

By the Committee on Appropriations; the Appropriations Committee on Agriculture, Environment, and General Government; and Senator Harrell

576-02812-26

2026480c2

1 A bill to be entitled
2 An act relating to information technology; providing
3 for a type two transfer of the duties and functions of
4 the Florida Digital Service from the Department of
5 Management Services to the Division of Integrated
6 Government Innovation and Technology; creating s.
7 14.205, F.S.; creating the Division of Integrated
8 Government Innovation and Technology (DIGIT) within
9 the Executive Office of the Governor; providing that
10 the division is a separate budget entity and must
11 prepare and submit a budget in accordance with
12 specified provisions; requiring the division to be
13 responsible for all professional, technical, and
14 administrative support to carry out its assigned
15 duties; providing for a director of the division;
16 providing that the director also serves as the state
17 chief information officer; providing for the
18 appointment of the director; prohibiting the state
19 chief information officer from having certain
20 conflicts of interest; providing the qualifications
21 for the state chief information officer; providing
22 that the deputy director also serves as the deputy
23 chief information officer; providing that the director
24 will select a state chief information security
25 officer, state chief data officer, state chief
26 technology officer, and state chief technology
27 procurement officer; transferring the state chief
28 information officer of the Department of Management
29 Services to DIGIT until the Governor appoints a

576-02812-26

2026480c2

30 permanent officer; requiring that such appointment
31 occur by a specified date; amending s. 20.055, F.S.;
32 requiring agency inspectors general to review and
33 report whether certain agency practices are consistent
34 with specified reporting requirements and standards;
35 requiring such inspectors general to prepare and
36 submit a certain compliance report to certain persons
37 by a specified date annually; requiring the chief
38 inspector general to review certain reports and
39 prepare a consolidated report; requiring that such
40 report be submitted to the Executive Office of the
41 Governor and the Legislature annually by a specified
42 date; requiring certain agency heads to submit certain
43 reports to the Executive Office of the Governor and
44 the Legislature annually by a specified date; amending
45 s. 97.0525, F.S.; requiring that the Division of
46 Elections comprehensive risk assessment comply with
47 the risk assessment methodology developed by DIGIT;
48 amending s. 112.22, F.S.; defining the term "DIGIT";
49 deleting the term "department"; revising the
50 definition of the term "prohibited application";
51 authorizing public employers to request a certain
52 waiver from DIGIT; requiring DIGIT to take specified
53 actions; deleting obsolete language; requiring DIGIT
54 to adopt rules; amending s. 119.0725, F.S.; requiring
55 that certain confidential and exempt information be
56 made available to DIGIT; amending s. 216.023, F.S.;
57 deleting a provision requiring state agencies and the
58 judicial branch to include a cumulative inventory and

576-02812-26

2026480c2

59 a certain status report of specified projects as part
60 of a budget request; deleting provisions relating to
61 ongoing technology-related projects; conforming a
62 cross-reference; amending s. 282.0041, F.S.; deleting
63 and revising definitions; defining the terms "DIGIT"
64 and "technical debt"; amending s. 282.00515, F.S.;

65 authorizing the Department of Legal Affairs, the
66 Department of Financial Services, and the Department
67 of Agriculture and Consumer Services to adopt
68 alternative standards that must be based on specified
69 industry-recognized best practices and standards;
70 requiring the departments to evaluate the adoption of
71 such standards on a case-by-case basis; requiring the
72 departments to follow specified standards under
73 certain circumstances; requiring the departments to
74 conduct a certain full baseline needs assessment;
75 authorizing the departments to contract with DIGIT to
76 assist or complete such assessment; requiring the
77 departments to each produce certain phased roadmaps
78 that must be submitted annually with specified budget
79 requests; authorizing the departments to contract with
80 DIGIT to assist or complete such roadmaps; authorizing
81 the departments to contract with DIGIT for specified
82 services; requiring the departments to use certain
83 information technology reports and follow a specified
84 reporting process; requiring the departments to submit
85 a certain report annually by a specified date to the
86 Governor and the Legislature; revising applicability;
87 authorizing DIGIT to perform project oversight on

576-02812-26

2026480c2

88 information technology projects of the departments
89 which have a specified project cost; requiring that
90 such projects comply with certain standards; requiring
91 DIGIT to report periodically to the Legislature high-
92 risk information technology projects; specifying
93 report requirements; requiring state agencies to
94 consult with DIGIT and work cooperatively with certain
95 departments under specified circumstances; revising
96 cross-references; creating s. 282.006, F.S.; requiring
97 DIGIT to operate as the state enterprise organization
98 for information technology governance and as the lead
99 entity responsible for understanding needs and
100 environments, creating standards and strategy,
101 supporting state agency technology efforts, and
102 reporting on the state of information technology in
103 this state; providing legislative intent; requiring
104 DIGIT to establish the strategic direction of
105 information technology in the state; requiring DIGIT
106 to develop and publish an information technology
107 policy for a specified purpose; requiring that such
108 policy be updated as necessary to meet certain
109 requirements and reflect advancements in technology;
110 requiring DIGIT, in coordination with certain subject
111 matter experts, to develop, publish, and maintain
112 specified enterprise architecture; requiring DIGIT to
113 take specified actions related to oversight of the
114 state's technology enterprise; requiring DIGIT to
115 develop open data standards and technologies for use
116 by state agencies; requiring DIGIT to develop certain

