a comprehensive risk
2138 assessment, which may be completed by a private sector vendor,
2139 to determine the security threats to the data, information, and
2140 information technology resources, including mobile devices and
2141 print environments, of the agency. The risk assessment must
2142 comply with the risk assessment methodology developed by the
2143 state chief information security officer and is confidential and
2144 exempt from s. 119.07(1), except that such information shall be
2145 available to the Auditor General, the state chief information
2146 security officer, the Cybercrime Office of the Department of Law

576-02447-25

20257026pb

2147 Enforcement, and, for state agencies under the jurisdiction of
2148 the Governor, the Chief Inspector General. If a private sector
2149 vendor is used to complete a comprehensive risk assessment, it
2150 must attest to the validity of the risk assessment findings. The
2151 comprehensive risk assessment must include all of the following:

2152 1. The results of vulnerability and penetration tests on
2153 any Internet website or mobile application that processes any
2154 sensitive personal information or confidential information and a
2155 plan to address any vulnerability identified in the tests.

2156 2. A written acknowledgment that the executive director or
2157 secretary of the agency, the chief financial officer of the
2158 agency, and each executive manager as designated by the state
2159 agency have been made aware of the risks revealed during the
2160 preparation of the agency's operational cybersecurity plan and
2161 the comprehensive risk assessment.

2162 (e) Develop, and periodically update, written internal
2163 policies and procedures, which include procedures for reporting
2164 cybersecurity incidents and breaches to the Cybercrime Office of
2165 the Department of Law Enforcement and the state chief
2166 information security officer ~~Florida Digital Service within the~~
2167 ~~department~~. Such policies and procedures must be consistent with
2168 the rules, guidelines, and processes established by ASSET ~~the~~
2169 ~~department~~ to ensure the security of the data, information, and
2170 information technology resources of the agency. The internal
2171 policies and procedures that, if disclosed, could facilitate the
2172 unauthorized modification, disclosure, or destruction of data or
2173 information technology resources are confidential information
2174 and exempt from s. 119.07(1), except that such information shall
2175 be available to the Auditor General, the Cybercrime Office of

576-02447-25

20257026pb

2176 the Department of Law Enforcement, the state chief information
2177 security officer ~~the Florida Digital Service within the~~
2178 ~~department~~, and, for state agencies under the jurisdiction of
2179 the Governor, the Chief Inspector General.

2180 (f) Implement managerial, operational, and technical
2181 safeguards and risk assessment remediation plans recommended by
2182 ASSET ~~the department~~ to address identified risks to the data,
2183 information, and information technology resources of the agency.
2184 The state chief information security officer ~~department~~, ~~through~~
2185 ~~the Florida Digital Service~~, shall track implementation by state
2186 agencies upon development of such remediation plans in
2187 coordination with agency inspectors general.

2188 (g) Ensure that periodic internal audits and evaluations of
2189 the agency's cybersecurity program for the data, information,
2190 and information technology resources of the agency are
2191 conducted. The results of such audits and evaluations are
2192 confidential information and exempt from s. 119.07(1), except
2193 that such information shall be available to the Auditor General,
2194 the Cybercrime Office of the Department of Law Enforcement, the
2195 state chief information security officer ~~Florida Digital Service~~
2196 ~~within the department~~, and, for agencies under the jurisdiction
2197 of the Governor, the Chief Inspector General.

2198 (h) Ensure that the cybersecurity requirements in the
2199 written specifications for the solicitation, contracts, and
2200 service-level agreement of information technology and
2201 information technology resources and services meet or exceed the
2202 applicable state and federal laws, regulations, and standards
2203 for cybersecurity, including the National Institute of Standards
2204 and Technology Cybersecurity Framework. Service-level agreements

576-02447-25

20257026pb

2205 must identify service provider and state agency responsibilities
2206 for privacy and security, protection of government data,
2207 personnel background screening, and security deliverables with
2208 associated frequencies.

2209 (i) Provide cybersecurity awareness training to all state
2210 agency employees within 30 days after commencing employment, and
2211 annually thereafter, concerning cybersecurity risks and the
2212 responsibility of employees to comply with policies, standards,
2213 guidelines, and operating procedures adopted by the state agency
2214 to reduce those risks. The training may be provided in
2215 collaboration with the Cybercrime Office of the Department of
2216 Law Enforcement, a private sector entity, or an institution of
2217 the State University System.

2218 (j) Develop a process for detecting, reporting, and
2219 responding to threats, breaches, or cybersecurity incidents
2220 which is consistent with the security rules, guidelines, and
2221 processes established by ASSET ~~the department~~ through the state
2222 chief information security officer ~~Florida Digital Service~~.

2223 1. All cybersecurity incidents and ransomware incidents
2224 must be reported by state agencies. Such reports must comply
2225 with the notification procedures and reporting timeframes
2226 established pursuant to paragraph (3) (c) ~~(3) (b)~~.

2227 2. For cybersecurity breaches, state agencies shall provide
2228 notice in accordance with s. 501.171.

2229 (k) Submit to the state chief information security officer
2230 ~~Florida Digital Service~~, within 1 week after the remediation of
2231 a cybersecurity incident or ransomware incident, an after-action
2232 report that summarizes the incident, the incident's resolution,
2233 and any insights gained as a result of the incident.

576-02447-25

20257026pb

2234 (7) The portions of records made confidential and exempt in
2235 subsections (5) and (6) shall be available to the Auditor
2236 General, the Cybercrime Office of the Department of Law
2237 Enforcement, the state chief information security officer, the
2238 Legislature ~~Florida Digital Service within the department~~, and,
2239 for agencies under the jurisdiction of the Governor, the Chief
2240 Inspector General. Such portions of records may be made
2241 available to a local government, another state agency, or a
2242 federal agency for cybersecurity purposes or in furtherance of
2243 the state agency's official duties.

2244 (10) ASSET ~~The department~~ shall adopt rules relating to
2245 cybersecurity and to administer this section.

2246 Section 20. Section 282.3185, Florida Statutes, is amended
2247 to read:

2248 282.3185 Local government cybersecurity.—

2249 (1) SHORT TITLE.—This section may be cited as the "Local
2250 Government Cybersecurity Act."

2251 (2) DEFINITION.—As used in this section, the term "local
2252 government" means any county or municipality.