576-02812-26

2026480c2

117 testing, best practices, and standards; specifying
118 such best practices and standards; requiring DIGIT to
119 produce specified reports and provide such reports to
120 the Governor and the Legislature by specified dates
121 and at specified intervals; specifying requirements
122 for such reports; requiring DIGIT to conduct a market
123 analysis at a certain interval beginning on a
124 specified date; specifying requirements for the market
125 analysis; requiring that each market analysis be used
126 to prepare a strategic plan for specified purposes;
127 requiring that the market analysis and strategic plan
128 be submitted by a specified date; requiring DIGIT to
129 develop, implement, and maintain a certain library;
130 specifying requirements for the library; requiring
131 DIGIT to establish procedures that ensure the
132 integrity, security, and availability of the library;
133 requiring DIGIT to regularly update documents and
134 materials in the library to reflect current state and
135 federal requirements, industry best practices, and
136 emerging technologies; requiring DIGIT to create
137 mechanisms for state agencies to submit feedback,
138 request clarification, and recommend updates;
139 requiring state agencies to actively participate and
140 collaborate with DIGIT to achieve certain objectives
141 and to reference and adhere to the policies,
142 standards, and guidelines of the library in specified
143 tasks; authorizing state agencies to request
144 exemptions to specific policies, standards, or
145 guidelines under specified circumstances; providing

576-02812-26

2026480c2

146 the mechanism for a state agency to request such
147 exemptions; requiring DIGIT to review the request and
148 make a recommendation to the state chief information
149 officer; requiring the state chief information officer
150 to present the exemption to the chief information
151 officer workgroup; requiring that approval of the
152 exemption be by majority vote; requiring that state
153 agencies granted an exemption be reviewed periodically
154 to determine whether such exemption is necessary or
155 whether compliance can be achieved; authorizing DIGIT
156 to adopt rules; creating s. 282.0061, F.S.; providing
157 legislative intent; requiring DIGIT to complete a
158 certain full baseline needs assessment of state
159 agencies, develop a specified plan to conduct such
160 assessments, and submit such plan to the Governor and
161 the Legislature within a specified timeframe;
162 requiring DIGIT to support state agency strategic
163 planning efforts and assist agencies with production
164 of a certain phased roadmap; specifying requirements
165 for such roadmaps; requiring DIGIT to make
166 recommendations for standardizing data across state
167 agencies for a specified purpose, identify any
168 opportunities for standardization and consolidation of
169 information technology services across state agencies,
170 support specified functions, review all state agency
171 legislative budget requests for compliance, and
172 provide a certain review to the Office of Policy and
173 Budget in the Executive Office of the Governor;
174 requiring DIGIT to develop standards for use by state

576-02812-26

2026480c2

175 agencies which support specified best practices for
176 data management at the state agency level; requiring
177 DIGIT to provide a certain report to the Governor and
178 the Legislature by a specified date; specifying
179 requirements for the report; providing the duties and
180 responsibilities of DIGIT related to state agency
181 technology projects; requiring DIGIT, in consultation
182 with state agencies, to create a methodology,
183 approach, and applicable templates and formats for
184 identifying and collecting information technology
185 expenditure data at the state agency level; requiring
186 DIGIT to continuously obtain, review, and maintain
187 records of the appropriations, expenditures, and
188 revenues for information technology for each state
189 agency; requiring DIGIT to prescribe the format for
190 state agencies to provide financial information to
191 DIGIT for inclusion in a certain annual report;
192 requiring state agencies to submit such information by
193 a specified date annually; requiring DIGIT to work
194 with state agencies to provide alternative standards,
195 policies, or requirements under specified
196 circumstances; creating s. 282.0062, F.S.;

197 establishing workgroups within DIGIT to facilitate
198 coordination with state agencies; providing for the
199 membership and duties of such workgroups; requiring
200 the appropriate staff of the Department of Legal
201 Affairs, the Department of Financial Services, and the
202 Department of Agriculture and Consumer Services to
203 participate in specified workgroups; authorizing such

576-02812-26

2026480c2

204 staff to participate in specified workgroups and any
205 other workgroups as authorized by their respective
206 elected official; creating s. 282.0063, F.S.;
207 requiring DIGIT to perform specified actions to
208 develop and manage career paths, progressions, and
209 training programs for the benefit of state agency
210 personnel; requiring DIGIT to consult with specified
211 entities to implement specified provisions; creating
212 s. 282.0064, F.S.; requiring DIGIT, in coordination
213 with the Department of Management Services, to
214 establish a policy for all information technology-
215 related solicitations, contracts, and procurements;
216 specifying requirements for the policy related to
217 state term contracts, all contracts, and information
218 technology projects that require oversight;
219 prohibiting entities providing independent
220 verification and validation from having certain
221 interests, responsibilities, or other participation in
222 the project; providing the primary objective of
223 independent verification and validation; requiring the
224 entity performing such verification and validation to
225 provide specified regular reports and assessments;
226 requiring the Division of State Purchasing within the
227 Department of Management Services to coordinate with
228 DIGIT on state term contract solicitations and
229 invitations to negotiate; specifying the scope of the
230 coordination; requiring DIGIT to evaluate vendor
231 responses and assist with answers to vendor questions
232 on such solicitations and invitations; authorizing the

576-02812-26

2026480c2

233 Department of Legal Affairs, the Department of
234 Financial Services, and the Department of Agriculture
235 and Consumer Services to adopt alternative information
236 technology policy; providing requirements for adopting
237 such alternative policy; amending s. 282.318, F.S.;
238 providing that DIGIT is the lead entity responsible
239 for establishing enterprise technology and
240 cybersecurity standards and processes and security
241 measures that comply with specified standards;
242 requiring DIGIT to adopt specified rules; requiring
243 DIGIT to take specified actions; revising the
244 responsibilities of the state chief information
245 security officer; revising the guidelines and
246 processes for state agency cybersecurity governance
247 frameworks; requiring state agencies to report all
248 ransomware incidents to the state chief information
249 security officer instead of the Cybersecurity
250 Operations Center; requiring state agencies to also
251 notify the Northwest Regional Data Center of such
252 incidents under specified conditions; requiring the
253 state chief information security officer, instead of
254 the Cybersecurity Operations Center, to notify the
255 Legislature of certain incidents; requiring state
256 agencies to notify the state chief information
257 security officer within specified timeframes after the
258 discovery of a specified cybersecurity incident or
259 ransomware incident; requiring state agencies to also
260 notify the Northwest Regional Data Center of such
261 incidents under specified conditions; requiring the