2253 (3) CYBERSECURITY TRAINING.—

2254 (a) The state chief information security officer ~~Florida~~
2255 ~~Digital Service~~ shall:

2256 1. Develop a basic cybersecurity training curriculum for
2257 local government employees. All local government employees with
2258 access to the local government's network must complete the basic
2259 cybersecurity training within 30 days after commencing
2260 employment and annually thereafter.

2261 2. Develop an advanced cybersecurity training curriculum
2262 for local governments which is consistent with the cybersecurity

576-02447-25

20257026pb

2263 training required under s. 282.318(3)(f) ~~s. 282.318(3)(g)~~. All
2264 local government technology professionals and employees with
2265 access to highly sensitive information must complete the
2266 advanced cybersecurity training within 30 days after commencing
2267 employment and annually thereafter.

2268 (b) The state chief information security officer ~~Florida~~
2269 ~~Digital Service~~ may provide the cybersecurity training required
2270 by this subsection in collaboration with the Cybercrime Office
2271 of the Department of Law Enforcement, a private sector entity,
2272 or an institution of the State University System.

2273 (4) CYBERSECURITY STANDARDS.—

2274 (a) Each local government shall adopt cybersecurity
2275 standards that safeguard its data, information technology, and
2276 information technology resources to ensure availability,
2277 confidentiality, and integrity. The cybersecurity standards must
2278 be consistent with generally accepted best practices for
2279 cybersecurity, including the National Institute of Standards and
2280 Technology Cybersecurity Framework.

2281 (b) Each county with a population of 75,000 or more must
2282 adopt the cybersecurity standards required by this subsection by
2283 January 1, 2024. Each county with a population of less than
2284 75,000 must adopt the cybersecurity standards required by this
2285 subsection by January 1, 2025.

2286 (c) Each municipality with a population of 25,000 or more
2287 must adopt the cybersecurity standards required by this
2288 subsection by January 1, 2024. Each municipality with a
2289 population of less than 25,000 must adopt the cybersecurity
2290 standards required by this subsection by January 1, 2025.

2291 (d) Each local government shall notify the state chief

576-02447-25

20257026pb

2292 information security officer ~~Florida Digital Service~~ of its
2293 compliance with this subsection as soon as possible.

2294 (5) INCIDENT NOTIFICATION.—

2295 (a) A local government shall provide notification of a
2296 cybersecurity incident or ransomware incident to the state chief
2297 information security officer ~~Cybersecurity Operations Center~~,
2298 the Cybercrime Office of the Department of Law Enforcement, and
2299 the sheriff who has jurisdiction over the local government in
2300 accordance with paragraph (b). The notification must include, at
2301 a minimum, the following information:

2302 1. A summary of the facts surrounding the cybersecurity
2303 incident or ransomware incident.

2304 2. The date on which the local government most recently
2305 backed up its data; the physical location of the backup, if the
2306 backup was affected; and if the backup was created using cloud
2307 computing.

2308 3. The types of data compromised by the cybersecurity
2309 incident or ransomware incident.

2310 4. The estimated fiscal impact of the cybersecurity
2311 incident or ransomware incident.

2312 5. In the case of a ransomware incident, the details of the
2313 ransom demanded.

2314 6. A statement requesting or declining assistance from ~~the~~
2315 ~~Cybersecurity Operations Center~~, the Cybercrime Office of the
2316 Department of Law Enforcement, or the sheriff who has
2317 jurisdiction over the local government.

2318 (b)1. A local government shall report all ransomware
2319 incidents and any cybersecurity incident determined by the local
2320 government to be of severity level 3, 4, or 5 as provided in s.

576-02447-25

20257026pb

2321 282.318(3)(b) ~~s. 282.318(3)(e)~~ to the state chief information
2322 security officer ~~Cybersecurity Operations Center~~, the Cybercrime
2323 Office of the Department of Law Enforcement, and the sheriff who
2324 has jurisdiction over the local government as soon as possible
2325 but no later than 12 ~~48~~ hours after discovery of the
2326 cybersecurity incident and no later than 6 ~~12~~ hours after
2327 discovery of the ransomware incident. The report must contain
2328 the information required in paragraph (a).

2329 2. The state chief information security officer
2330 ~~Cybersecurity Operations Center~~ shall notify the state chief
2331 information officer, the Governor, the Commissioner of
2332 Agriculture, the Chief Financial Officer, the Attorney General,
2333 the President of the Senate, and the Speaker of the House of
2334 Representatives of any severity level 3, 4, or 5 incident as
2335 soon as possible but no later than 12 hours after receiving a
2336 local government's incident report. The notification must
2337 include a high-level description of the incident and the likely
2338 effects.

2339 (c) A local government may report a cybersecurity incident
2340 determined by the local government to be of severity level 1 or
2341 2 as provided in s. 282.318(3)(b) ~~s. 282.318(3)(e)~~ to the state
2342 chief information security officer ~~Cybersecurity Operations~~
2343 ~~Center~~, the Cybercrime Office of the Department of Law
2344 Enforcement, and the sheriff who has jurisdiction over the local
2345 government. The report shall contain the information required in
2346 paragraph (a).

2347 (d) The state chief information security officer
2348 ~~Cybersecurity Operations Center~~ shall provide a consolidated
2349 incident report by the 30th day after the end of each quarter ~~on~~

576-02447-25

20257026pb

2350 ~~a quarterly basis to the Governor, the Commissioner of~~
2351 ~~Agriculture, the Chief Financial Officer, the Attorney General,~~
2352 ~~the President of the Senate, and the Speaker of the House of~~
2353 ~~Representatives, and the Florida Cybersecurity Advisory Council.~~
2354 ~~The report provided to the Florida Cybersecurity Advisory~~
2355 ~~Council may not contain the name of any local government,~~
2356 ~~network information, or system identifying information but must~~
2357 ~~contain sufficient relevant information to allow the Florida~~
2358 ~~Cybersecurity Advisory Council to fulfill its responsibilities~~
2359 ~~as required in s. 282.319(9).~~

2360 (6) AFTER-ACTION REPORT.—A local government must submit to
2361 the state chief information security officer Florida Digital
2362 Service, within 1 week after the remediation of a cybersecurity
2363 incident or ransomware incident, an after-action report that
2364 summarizes the incident, the incident's resolution, and any
2365 insights gained as a result of the incident. By December 1, 2027
2366 2022, the state chief information security officer Florida
2367 Digital Service shall establish guidelines and processes for
2368 submitting an after-action report.