576-02812-26

2026480c2

262 state chief information security officer, instead of
263 the Cybersecurity Operations Center, to provide a
264 certain report on a quarterly basis to the
265 Legislature; revising the actions that state agency
266 heads are required to perform relating to
267 cybersecurity; revising the timeframe that the state
268 agency strategic cybersecurity plan must cover;
269 requiring that a specified comprehensive risk
270 assessment be completed biennially; authorizing such
271 assessment to be completed by an independent third
272 party; requiring the third party to attest to the
273 validity of the findings; specifying requirements for
274 the comprehensive risk assessment; providing that
275 confidential and exempt records be made available to
276 the state chief information security officer and
277 Legislature; conforming provisions to changes made by
278 the act; amending s. 282.3185, F.S.; requiring the
279 state chief information security officer to perform
280 specified actions relating to cybersecurity training
281 for state employees; deleting obsolete language;
282 requiring local governments to notify the state chief
283 information security officer of compliance with
284 specified provisions as soon as possible; requiring
285 local governments to notify the state chief
286 information security officer, instead of the
287 Cybersecurity Operations Center, of cybersecurity or
288 ransomware incidents; revising the timeframes in which
289 such notifications must be made; requiring the state
290 chief information security officer to notify the

576-02812-26

2026480c2

291 Governor and the Legislature of certain incidents
292 within a specified timeframe; authorizing local
293 governments to report certain cybersecurity incidents
294 to the state chief information security officer
295 instead of the Cybersecurity Operations Center;
296 requiring the state chief information security officer
297 to provide a certain consolidated incident report
298 within a specified timeframe to the Legislature;
299 requiring the state chief information security officer
300 to establish certain guidelines and processes by a
301 specified date; conforming provisions to changes made
302 by the act; repealing s. 282.319, F.S., relating to
303 the Florida Cybersecurity Advisory Council; amending
304 s. 282.201, F.S.; establishing the state data center
305 within the Northwest Regional Data Center; requiring
306 the Northwest Regional Data Center to meet or exceed
307 specified information technology standards; revising
308 requirements of the state data center; abrogating the
309 scheduled repeal of the Division of Emergency
310 Management's exemption from using the state data
311 center; deleting the Department of Management
312 Services' responsibilities related to the state data
313 center; deleting provisions relating to contracting
314 with the Northwest Regional Data Center; creating s.
315 282.2011, F.S.; designating the Northwest Regional
316 Data Center as the state data center for all state
317 agencies; requiring the data center to engage in
318 specified actions; requiring the Department of Law
319 Enforcement to serve as the arbiter of certain

576-02812-26

2026480c2

320 disputes in accordance with the federal criminal
321 justice information guidelines; prohibiting state
322 agencies from terminating services with the data
323 center without giving written notice within a
324 specified timeframe, procuring third-party cloud-
325 computing services without evaluating the data
326 center's cloud-computing services, and exceeding a
327 specified timeframe to remit payments for services
328 provided by the data center; specifying circumstances
329 under which the data center's authorization to provide
330 services may be terminated; providing that the data
331 center has a specified timeframe to provide for the
332 transition of state agency customers to a qualified
333 alternative cloud-based data center that meets
334 specified standards; providing that the data center is
335 the lead entity responsible for creating, operating,
336 and managing the Florida Behavioral Health Care Data
337 Repository; providing the purpose of the repository;
338 requiring the data center, in collaboration with the
339 Data Analysis Committee of the Commission on Mental
340 Health and Substance Use Disorder, to develop a
341 specified plan; requiring, beginning on a specified
342 date, the data center to submit a certain report
343 annually to the Governor and the Legislature;
344 providing for a transition to an alternative cloud-
345 based data center under specified circumstances;
346 revising the information the plan identifies and
347 documents; amending s. 282.206, F.S.; requiring state
348 agencies to submit a certain strategic plan to DIGIT

576-02812-26

2026480c2

349 and the Northwest Regional Data Center annually by a
350 specified date; amending s. 1004.649, F.S.; creating
351 the Northwest Regional Data Center at Florida State
352 University; conforming provisions to changes made by
353 the act; creating s. 287.0583, F.S.; requiring that
354 contracts for information technology commodities and
355 services ensure extraction of data, certain
356 documentation, assistance and support, and anticipated
357 fees; amending s. 287.0591, F.S.; requiring the
358 Department of Management Services to coordinate with
359 DIGIT in specified solicitations; specifying the scope
360 of the coordination; requiring agencies to maintain
361 copies of certain documents when issuing a request for
362 quote for state term contracts within specified
363 threshold amounts; providing that agencies that issue
364 requests for quotes in excess of certain thresholds
365 are subject to specified public records requirements;
366 requiring such agencies to publish specified
367 information; requiring such agencies to maintain
368 copies of certain documentation for a specified
369 timeframe; providing that use of a request for quote
370 is not subject to certain protest provisions;
371 authorizing agencies to request certain services from
372 DIGIT; requiring the department to prequalify firms
373 and individuals who provide information technology
374 commodities; authorizing such firms and individuals to
375 submit responses to requests for quotes; amending s.
376 20.22, F.S.; conforming provisions to changes made by
377 the act; amending s. 282.802, F.S.; providing that the

576-02812-26

2026480c2

378 Government Technology Modernization Council is located
379 within DIGIT; providing that the state chief
380 information officer, rather than the Secretary of
381 Management Services, is the ex officio head of the
382 council; conforming a cross-reference; amending s.
383 282.604, F.S.; conforming provisions to changes made
384 by the act; amending s. 443.1113, F.S.; conforming
385 provisions to changes made by the act; amending s.
386 943.0415, F.S.; requiring the state chief information
387 security officer, rather than the Florida Digital
388 Service, to consult with the Department of Law
389 Enforcement's Cybercrime Office in the adoption of
390 certain rules; amending s. 1004.444, F.S.; revising
391 the list of who may request certain assistance from
392 the Florida Center for Cybersecurity; providing an
393 effective date.