2369 Section 21. Effective July 1, 2026, paragraph (a) of
2370 subsection (3) and paragraphs (b) and (c) of subsection (5) of
2371 section 282.3185, Florida Statutes, as amended by this act, are
2372 amended to read:

2373 282.3185 Local government cybersecurity.—

2374 (3) CYBERSECURITY TRAINING.—

2375 (a) The state chief information security officer shall:

2376 1. Develop a basic cybersecurity training curriculum for
2377 local government employees. All local government employees with
2378 access to the local government's network must complete the basic

576-02447-25

20257026pb

2379 cybersecurity training within 30 days after commencing
2380 employment and annually thereafter.

2381 2. Develop an advanced cybersecurity training curriculum
2382 for local governments which is consistent with the cybersecurity
2383 training required under s. 282.318(3)(g) ~~s. 282.318(3)(f)~~. All
2384 local government technology professionals and employees with
2385 access to highly sensitive information must complete the
2386 advanced cybersecurity training within 30 days after commencing
2387 employment and annually thereafter.

2388 (5) INCIDENT NOTIFICATION.—

2389 (b)1. A local government shall report all ransomware
2390 incidents and any cybersecurity incident determined by the local
2391 government to be of severity level 3, 4, or 5 as provided in s.
2392 282.318(3)(c) ~~s. 282.318(3)(b)~~ to the state chief information
2393 security officer, the Cybercrime Office of the Department of Law
2394 Enforcement, and the sheriff who has jurisdiction over the local
2395 government as soon as possible but no later than 12 hours after
2396 discovery of the cybersecurity incident and no later than 6
2397 hours after discovery of the ransomware incident. The report
2398 must contain the information required in paragraph (a).

2399 2. The state chief information security officer shall
2400 notify the state chief information officer, the Governor, the
2401 Commission of Agriculture, the Chief Financial Officer, the
2402 Attorney General, the President of the Senate and the Speaker of
2403 the House of Representatives of any severity level 3, 4, or 5
2404 incident as soon as possible but no later than 12 hours after
2405 receiving a local government's incident report. The notification
2406 must include a high-level description of the incident and the
2407 likely effects.

576-02447-25

20257026pb

2408 (c) A local government may report a cybersecurity incident
2409 determined by the local government to be of severity level 1 or
2410 2 as provided in s. 282.318(3)(c) ~~s. 282.318(3)(b)~~ to the state
2411 chief information security officer, the Cybercrime Office of the
2412 Department of Law Enforcement, and the sheriff who has
2413 jurisdiction over the local government. The report shall contain
2414 the information required in paragraph (a).

2415 Section 22. Section 282.319, Florida Statutes, is repealed.

2416 Section 23. (1) POSITIONS.—

2417 (a) The following positions are established within the
2418 Agency for State Systems and Enterprise Technology:

2419 1. Chief operations officer.

2420 2. Chief information officer.

2421 (b) Effective July 1, 2026, the following positions are
2422 established within the Agency for State Systems and Enterprise
2423 Technology, all of whom shall be appointed by the executive
2424 director:

2425 1. Deputy executive director, who shall serve as the state
2426 chief information architect, and the following:

2427 a. A minimum of six lead technology coordinators. At least
2428 one coordinator shall be assigned to each of the following major
2429 program areas: health and human services, education, government
2430 operations, criminal and civil justice, agriculture and natural
2431 resources, and transportation and economic development.

2432 b. A minimum of six assistant technology coordinators. At
2433 least one coordinator shall be assigned to each of the following
2434 major program areas: health and human services, education,
2435 government operations, criminal and civil justice, agriculture
2436 and natural resources, and transportation and economic

576-02447-25

20257026pb

2437 development.

2438 2. State chief information security officer and six lead
2439 security consultants. One consultant shall be assigned to each
2440 of the following major program areas: health and human services,
2441 education, government operations, criminal and civil justice,
2442 agriculture and natural resources, and transportation and
2443 economic development.

2444 3. State chief data officer and the following:

2445 a. A minimum of three data specialists with at least one
2446 specialist dedicated to each of the following areas of data
2447 expertise:

2448 (I) Personally identifiable information.

2449 (II) Protected health information.

2450 (III) Criminal justice information services.

2451 b. A minimum of six data security consultants. At least one
2452 consultant shall be assigned to each of the following major
2453 program areas: health and human services, education, government
2454 operations, criminal and civil justice, agriculture and natural
2455 resources, and transportation and economic development.

2456 4. State chief information technology procurement officer
2457 and a minimum of six lead information technology procurement
2458 consultants. At least one coordinator shall be assigned to each
2459 of the following major program areas: health and human services,
2460 education, government operations, criminal and civil justice,
2461 agriculture and natural resources, and transportation and
2462 economic development.

2463 5. State chief technology officer and the following:

2464 a. A minimum of 42 information technology business analyst
2465 consultants that shall be assigned to major program areas as

576-02447-25

20257026pb

2466 follows:

2467 (I) At least 11 consultants shall be assigned to health and
2468 human services and dedicated to state agencies at a minimum as
2469 follows:

2470 (A) Two dedicated to the Department of Health.

2471 (B) Four dedicated to the Agency for Health Care
2472 Administration.

2473 (C) Three dedicated to the Department of Children and
2474 Families.

2475 (D) Two dedicated to the remaining health and human
2476 services state agencies.

2477 (II) At least four consultants shall be assigned to
2478 education.

2479 (III) At least eight consultants shall be assigned to
2480 government operations and dedicated to state agencies at a
2481 minimum as follows:

2482 (A) Two dedicated to the Department of Financial Services.

2483 (B) One dedicated to the Department of Business and
2484 Professional Regulation.

2485 (C) Two dedicated to the Department of Management Services.

2486 (D) Three dedicated to the remaining government operations
2487 state agencies.

2488 (IV) At least six consultants shall be assigned to criminal
2489 and civil justice and dedicated to state agencies at a minimum
2490 as follows:

2491 (A) One dedicated to the Department of Law Enforcement.

2492 (B) Two dedicated to the Department of Corrections.

2493 (C) One dedicated to the Department of Juvenile Justice.

2494 (D) One dedicated to the Department of Legal Affairs.

576-02447-25

20257026pb

2495 (E) One dedicated to the remaining criminal and civil
2496 justice state agencies.

2497 (V) At least four consultants shall be assigned to
2498 agriculture and natural resources and dedicated to state
2499 agencies at a minimum as follows:

2500 (A) One dedicated the Department of Agriculture and
2501 Consumer Services.

2502 (B) One dedicated to the Department of Environmental
2503 Protection.

2504 (C) One dedicated to the Fish and Wildlife Conservation
2505 Commission.

2506 (D) One dedicated to the remaining agriculture and natural
2507 resources state agencies.

2508 (VI) At least nine consultants shall be assigned to
2509 transportation and economic development and dedicated to state
2510 agencies at a minimum as follows:

2511 (A) Two dedicated to the Department of Transportation.

2512 (B) Two dedicated to the Department of State.

2513 (C) One dedicated to the Department of Highway Safety and
2514 Motor Vehicles.

2515 (D) Two dedicated to the Department of Commerce.

2516 (E) One dedicated to the Division of Emergency Management.

2517 (F) One dedicated to the remaining transportation and
2518 economic development state agencies.

2519 b. A minimum of six information technology project
2520 management professional consultants. At least one consultant
2521 shall be assigned to each of the following major program areas:
2522 health and human services, education, government operations,
2523 criminal and civil justice, agriculture and natural resources,

576-02447-25

20257026pb

2524 and transportation and economic development.

2525 c. A minimum of six information technology contract
2526 management consultants. At least one consultant shall be
2527 assigned to each of the following major program areas: health
2528 and human services, education, government operations, criminal
2529 and civil justice, agriculture and natural resources, and
2530 transportation and economic development.

2531 d. A minimum of six information technology quality
2532 assurance consultants. At least one consultant shall be assigned
2533 to each of the following major program areas: health and human
2534 services, education, government operations, criminal and civil
2535 justice, agriculture and natural resources, and transportation
2536 and economic development.

2537 (2) BUREAUS.—

2538 (a) The Division of Enterprise Information Technology
2539 Services shall include:

2540 1. The Bureau of Enterprise Information Technology
2541 Operations, responsible for assessing state agency information
2542 technology needs and risks as established under s. 282.006,
2543 Florida Statutes.

2544 2. The Bureau of Enterprise Information Technology Quality
2545 Assurance, responsible for activities established under s.
2546 282.006, Florida Statutes.

2547 3. The Bureau of Enterprise Information Technology Project
2548 Management, responsible for project management oversight and
2549 activities established under s. 282.006, Florida Statutes.

2550 4. The Bureau of Enterprise Information Technology Contract
2551 Management, responsible for contract management oversight and
2552 activities established under s. 282.006, Florida Statutes.

576-02447-25

20257026pb

- 2553 (b) The Division of Enterprise Information Technology
2554 Purchasing shall include:
- 2555 1. The Bureau of Enterprise Information Technology
2556 Procurement Services, responsible for procurement activities
2557 established under s. 282.006, Florida Statutes.
- 2558 2. The Bureau of Enterprise Information Technology
2559 Procurement Policy and Oversight, responsible for activities
2560 established under s. 282.006, Florida Statutes.
- 2561 (3) WORKGROUP.—
- 2562 (a) The chief information officer policy workgroup shall be
2563 composed of all state agency chief information officers.
- 2564 (b) The purpose of the workgroup is to provide the
2565 Legislature with input and feedback regarding the structure,
2566 budget, and governance of the Agency for State Systems and
2567 Enterprise Technology.
- 2568 (c) The chair of the workgroup shall be the interim state
2569 chief information officer.
- 2570 (d) The voting members of the workgroup shall include the
2571 chair of the workgroup and the chief information officers from
2572 the Department of Financial Services, the Department of
2573 Agriculture and Consumer Services, and the Department of Legal
2574 Affairs.
- 2575 (e) The chair of the workgroup shall submit a report to the
2576 Governor, the Commissioner of Agriculture, the Chief Financial
2577 Officer, the Attorney General, the President of the Senate, and
2578 the Speaker of the House of Representatives which includes
2579 recommendations and justifications for changes by December 1,
2580 2025. The final report must be voted on and accepted by a
2581 unanimous vote of the voting members of the workgroup.

576-02447-25

20257026pb

2582 (f) The workgroup shall expire after submission of the
2583 report required in paragraph (e).

2584 Section 24. Section 282.201, Florida Statutes, is amended
2585 to read:

2586 282.201 State data center.—The state data center is
2587 established within the Northwest Regional Data Center pursuant
2588 to s. 282.2011 the department. The provision of data center
2589 services must comply with applicable state and federal laws,
2590 regulations, and policies, including all applicable security,
2591 privacy, and auditing requirements. The department shall appoint
2592 a director of the state data center who has experience in
2593 leading data center facilities and has expertise in cloud-
2594 computing management.

2595 ~~(1) STATE DATA CENTER DUTIES. The state data center shall:~~

2596 ~~(a) Offer, develop, and support the services and~~
2597 ~~applications defined in service-level agreements executed with~~
2598 ~~its customer entities.~~

2599 ~~(b) Maintain performance of the state data center by~~
2600 ~~ensuring proper data backup; data backup recovery; disaster~~
2601 ~~recovery; and appropriate security, power, cooling, fire~~
2602 ~~suppression, and capacity.~~

2603 ~~(c) Develop and implement business continuity and disaster~~
2604 ~~recovery plans, and annually conduct a live exercise of each~~
2605 ~~plan.~~

2606 ~~(d) Enter into a service-level agreement with each customer~~
2607 ~~entity to provide the required type and level of service or~~
2608 ~~services. If a customer entity fails to execute an agreement~~
2609 ~~within 60 days after commencement of a service, the state data~~
2610 ~~center may cease service. A service-level agreement may not have~~