394

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

396

397 Section 1. All duties, functions, records, pending issues,
398 existing contracts, administrative authority, and administrative
399 rules relating to the Florida Digital Service are transferred by
400 a type two transfer, as described in s. 20.06, Florida Statutes,
401 to the Division of Integrated Government Innovation and
402 Technology as created by this act. Any unexpended balances of
403 appropriations, allocations, and other public funds will revert
404 or will be appropriated or allocated as provided in the General
405 Appropriations Act or otherwise by law.

406

Section 2. Section 14.205, Florida Statutes, is created to

576-02812-26

2026480c2

407 read:

408 14.205 Division of Integrated Government Innovation and
409 Technology.—

410 (1) The Division of Integrated Government Innovation and
411 Technology is established within the Executive Office of the
412 Governor. The division shall be a separate budget entity, as
413 provided in the General Appropriations Act, and shall prepare
414 and submit a budget request in accordance with chapter 216. The
415 division shall be responsible for all professional, technical,
416 and administrative support functions necessary to carry out its
417 responsibilities under chapter 282 and as otherwise provided in
418 law.

419 (2) (a) The director of the division shall serve as the
420 state chief information officer. The director shall be appointed
421 by the Governor, subject to confirmation by the Senate. The
422 state chief information officer is prohibited from having any
423 financial, personal, or business conflicts of interest related
424 to technology vendors, contractors, or other information
425 technology service providers doing business with the state.

426 (b) The state chief information officer must meet the
427 following qualifications:

428 1. Education requirements.—The state chief information
429 officer must meet one of the following criteria:

430 a. Hold a bachelor's degree from an accredited institution
431 in information technology, computer science, business
432 administration, public administration, or a related field; or

433 b. Hold a master's degree in any of the fields listed in
434 sub-subparagraph a., which may be substituted for a portion of
435 the professional experience requirements in subparagraph 2.

576-02812-26

2026480c2

436 2. Professional experience requirements.—The state chief
437 information officer must have at least 10 years of progressively
438 responsible experience in information technology management,
439 digital transformation, cybersecurity, or information technology
440 governance, including:

441 a. A minimum of 5 years in an executive or senior
442 leadership role, overseeing information technology strategy,
443 operations, or enterprise technology management, in either the
444 public or private sector;

445 b. Managing large-scale information technology projects,
446 enterprise infrastructure, and implementation of emerging
447 technologies;

448 c. Budget planning, procurement oversight, and financial
449 management of information technology investments; and

450 d. Working with state and federal information technology
451 regulations, digital services, and cybersecurity compliance
452 frameworks.

453 3. Technical and policy expertise.—The state chief
454 information officer must have demonstrated expertise in:

455 a. Cybersecurity and data protection by demonstrating
456 knowledge of cybersecurity risk management, compliance with the
457 National Institute of Standards and Technology Cybersecurity
458 Framework, ISO 27001, and applicable federal and state security
459 regulations;

460 b. Cloud and digital services with experience in cloud
461 computing, enterprise systems modernization, digital
462 transformation, and emerging information technology trends;

463 c. Information technology governance and policy development
464 by demonstrating an understanding of statewide information

576-02812-26

2026480c2

465 technology governance structures, digital services, and
466 information technology procurement policies; and

467 d. Public sector information technology management by
468 demonstrating familiarity with government information technology
469 funding models, procurement requirements, and legislative
470 processes affecting information technology strategy.

471 4. Leadership and administrative competencies.—The state
472 chief information officer must demonstrate:

473 a. Strategic vision and innovation by possessing the
474 capability to modernize information technology systems, drive
475 digital transformation, and align information technology
476 initiatives with state goals;

477 b. Collaboration and engagement with stakeholders by
478 working with legislators, state agency heads, local governments,
479 and private sector partners to implement information technology
480 initiatives;

481 c. Crisis management and cyber resilience by possessing the
482 capability to develop and lead cyber incident response, disaster
483 recovery, and information technology continuity plans; and

484 d. Fiscal management and budget expertise managing multi-
485 million-dollar information technology budgets, cost-control
486 strategies, and financial oversight of information technology
487 projects.

488 (3) The deputy director of the division shall serve as the
489 deputy chief information officer.

490 (4) The director shall select separate individuals to serve
491 as the state chief information security officer, state chief
492 data officer, state chief technology officer, and state chief
493 technology procurement officer.

576-02812-26

2026480c2

494 Section 3. Until a state chief information officer is
495 appointed pursuant to s. 14.205, Florida Statutes, the current
496 state chief information officer of the Department of Management
497 Services shall be transferred to the Division of Integrated
498 Government Innovation and Technology and serve as interim state
499 chief information officer. A state chief information officer for
500 the Division of Integrated Government Innovation and Technology
501 must be appointed by the Governor by June 30, 2027.

502 Section 4. Subsection (6) of section 20.055, Florida
503 Statutes, is amended to read:

504 20.055 Agency inspectors general.-

505 (6) In carrying out the auditing duties and
506 responsibilities of this act, each inspector general shall
507 review and evaluate internal controls necessary to ensure the
508 fiscal accountability of the state agency. The inspector general
509 shall conduct financial, compliance, electronic data processing,
510 and performance audits of the agency and prepare audit reports
511 of his or her findings. The scope and assignment of the audits
512 are shall be determined by the inspector general; however, the
513 agency head may at any time request the inspector general to
514 perform an audit of a special program, function, or
515 organizational unit. In addition to the duties prescribed in
516 this section, each inspector general annually shall review and
517 report on whether agency practices related to information
518 technology reporting, projects, contracts, and procurements are
519 consistent with the applicable reporting requirements and
520 standards published by the Division of Integrated Government
521 Innovation and Technology within the Executive Office of the
522 Governor. The inspector general shall prepare an annual agency

576-02812-26

2026480c2

523 information technology compliance report that assesses the
524 adequacy of internal controls, documentation, and implementation
525 processes to ensure conformity with statewide information
526 technology governance, security, and performance standards. The
527 performance of the audits is ~~audit shall be~~ under the direction
528 of the inspector general, except that if the inspector general
529 does not possess the qualifications specified in subsection (4),
530 the director of auditing must ~~shall~~ perform the functions listed
531 in this subsection.