576-02447-25

20257026pb

- 2611 ~~a term exceeding 3 years and at a minimum must:~~
- 2612 ~~1. Identify the parties and their roles, duties, and~~
- 2613 ~~responsibilities under the agreement.~~
- 2614 ~~2. State the duration of the contract term and specify the~~
- 2615 ~~conditions for renewal.~~
- 2616 ~~3. Identify the scope of work.~~
- 2617 ~~4. Identify the products or services to be delivered with~~
- 2618 ~~sufficient specificity to permit an external financial or~~
- 2619 ~~performance audit.~~
- 2620 ~~5. Establish the services to be provided, the business~~
- 2621 ~~standards that must be met for each service, the cost of each~~
- 2622 ~~service by agency application, and the metrics and processes by~~
- 2623 ~~which the business standards for each service are to be~~
- 2624 ~~objectively measured and reported.~~
- 2625 ~~6. Provide a timely billing methodology to recover the~~
- 2626 ~~costs of services provided to the customer entity pursuant to s.~~
- 2627 ~~215.422.~~
- 2628 ~~7. Provide a procedure for modifying the service-level~~
- 2629 ~~agreement based on changes in the type, level, and cost of a~~
- 2630 ~~service.~~
- 2631 ~~8. Include a right-to-audit clause to ensure that the~~
- 2632 ~~parties to the agreement have access to records for audit~~
- 2633 ~~purposes during the term of the service-level agreement.~~
- 2634 ~~9. Provide that a service-level agreement may be terminated~~
- 2635 ~~by either party for cause only after giving the other party and~~
- 2636 ~~the department notice in writing of the cause for termination~~
- 2637 ~~and an opportunity for the other party to resolve the identified~~
- 2638 ~~cause within a reasonable period.~~
- 2639 ~~10. Provide for mediation of disputes by the Division of~~

576-02447-25

20257026pb

2640 ~~Administrative Hearings pursuant to s. 120.573.~~

2641 ~~(e) For purposes of chapter 273, be the custodian of~~
2642 ~~resources and equipment located in and operated, supported, and~~
2643 ~~managed by the state data center.~~

2644 ~~(f) Assume administrative access rights to resources and~~
2645 ~~equipment, including servers, network components, and other~~
2646 ~~devices, consolidated into the state data center.~~

2647 ~~1. Upon consolidation, a state agency shall relinquish~~
2648 ~~administrative rights to consolidated resources and equipment.~~
2649 ~~State agencies required to comply with federal and state~~
2650 ~~criminal justice information security rules and policies shall~~
2651 ~~retain administrative access rights sufficient to comply with~~
2652 ~~the management control provisions of those rules and policies;~~
2653 ~~however, the state data center shall have the appropriate type~~
2654 ~~or level of rights to allow the center to comply with its duties~~
2655 ~~pursuant to this section. The Department of Law Enforcement~~
2656 ~~shall serve as the arbiter of disputes pertaining to the~~
2657 ~~appropriate type and level of administrative access rights~~
2658 ~~pertaining to the provision of management control in accordance~~
2659 ~~with the federal criminal justice information guidelines.~~

2660 ~~2. The state data center shall provide customer entities~~
2661 ~~with access to applications, servers, network components, and~~
2662 ~~other devices necessary for entities to perform business~~
2663 ~~activities and functions, and as defined and documented in a~~
2664 ~~service-level agreement.~~

2665 ~~(g) In its procurement process, show preference for cloud-~~
2666 ~~computing solutions that minimize or do not require the~~
2667 ~~purchasing, financing, or leasing of state data center~~
2668 ~~infrastructure, and that meet the needs of customer agencies,~~

576-02447-25

20257026pb

2669 ~~that reduce costs, and that meet or exceed the applicable state~~
2670 ~~and federal laws, regulations, and standards for cybersecurity.~~

2671 ~~(h) Assist customer entities in transitioning from state~~
2672 ~~data center services to the Northwest Regional Data Center or~~
2673 ~~other third-party cloud computing services procured by a~~
2674 ~~customer entity or by the Northwest Regional Data Center on~~
2675 ~~behalf of a customer entity.~~

2676 (1)~~(2)~~ USE OF THE STATE DATA CENTER.—

2677 ~~(a)~~ The following are exempt from the use of the state data
2678 center: the Department of Law Enforcement, the Department of the
2679 Lottery's Gaming System, Systems Design and Development in the
2680 Office of Policy and Budget, the regional traffic management
2681 centers as described in s. 335.14(2) and the Office of Toll
2682 Operations of the Department of Transportation, the State Board
2683 of Administration, state attorneys, public defenders, criminal
2684 conflict and civil regional counsel, capital collateral regional
2685 counsel, ~~and~~ the Florida Housing Finance Corporation, and the
2686 Division of Emergency Management within the Executive Office of
2687 the Governor.

2688 ~~(b) The Division of Emergency Management is exempt from the~~
2689 ~~use of the state data center. This paragraph expires July 1,~~
2690 ~~2025.~~

2691 (2)~~(3)~~ AGENCY LIMITATIONS.—Unless exempt from the use of
2692 the state data center pursuant to this section or authorized by
2693 the Legislature, a state agency may not:

2694 (a) Create a new agency computing facility or data center,
2695 or expand the capability to support additional computer
2696 equipment in an existing agency computing facility or data
2697 center; or

576-02447-25

20257026pb

2698 (b) Terminate services with the state data center without
2699 giving written notice of intent to terminate services 180 days
2700 before such termination.

2701 ~~(4) DEPARTMENT RESPONSIBILITIES. The department shall~~
2702 ~~provide operational management and oversight of the state data~~
2703 ~~center, which includes:~~

2704 ~~(a) Implementing industry standards and best practices for~~
2705 ~~the state data center's facilities, operations, maintenance,~~
2706 ~~planning, and management processes.~~

2707 ~~(b) Developing and implementing cost-recovery mechanisms~~
2708 ~~that recover the full direct and indirect cost of services~~
2709 ~~through charges to applicable customer entities. Such cost-~~
2710 ~~recovery mechanisms must comply with applicable state and~~
2711 ~~federal regulations concerning distribution and use of funds and~~
2712 ~~must ensure that, for any fiscal year, no service or customer~~
2713 ~~entity subsidizes another service or customer entity. The~~
2714 ~~department may recommend other payment mechanisms to the~~
2715 ~~Executive Office of the Governor, the President of the Senate,~~
2716 ~~and the Speaker of the House of Representatives. Such mechanisms~~
2717 ~~may be implemented only if specifically authorized by the~~
2718 ~~Legislature.~~

2719 ~~(c) Developing and implementing appropriate operating~~
2720 ~~guidelines and procedures necessary for the state data center to~~
2721 ~~perform its duties pursuant to subsection (1). The guidelines~~
2722 ~~and procedures must comply with applicable state and federal~~
2723 ~~laws, regulations, and policies and conform to generally~~
2724 ~~accepted governmental accounting and auditing standards. The~~
2725 ~~guidelines and procedures must include, but need not be limited~~
2726 ~~to:~~

576-02447-25

20257026pb

2727 ~~1. Implementing a consolidated administrative support~~
2728 ~~structure responsible for providing financial management,~~
2729 ~~procurement, transactions involving real or personal property,~~
2730 ~~human resources, and operational support.~~

2731 ~~2. Implementing an annual reconciliation process to ensure~~
2732 ~~that each customer entity is paying for the full direct and~~
2733 ~~indirect cost of each service as determined by the customer~~
2734 ~~entity's use of each service.~~

2735 ~~3. Providing rebates that may be credited against future~~
2736 ~~billings to customer entities when revenues exceed costs.~~

2737 ~~4. Requiring customer entities to validate that sufficient~~
2738 ~~funds exist before implementation of a customer entity's request~~
2739 ~~for a change in the type or level of service provided, if such~~
2740 ~~change results in a net increase to the customer entity's cost~~
2741 ~~for that fiscal year.~~

2742 ~~5. By November 15 of each year, providing to the Office of~~
2743 ~~Policy and Budget in the Executive Office of the Governor and to~~
2744 ~~the chairs of the legislative appropriations committees the~~
2745 ~~projected costs of providing data center services for the~~
2746 ~~following fiscal year.~~

2747 ~~6. Providing a plan for consideration by the Legislative~~
2748 ~~Budget Commission if the cost of a service is increased for a~~
2749 ~~reason other than a customer entity's request made pursuant to~~
2750 ~~subparagraph 4. Such a plan is required only if the service cost~~
2751 ~~increase results in a net increase to a customer entity for that~~
2752 ~~fiscal year.~~

2753 ~~7. Standardizing and consolidating procurement and~~
2754 ~~contracting practices.~~

2755 ~~(d) In collaboration with the Department of Law Enforcement~~

576-02447-25

20257026pb

2756 and the Florida Digital Service, developing and implementing a
2757 process for detecting, reporting, and responding to
2758 cybersecurity incidents, breaches, and threats.

2759 ~~(c) Adopting rules relating to the operation of the state~~
2760 ~~data center, including, but not limited to, budgeting and~~
2761 ~~accounting procedures, cost recovery methodologies, and~~
2762 ~~operating procedures.~~

2763 ~~(5) NORTHWEST REGIONAL DATA CENTER CONTRACT. In order for~~
2764 ~~the department to carry out its duties and responsibilities~~
2765 ~~relating to the state data center, the secretary of the~~
2766 ~~department shall contract by July 1, 2022, with the Northwest~~
2767 ~~Regional Data Center pursuant to s. 287.057(11). The contract~~
2768 ~~shall provide that the Northwest Regional Data Center will~~
2769 ~~manage the operations of the state data center and provide data~~
2770 ~~center services to state agencies.~~

2771 ~~(a) The department shall provide contract oversight,~~
2772 ~~including, but not limited to, reviewing invoices provided by~~
2773 ~~the Northwest Regional Data Center for services provided to~~
2774 ~~state agency customers.~~

2775 ~~(b) The department shall approve or request updates to~~
2776 ~~invoices within 10 business days after receipt. If the~~
2777 ~~department does not respond to the Northwest Regional Data~~
2778 ~~Center, the invoice will be approved by default. The Northwest~~
2779 ~~Regional Data Center must submit approved invoices directly to~~
2780 ~~state agency customers.~~

2781 Section 25. Section 1004.649, Florida Statutes, is
2782 transferred, renumbered as section 282.0211, Florida Statutes,
2783 and amended to read:

2784 282.0211 ~~1004.649~~ Northwest Regional Data Center.—

576-02447-25

20257026pb

2785 (1) For the purpose of providing data center services to
2786 its state agency customers, the Northwest Regional Data Center
2787 is designated as a state data center for all state agencies and
2788 shall:

2789 (a) Operate under a governance structure that represents
2790 its customers proportionally.

2791 (b) Maintain an appropriate cost-allocation methodology
2792 that accurately bills state agency customers based solely on the
2793 actual direct and indirect costs of the services provided to
2794 state agency customers and ensures that, for any fiscal year,
2795 state agency customers are not subsidizing other customers of
2796 the data center. Such cost-allocation methodology must comply
2797 with applicable state and federal regulations concerning the
2798 distribution and use of state and federal funds.

2799 (c) Enter into a service-level agreement with each state
2800 agency customer to provide services as defined and approved by
2801 the governing board of the center. At a minimum, such service-
2802 level agreements must:

2803 1. Identify the parties and their roles, duties, and
2804 responsibilities under the agreement;

2805 2. State the duration of the agreement term, which may not
2806 exceed 3 years, and specify the conditions for up to two
2807 optional 1-year renewals of the agreement before execution of a
2808 new agreement;

2809 3. Identify the scope of work;

2810 4. Establish the services to be provided, the business
2811 standards that must be met for each service, the cost of each
2812 service, and the process by which the business standards for
2813 each service are to be objectively measured and reported;

576-02447-25

20257026pb

2814 5. Provide a timely billing methodology for recovering the
2815 cost of services provided pursuant to s. 215.422;

2816 6. Provide a procedure for modifying the service-level
2817 agreement to address any changes in projected costs of service;

2818 7. Include a right-to-audit clause to ensure that the
2819 parties to the agreement have access to records for audit
2820 purposes during the term of the service-level agreement;

2821 8. Identify the products or services to be delivered with
2822 sufficient specificity to permit an external financial or
2823 performance audit;

2824 9. Provide that the service-level agreement may be
2825 terminated by either party for cause only after giving the other
2826 party notice in writing of the cause for termination and an
2827 opportunity for the other party to resolve the identified cause
2828 within a reasonable period; and

2829 10. Provide state agency customer entities with access to
2830 applications, servers, network components, and other devices
2831 necessary for entities to perform business activities and
2832 functions and as defined and documented in a service-level
2833 agreement.

2834 (d) In its procurement process, show preference for cloud-
2835 computing solutions that minimize or do not require the
2836 purchasing or financing of state data center infrastructure,
2837 that meet the needs of state agency customer entities, that
2838 reduce costs, and that meet or exceed the applicable state and
2839 federal laws, regulations, and standards for cybersecurity.