532 (a) Such audits must ~~shall~~ be conducted in accordance with
533 the current International Standards for the Professional
534 Practice of Internal Auditing as published by the Institute of
535 Internal Auditors, Inc., or, where appropriate, in accordance
536 with generally accepted governmental auditing standards. All
537 audit reports issued by internal audit staff must ~~shall~~ include
538 a statement that the audit was conducted pursuant to the
539 appropriate standards.

540 (b) Audit workpapers and reports are ~~shall be~~ public
541 records to the extent that they do not include information which
542 has been made confidential and exempt from the provisions of s.
543 119.07(1) pursuant to law. However, when the inspector general
544 or a member of the staff receives from an individual a complaint
545 or information that falls within the definition provided in s.
546 112.3187(5), the name or identity of the individual may not be
547 disclosed to anyone else without the written consent of the
548 individual, unless the inspector general determines that such
549 disclosure is unavoidable during the course of the audit or
550 investigation.

551 (c) The inspector general and the staff shall have access

576-02812-26

2026480c2

552 to any records, data, and other information of the state agency
553 he or she deems necessary to carry out his or her duties. The
554 inspector general may also request such information or
555 assistance as may be necessary from the state agency or from any
556 federal, state, or local government entity.

557 (d) At the conclusion of each audit, the inspector general
558 shall submit preliminary findings and recommendations to the
559 person responsible for supervision of the program function or
560 operational unit who shall respond to any adverse findings
561 within 20 working days after receipt of the preliminary
562 findings. Such response and the inspector general's rebuttal to
563 the response must ~~shall~~ be included in the final audit report.

564 (e) At the conclusion of an audit in which the subject of
565 the audit is a specific entity contracting with the state or an
566 individual substantially affected, if the audit is not
567 confidential or otherwise exempt from disclosure by law, the
568 inspector general must ~~shall~~, consistent with s. 119.07(1),
569 submit the findings to the entity contracting with the state or
570 the individual substantially affected, who must ~~shall~~ be advised
571 in writing that they may submit a written response within 20
572 working days after receipt of the findings. The response and the
573 inspector general's rebuttal to the response, if any, must be
574 included in the final audit report.

575 (f) The inspector general shall submit the final report to
576 the agency head, the Auditor General, and, for state agencies
577 under the jurisdiction of the Governor, the Chief Inspector
578 General.

579 1. The agency information technology compliance reports
580 must be submitted to the agency head, the Auditor General, and,

576-02812-26

2026480c2

581 for state agencies under the jurisdiction of the Governor, the
582 Chief Inspector General by September 30 of each year.

583 2. The Chief Inspector General shall review the annual
584 agency information technology compliance reports submitted by
585 agency inspectors general under the jurisdiction of the
586 Governor, and shall prepare a consolidated statewide information
587 technology compliance report summarizing agency performance,
588 findings, and recommendations for improvement. The consolidated
589 report must be submitted to the Executive Office of the
590 Governor, the President of the Senate, and the Speaker of the
591 House of Representatives by December 1 of each year.

592 3. Agency heads for agencies not under the jurisdiction of
593 the Governor shall submit the annual agency information
594 technology compliance reports to the Executive Office of the
595 Governor, the President of the Senate, and the Speaker of the
596 House of Representatives by December 1 of each year.

597 (g) The Auditor General, in connection with the independent
598 postaudit of the same agency pursuant to s. 11.45, shall give
599 appropriate consideration to internal audit reports and the
600 resolution of findings therein. The Legislative Auditing
601 Committee may inquire into the reasons or justifications for
602 failure of the agency head to correct the deficiencies reported
603 in internal audits that are also reported by the Auditor General
604 and shall take appropriate action.

605 (h) The inspector general shall monitor the implementation
606 of the state agency's response to any report on the state agency
607 issued by the Auditor General or by the Office of Program Policy
608 Analysis and Government Accountability. No later than 6 months
609 after the Auditor General or the Office of Program Policy

576-02812-26

2026480c2

610 Analysis and Government Accountability publishes a report on the
611 state agency, the inspector general shall provide a written
612 response to the agency head or, for state agencies under the
613 jurisdiction of the Governor, the Chief Inspector General on the
614 status of corrective actions taken. The inspector general shall
615 file a copy of such response with the Legislative Auditing
616 Committee.

617 (i) The inspector general shall develop long-term and
618 annual audit plans based on the findings of periodic risk
619 assessments. The plan, where appropriate, should include
620 postaudit samplings of payments and accounts. The plan must
621 ~~shall~~ show the individual audits to be conducted during each
622 year and related resources to be devoted to the respective
623 audits. The plan must ~~shall~~ include a specific cybersecurity
624 audit plan. The Chief Financial Officer, to assist in fulfilling
625 the responsibilities for examining, auditing, and settling
626 accounts, claims, and demands pursuant to s. 17.03(1), and
627 examining, auditing, adjusting, and settling accounts pursuant
628 to s. 17.04, may use audits performed by the inspectors general
629 and internal auditors. For state agencies under the jurisdiction
630 of the Governor, the audit plans must ~~shall~~ be submitted to the
631 Chief Inspector General. The plan must ~~shall~~ be submitted to the
632 agency head for approval. A copy of the approved plan must ~~shall~~
633 be submitted to the Auditor General.

634 Section 5. Paragraph (b) of subsection (3) of section
635 97.0525, Florida Statutes, is amended to read:

636 97.0525 Online voter registration.—

637 (3)

638 (b) The division shall conduct a comprehensive risk

576-02812-26

2026480c2

639 assessment of the online voter registration system every 2
640 years. The comprehensive risk assessment must comply with the
641 risk assessment methodology developed by the Division of
642 Integrated Government Innovation and Technology within the
643 Executive Office of the Governor ~~Department of Management~~
644 ~~Services~~ for identifying security risks, determining the
645 magnitude of such risks, and identifying areas that require
646 safeguards. In addition, the comprehensive risk assessment must
647 incorporate all of the following:

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

653 2. Screening of computers and networks used to support the
654 online voter registration system for malware and other
655 vulnerabilities.