2840 (e) Assist state agency customer entities in transitioning
2841 from state data center services to other third-party cloud-
2842 computing services procured by a customer entity or by the

576-02447-25

20257026pb

2843 Northwest Regional Data Center on behalf of the customer entity.

2844 (f) Provide to the Board of Governors the total annual
2845 budget by major expenditure category, including, but not limited
2846 to, salaries, expenses, operating capital outlay, contracted
2847 services, or other personnel services by July 30 each fiscal
2848 year.

2849 (g) Provide to each state agency customer its projected
2850 annual cost for providing the agreed-upon data center services
2851 by September 1 each fiscal year.

2852 (h) By November 15 of each year, provide to the Office of
2853 Policy and Budget in the Executive Office of the Governor and to
2854 the chairs of the legislative appropriations committees the
2855 projected costs of providing data center services for the
2856 following fiscal year.

2857 (i)~~(h)~~ Provide a plan for consideration by the Legislative
2858 Budget Commission if the governing body of the center approves
2859 the use of a billing rate schedule after the start of the fiscal
2860 year that increases any state agency customer's costs for that
2861 fiscal year.

2862 (j)~~(i)~~ Provide data center services that comply with
2863 applicable state and federal laws, regulations, and policies,
2864 including all applicable security, privacy, and auditing
2865 requirements.

2866 (k)~~(j)~~ Maintain performance of the data center facilities
2867 by ensuring proper data backup; data backup recovery; disaster
2868 recovery; and appropriate security, power, cooling, fire
2869 suppression, and capacity.

2870 (l)~~(k)~~ ~~Prepare and submit state agency customer invoices to~~
2871 ~~the Department of Management Services for approval. Upon~~

576-02447-25

20257026pb

2872 ~~approval or by default pursuant to s. 282.201(5),~~ Submit
2873 invoices to state agency customers.

2874 (m)~~(l)~~ As funded in the General Appropriations Act, provide
2875 data center services to state agencies from multiple facilities.

2876 (2) Unless exempt from the requirement to use the state
2877 data center pursuant to s. 282.201(1) ~~s. 282.201(2)~~ or as
2878 authorized by the Legislature, a state agency may not do any of
2879 the following:

2880 (a) Terminate services with the Northwest Regional Data
2881 Center without giving written notice of intent to terminate
2882 services 180 days before such termination.

2883 (b) Procure third-party cloud-computing services without
2884 evaluating the cloud-computing services provided by the
2885 Northwest Regional Data Center.

2886 (c) Exceed 30 days from receipt of approved invoices to
2887 remit payment for state data center services provided by the
2888 Northwest Regional Data Center.

2889 (3) The Northwest Regional Data Center's authority to
2890 provide data center services to its state agency customers may
2891 be terminated if:

2892 (a) The center requests such termination to the Board of
2893 Governors, the President of the Senate, and the Speaker of the
2894 House of Representatives; or

2895 (b) The center fails to comply with the provisions of this
2896 section.

2897 (4) If such authority is terminated, the center has 1 year
2898 to provide for the transition of its state agency customers to a
2899 qualified alternative cloud-based data center that meets the
2900 enterprise architecture standards established by the Florida

576-02447-25

20257026pb

2901 Digital Service.

2902 Section 26. Effective July 1, 2026, subsection (2) of
2903 section 20.22, Florida Statutes, is amended to read:

2904 20.22 Department of Management Services.—There is created a
2905 Department of Management Services.

2906 (2) The following divisions, programs, and services within
2907 the Department of Management Services are established:

2908 (a) Facilities Program.

2909 (b) ~~The Florida Digital Service.~~

2910 ~~(c)~~ Workforce Program.

2911 (c)1. ~~(d)1.~~ Support Program.

2912 2. Federal Property Assistance Program.

2913 (d) ~~(e)~~ Administration Program.

2914 (e) ~~(f)~~ Division of Administrative Hearings.

2915 (f) ~~(g)~~ Division of Retirement.

2916 (g) ~~(h)~~ Division of State Group Insurance.

2917 (h) ~~(i)~~ Division of Telecommunications.

2918 Section 27. Effective July 1, 2026, subsections (1), (5),
2919 (7), and (8) of section 282.802, Florida Statutes, are amended
2920 to read:

2921 282.802 Government Technology Modernization Council.—

2922 (1) The Government Technology Modernization Council, an
2923 advisory council as defined in s. 20.03(7), is located ~~created~~
2924 within ASSET ~~the department~~. Except as otherwise provided in
2925 this section, the advisory council shall operate in a manner
2926 consistent with s. 20.052.

2927 (5) The state chief information officer ~~Secretary of~~
2928 ~~Management Services~~, or his or her designee, shall serve as the
2929 ex officio, nonvoting executive director of the council.

576-02447-25

20257026pb

- 2930 (7) ~~(a)~~ The council shall meet at least quarterly to:
- 2931 (a)1. Recommend legislative and administrative actions that
- 2932 the Legislature and state agencies as defined in s. 282.0041 ~~s.~~
- 2933 ~~282.318(2)~~ may take to promote the development of data
- 2934 modernization in this state.
- 2935 (b)2. Assess and provide guidance on necessary legislative
- 2936 reforms and the creation of a state code of ethics for
- 2937 artificial intelligence systems in state government.
- 2938 (c)3. Assess the effect of automated decision systems or
- 2939 identity management on constitutional and other legal rights,
- 2940 duties, and privileges of residents of this state.
- 2941 (d)4. Evaluate common standards for artificial intelligence
- 2942 safety and security measures, including the benefits of
- 2943 requiring disclosure of the digital provenance for all images
- 2944 and audio created using generative artificial intelligence as a
- 2945 means of revealing the origin and edit of the image or audio, as
- 2946 well as the best methods for such disclosure.
- 2947 (e)5. Assess the manner in which governmental entities and
- 2948 the private sector are using artificial intelligence with a
- 2949 focus on opportunity areas for deployments in systems across
- 2950 this state.
- 2951 (f)6. Determine the manner in which artificial intelligence
- 2952 is being exploited by bad actors, including foreign countries of
- 2953 concern as defined in s. 287.138(1).
- 2954 (g)7. Evaluate the need for curriculum to prepare school-
- 2955 age audiences with the digital media and visual literacy skills
- 2956 needed to navigate the digital information landscape.
- 2957 ~~(b) At least one quarterly meeting of the council must be a~~
- 2958 ~~joint meeting with the Florida Cybersecurity Advisory Council.~~

576-02447-25

20257026pb

2959 (8) ~~By December 31, 2024, and Each December 31 thereafter,~~
2960 the council shall submit to the Governor, the Commissioner of
2961 Agriculture, the Chief Financial Officer, the Attorney General,
2962 the President of the Senate, and the Speaker of the House of
2963 Representatives any legislative recommendations considered
2964 necessary by the council to modernize government technology,
2965 including:

2966 (a) Recommendations for policies necessary to:

2967 1. Accelerate adoption of technologies that will increase
2968 productivity of state enterprise information technology systems,
2969 improve customer service levels of government, and reduce
2970 administrative or operating costs.

2971 2. Promote the development and deployment of artificial
2972 intelligence systems, financial technology, education
2973 technology, or other enterprise management software in this
2974 state.

2975 3. Protect Floridians from bad actors who use artificial
2976 intelligence.

2977 (b) Any other information the council considers relevant.

2978 Section 28. Effective July 1, 2026, section 282.604,
2979 Florida Statutes, is amended to read:

2980 282.604 Adoption of rules.—~~ASSET The Department of~~
2981 ~~Management Services~~ shall, with input from stakeholders, adopt
2982 rules pursuant to ss. 120.536(1) and 120.54 for the development,
2983 procurement, maintenance, and use of accessible electronic
2984 information technology by governmental units.

2985 Section 29. Subsection (4) of section 287.0591, Florida
2986 Statutes, is amended to read:

2987 287.0591 Information technology; vendor disqualification.—

576-02447-25

20257026pb

2988 (4) If the department issues a competitive solicitation for
2989 information technology commodities, consultant services, or
2990 staff augmentation contractual services, the state chief
2991 information officer must ~~Florida Digital Service within the~~
2992 ~~department shall~~ participate in such solicitations.

2993 Section 30. Subsection (4) of section 288.012, Florida
2994 Statutes, is amended to read:

2995 288.012 State of Florida international offices; direct-
2996 support organization.—The Legislature finds that the expansion
2997 of international trade and tourism is vital to the overall
2998 health and growth of the economy of this state. This expansion
2999 is hampered by the lack of technical and business assistance,
3000 financial assistance, and information services for businesses in
3001 this state. The Legislature finds that these businesses could be
3002 assisted by providing these services at State of Florida
3003 international offices. The Legislature further finds that the
3004 accessibility and provision of services at these offices can be
3005 enhanced through cooperative agreements or strategic alliances
3006 between private businesses and state, local, and international
3007 governmental entities.

3008 (4) The Department of Commerce, in connection with the
3009 establishment, operation, and management of any of its offices
3010 located in another country, is exempt from the provisions of ss.
3011 255.21, 255.25, and 255.254 relating to leasing of buildings;
3012 ss. 283.33 and 283.35 relating to bids for printing; ss.
3013 287.001-287.20 relating to purchasing and motor vehicles; and
3014 ss. 282.0051 and 282.702-282.7101 ~~ss. 282.003-282.00515 and~~
3015 ~~282.702-282.7101~~ relating to communications, and from all
3016 statutory provisions relating to state employment.

576-02447-25

20257026pb

3017 (a) The department may exercise such exemptions only upon
3018 prior approval of the Governor.

3019 (b) If approval for an exemption under this section is
3020 granted as an integral part of a plan of operation for a
3021 specified international office, such action shall constitute
3022 continuing authority for the department to exercise the
3023 exemption, but only in the context and upon the terms originally
3024 granted. Any modification of the approved plan of operation with
3025 respect to an exemption contained therein must be resubmitted to
3026 the Governor for his or her approval. An approval granted to
3027 exercise an exemption in any other context shall be restricted
3028 to the specific instance for which the exemption is to be
3029 exercised.

3030 (c) As used in this subsection, the term "plan of
3031 operation" means the plan developed pursuant to subsection (2).

3032 (d) Upon final action by the Governor with respect to a
3033 request to exercise the exemption authorized in this subsection,
3034 the department shall report such action, along with the original
3035 request and any modifications thereto, to the President of the
3036 Senate and the Speaker of the House of Representatives within 30
3037 days.

3038 Section 31. Effective July 1, 2026, paragraph (b) of
3039 subsection (4) of section 443.1113, Florida Statutes, is amended
3040 to read:

3041 443.1113 Reemployment Assistance Claims and Benefits
3042 Information System.—

3043 (4)

3044 (b) The department shall seek input on recommended
3045 enhancements from, at a minimum, the following entities:

576-02447-25

20257026pb

3046 1. The Agency for State Systems and Enterprise Technology
3047 ~~Florida Digital Service within the Department of Management~~
3048 ~~Services.~~

3049 2. The General Tax Administration Program Office within the
3050 Department of Revenue.

3051 3. The Division of Accounting and Auditing within the
3052 Department of Financial Services.

3053 Section 32. Effective July 1, 2026, subsection (5) of
3054 section 943.0415, Florida Statutes, is amended to read:

3055 943.0415 Cybercrime Office.—There is created within the
3056 Department of Law Enforcement the Cybercrime Office. The office
3057 may:

3058 (5) Consult with the state chief information security
3059 officer of the Agency for State Systems and Enterprise
3060 Technology ~~Florida Digital Service within the Department of~~
3061 ~~Management Services~~ in the adoption of rules relating to the
3062 information technology security provisions in s. 282.318.

3063 Section 33. Effective July 1, 2026, subsection (3) of
3064 section 1004.444, Florida Statutes, is amended to read:

3065 1004.444 Florida Center for Cybersecurity.—

3066 (3) Upon receiving a request for assistance from a ~~the~~
3067 ~~Department of Management Services, the Florida Digital Service,~~
3068 ~~or another~~ state agency, the center is authorized, but may not
3069 be compelled by the agency, to conduct, consult on, or otherwise
3070 assist any state-funded initiatives related to:

3071 (a) Cybersecurity training, professional development, and
3072 education for state and local government employees, including
3073 school districts and the judicial branch; and

3074 (b) Increasing the cybersecurity effectiveness of the

576-02447-25

20257026pb

3075 state's and local governments' technology platforms and
3076 infrastructure, including school districts and the judicial
3077 branch.

3078 Section 34. Except as otherwise provided in this act, this
3079 act shall take effect July 1, 2025.