656 3. Evaluation of database infrastructure, including
657 software and operating systems, in order to fortify defenses
658 against cyberattacks.

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

662 Section 6. Paragraphs (a) and (f) of subsection (1),
663 paragraphs (b) and (c) of subsection (2), and subsections (3)
664 and (4) of section 112.22, Florida Statutes, are amended to
665 read:

666 112.22 Use of applications from foreign countries of
667 concern prohibited.—

576-02812-26

2026480c2

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

669 (a) "DIGIT" means the Division of Integrated Government
670 Innovation and Technology within the Executive Office of the
671 Governor ~~"Department" means the Department of Management~~
672 ~~Services.~~

673 (f) "Prohibited application" means an application that
674 meets the following criteria:

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

678 a. Collecting keystrokes or sensitive personal, financial,
679 proprietary, or other business data;

680 b. Compromising e-mail and acting as a vector for
681 ransomware deployment;

682 c. Conducting cyber-espionage against a public employer;

683 d. Conducting surveillance and tracking of individual
684 users; or

685 e. Using algorithmic modifications to conduct
686 disinformation or misinformation campaigns; or

687 2. Any Internet application that DIGIT ~~the department~~ deems
688 to present a security risk in the form of unauthorized access to
689 or temporary unavailability of the public employer's records,
690 digital assets, systems, networks, servers, or information.

691 (2)

692 (b) A person, including an employee or officer of a public
693 employer, may not download or access any prohibited application
694 on any government-issued device.

695 1. This paragraph does not apply to a law enforcement
696 officer as defined in s. 943.10(1) if the use of the prohibited

576-02812-26

2026480c2

697 application is necessary to protect the public safety or conduct
698 an investigation within the scope of his or her employment.

699 2. A public employer may request a waiver from DIGIT ~~the~~
700 ~~department~~ to allow designated employees or officers to download
701 or access a prohibited application on a government-issued
702 device.

703 (c) Within 15 calendar days after DIGIT ~~the department~~
704 issues or updates its list of prohibited applications pursuant
705 to paragraph (3)(a), an employee or officer of a public employer
706 who uses a government-issued device must remove, delete, or
707 uninstall any prohibited applications from his or her
708 government-issued device.

709 (3) DIGIT ~~The department~~ shall do all of the following:

710 (a) Compile and maintain a list of prohibited applications
711 and publish the list on its website. DIGIT ~~The department~~ shall
712 update this list quarterly and shall provide notice of any
713 update to public employers.

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

717 1. A description of the activity to be conducted and the
718 state interest furthered by the activity.

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

721 3. The length of time necessary for the waiver. Any waiver
722 granted pursuant to subparagraph (2)(b)2. must be limited to a
723 timeframe of no more than 1 year, but DIGIT ~~the department~~ may
724 approve an extension.

725 4. Risk mitigation actions that will be taken to prevent

576-02812-26

2026480c2

726 access to sensitive data, including methods to ensure that the
727 activity does not connect to a state system, network, or server.

728 5. A description of the circumstances under which the
729 waiver applies.

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

735 ~~(b) DIGIT~~ The department shall adopt rules necessary to
736 administer this section.

737 Section 7. Paragraph (a) of subsection (5) of section
738 119.0725, Florida Statutes, is amended to read:

739 119.0725 Agency cybersecurity information; public records
740 exemption; public meetings exemption.—

741 (5) (a) Information made confidential and exempt pursuant to
742 this section must ~~shall~~ be made available to a law enforcement
743 agency, the Auditor General, the Cybercrime Office of the
744 Department of Law Enforcement, the Division of Integrated
745 Government Innovation and Technology within the Executive Office
746 of the Governor ~~Florida Digital Service within the Department of~~
747 ~~Management Services~~, and, for agencies under the jurisdiction of
748 the Governor, the Chief Inspector General.

749 Section 8. Paragraph (a) of subsection (4) and subsection
750 (7) of section 216.023, Florida Statutes, are amended to read:

751 216.023 Legislative budget requests to be furnished to
752 Legislature by agencies.—

753 (4) (a) The legislative budget request for each program must
754 contain:

576-02812-26

2026480c2

- 755 1. The constitutional or statutory authority for a program,
756 a brief purpose statement, and approved program components.
- 757 2. Information on expenditures for 3 fiscal years (actual
758 prior-year expenditures, current-year estimated expenditures,
759 and agency budget requested expenditures for the next fiscal
760 year) by appropriation category.
- 761 3. Details on trust funds and fees.
- 762 4. The total number of positions (authorized, fixed, and
763 requested).
- 764 5. An issue narrative describing and justifying changes in
765 amounts and positions requested for current and proposed
766 programs for the next fiscal year.
- 767 6. Information resource requests.
- 768 7. Supporting information, including applicable cost-
769 benefit analyses, business case analyses, performance
770 contracting procedures, service comparisons, and impacts on
771 performance standards for any request to outsource or privatize
772 agency functions. The cost-benefit and business case analyses
773 must include an assessment of the impact on each affected
774 activity from those identified in accordance with paragraph (b).
775 Performance standards must include standards for each affected
776 activity and be expressed in terms of the associated unit of
777 activity.
- 778 8. An evaluation of major outsourcing and privatization
779 initiatives undertaken during the last 5 fiscal years having
780 aggregate expenditures exceeding \$10 million during the term of
781 the contract. The evaluation must include an assessment of
782 contractor performance, a comparison of anticipated service
783 levels to actual service levels, and a comparison of estimated

576-02812-26

2026480c2

784 savings to actual savings achieved. Consolidated reports issued
785 by the Department of Management Services may be used to satisfy
786 this requirement.

787 9. Supporting information for any proposed consolidated
788 financing of deferred-payment commodity contracts including
789 guaranteed energy performance savings contracts. Supporting
790 information must also include narrative describing and
791 justifying the need, baseline for current costs, estimated cost
792 savings, projected equipment purchases, estimated contract
793 costs, and return on investment calculation.

794 10. For projects that exceed \$10 million in total cost, the
795 statutory reference of the existing policy or the proposed
796 substantive policy that establishes and defines the project's
797 governance structure, planned scope, main business objectives
798 that must be achieved, and estimated completion timeframes. The
799 governance structure for information technology-related projects
800 must incorporate the applicable project management and oversight
801 standards established pursuant to s. 282.0061 ~~s. 282.0051~~.
802 Information technology budget requests for the continuance of
803 existing hardware and software maintenance agreements, renewal
804 of existing software licensing agreements, or the replacement of
805 desktop units with new technology that is similar to the
806 technology currently in use are exempt from this requirement.

807 ~~(7) As part of the legislative budget request, each state~~
808 ~~agency and the judicial branch shall include an inventory of all~~
809 ~~ongoing technology-related projects that have a cumulative~~
810 ~~estimated or realized cost of more than \$1 million. The~~
811 ~~inventory must, at a minimum, contain all of the following~~
812 ~~information:~~

576-02812-26

2026480c2

- 813 ~~(a) The name of the technology system.~~
- 814 ~~(b) A brief description of the purpose and function of the~~
815 ~~system.~~
- 816 ~~(c) A brief description of the goals of the project.~~
- 817 ~~(d) The initiation date of the project.~~
- 818 ~~(e) The key performance indicators for the project.~~
- 819 ~~(f) Any other metrics for the project evaluating the health~~
820 ~~and status of the project.~~
- 821 ~~(g) The original and current baseline estimated end dates~~
822 ~~of the project.~~
- 823 ~~(h) The original and current estimated costs of the~~
824 ~~project.~~
- 825 ~~(i) Total funds appropriated or allocated to the project~~
826 ~~and the current realized cost for the project by fiscal year.~~
827
- 828 ~~For purposes of this subsection, an ongoing technology-related~~
829 ~~project is one which has been funded or has had or is expected~~
830 ~~to have expenditures in more than one fiscal year. An ongoing~~
831 ~~technology-related project does not include the continuance of~~
832 ~~existing hardware and software maintenance agreements, the~~
833 ~~renewal of existing software licensing agreements, or the~~
834 ~~replacement of desktop units with new technology that is~~
835 ~~substantially similar to the technology being replaced. This~~
836 ~~subsection expires July 1, 2026.~~
- 837 Section 9. Present subsections (36), (37), and (38) of
838 section 282.0041, Florida Statutes, are redesignated as
839 subsections (37), (38), and (39), respectively, new subsections
840 (11) and (36) are added to that section, and subsection (1),
841 present subsection (7), and subsections (27) and (29) of that

576-02812-26

2026480c2

842 section are amended, to read:

843 282.0041 Definitions.—As used in this chapter, the term:

844 ~~(1) "Agency assessment" means the amount each customer~~
845 ~~entity must pay annually for services from the Department of~~
846 ~~Management Services and includes administrative and data center~~
847 ~~services costs.~~

848 (6)~~(7)~~ "Customer entity" means an entity that obtains
849 services from DIGIT ~~the Department of Management Services.~~

850 (11) "DIGIT" means the Division of Integrated Government
851 Innovation and Technology within the Executive Office of the
852 Governor.

853 (27) "Project oversight" means an independent review and
854 assessment ~~analysis~~ of an information technology project that
855 provides information on the project's scope, completion
856 timeframes, and budget and that identifies and quantifies issues
857 or risks affecting the successful and timely completion of the
858 project.

859 (29) "Risk assessment" means the process of identifying
860 operational risks and security risks, determining their
861 magnitude, and identifying areas needing safeguards.

862 (36) "Technical debt" means the accumulated cost and
863 operational impact resulting from the use of suboptimal,
864 expedient, or outdated technology solutions that require future
865 remediation, refactoring, or replacement to ensure
866 maintainability, security, efficiency, and compliance with
867 enterprise architecture standards.

868 Section 10. Section 282.00515, Florida Statutes, is amended
869 to read:

870 282.00515 Duties of Cabinet agencies.—

576-02812-26

2026480c2

871 (1) (a) The Department of Legal Affairs, the Department of
872 Financial Services, and the Department of Agriculture and
873 Consumer Services shall adopt the standards, best practices,
874 processes, and methodologies established in s. 282.0061(4) and
875 (5) (b) and (d). However, such departments may ~~s. 282.0051(1) (b),~~
876 ~~(c), and (r) and (3) (e) or~~ adopt alternative standards, best
877 practices, and methodologies that must be based on industry-
878 recognized best practices and industry standards that enable
879 allow for open data exchange, interoperability, and vendor-
880 neutral integration. Such departments shall evaluate the
881 adoption of alternative standards on a case-by-case basis for
882 each standard, project, or system and reevaluate such
883 alternative standards periodically.

884 (b) Notwithstanding paragraph (a), if an enterprise project
885 has a measurable impact on, or requires participation from, a
886 state agency and the Department of Legal Affairs, the Department
887 of Financial Services, or the Department of Agriculture and
888 Consumer Services, then the Department of Legal Affairs, the
889 Department of Financial Services, or the Department of
890 Agriculture and Consumer Services, as applicable, must follow
891 the standards established under this chapter.

892 (2) If the Department of Legal Affairs, the Department of
893 Financial Services, or the Department of Agriculture and
894 Consumer Services adopts alternative standards, best practices,
895 processes, and methodologies in lieu of the ~~enterprise~~
896 ~~architecture~~ standards, best practices, processes, and
897 methodologies adopted pursuant to s. 282.0061(4) and (5) (b) and
898 (d) ~~s. 282.0051~~, such department must notify DIGIT, the
899 Governor, the President of the Senate, and the Speaker of the

576-02812-26

2026480c2

900 House of Representatives in writing of the adoption of the
901 alternative standards and provide a justification for adoption
902 of the alternative standards and explain the manner in which ~~how~~
903 the agency will achieve the policy, standard, guideline, or best
904 practice while promoting open data interoperability.

905 (3) The Department of Legal Affairs, the Department of
906 Financial Services, and the Department of Agriculture and
907 Consumer Services shall each conduct a full baseline needs
908 assessment to document their respective technical environments,
909 existing technical debt, security risks, and compliance with
910 adopted information technology best practices, guidelines, and
911 standards, similar to the assessments conducted by DIGIT
912 pursuant to s. 282.0061(2) (a) and (b). The Department of Legal
913 Affairs, the Department of Financial Services, and the
914 Department of Agriculture and Consumer Services may contract
915 with DIGIT to assist with or complete the assessments.

916 (4) The Department of Legal Affairs, the Department of
917 Financial Services, and the Department of Agriculture and
918 Consumer Services shall each produce a phased roadmap for
919 strategic planning to address known technology gaps and
920 deficiencies, similar to the assessments conducted by DIGIT
921 pursuant to s. 282.0061(2) (d). The phased roadmap must be
922 submitted annually with legislative budget requests required
923 under s. 216.023. The Department of Legal Affairs, the
924 Department of Financial Services, and the Department of
925 Agriculture and Consumer Services may contract with DIGIT to
926 assist with or complete the phased roadmap.

927 (5) The Department of Legal Affairs, the Department of
928 Financial Services, and the Department of Agriculture and

576-02812-26

2026480c2

929 Consumer Services may, but are not required to, contract with
930 DIGIT ~~the department~~ to provide procurement advisory and review
931 services for information technology projects as provided in s.
932 282.0061(5)(a) ~~or perform any of the services and functions~~
933 ~~described in s. 282.0051.~~

934 (6) The Department of Legal Affairs, the Department of
935 Financial Services, and the Department of Agriculture and
936 Consumer Services shall use the information technology reports
937 developed by DIGIT pursuant to s. 282.0061(5)(f) and follow the
938 streamlined reporting process pursuant to s. 282.0061(5)(i). The
939 Department of Legal Affairs, the Department of Financial
940 Services, and the Department of Agriculture and Consumer
941 Services shall report annually to the President of the Senate
942 and the Speaker of the House of Representatives by December 15
943 information related to the respective department similar to the
944 information required under s. 282.006(6)(a) and the information
945 technology financial data methodology and reporting required by
946 s. 282.0061(6). The Department of Legal Affairs, the Department
947 of Financial Services, and the Department of Agriculture and
948 Consumer Services may provide the report required under this
949 subsection collectively with DIGIT or shall report separately to
950 the Governor, the President of the Senate, and the Speaker of
951 the House of Representatives.

952 (7)(a) ~~(4)(a)~~ Nothing in this chapter ~~section or in s.~~
953 282.0051 requires the Department of Legal Affairs, the
954 Department of Financial Services, or the Department of
955 Agriculture and Consumer Services to integrate with information
956 technology outside its own department or with DIGIT ~~the Florida~~
957 ~~Digital Service.~~

576-02812-26

2026480c2

958 (b) ~~DIGIT The department, acting through the Florida~~
959 ~~Digital Service,~~ may not retrieve or disclose any data without a
960 shared-data agreement in place between DIGIT ~~the department~~ and
961 the Department of Legal Affairs, the Department of Financial
962 Services, or the Department of Agriculture and Consumer
963 Services.

964 (8) Notwithstanding s. 282.0061(5) (h), DIGIT may perform
965 project oversight only on information technology projects of the
966 Department of Legal Affairs, the Department of Financial
967 Services, and the Department of Agriculture and Consumer
968 Services which have a project cost of \$20 million or more. Such
969 information technology projects must also comply with the
970 applicable information technology architecture, project
971 management and oversight, and reporting standards established by
972 DIGIT. DIGIT shall report by the 30th day after the end of each
973 quarter to the President of the Senate and the Speaker of the
974 House of Representatives on any information technology project
975 under this subsection which DIGIT identifies as high risk. The
976 report must include a risk assessment, including fiscal risks,
977 associated with proceeding to the next stage of the project, and
978 a recommendation for any corrective action required, including
979 suspension or termination of the project.

980 (9) If an information technology project implemented by a
981 state agency must be connected to or otherwise accommodated by
982 an information technology system administered by the Department
983 of Legal Affairs, the Department of Financial Services, or the
984 Department of Agriculture and Consumer Services, the state
985 agency must consult with DIGIT regarding the risks and other
986 effects of such project on the information technology systems of

576-02812-26

2026480c2

987 the Department of Legal Affairs, the Department of Financial
988 Services, or the Department of Agriculture and Consumer
989 Services, as applicable, and must work cooperatively with the
990 Department of Legal Affairs, the Department of Financial
991 Services, or the Department of Agriculture and Consumer
992 Services, as applicable, regarding connections, interfaces,
993 timing, or accommodations required to implement such project.

994 Section 11. Section 282.006, Florida Statutes, is created
995 to read:

996 282.006 Division of Integrated Government Innovation and
997 Technology; enterprise responsibilities; reporting.-

998 (1) The Division of Integrated Government Innovation and
999 Technology established in s. 14.205 is the state organization
1000 for information technology governance and is the lead entity
1001 responsible for understanding the unique state agency
1002 information technology needs and environments, creating
1003 technology standards and strategy, supporting state agency
1004 technology efforts, and reporting on the status of technology
1005 for state agencies.

1006 (2) The Legislature intends for DIGIT policy, standards,
1007 guidance, and oversight to allow for adaptability to emerging
1008 technology and organizational needs while maintaining compliance
1009 with industry best practices. All policies, standards, and
1010 guidelines established pursuant to this chapter must be
1011 technology-agnostic and may not prescribe specific tools,
1012 platforms, or vendors.

1013 (3) DIGIT shall establish the strategic direction of
1014 information technology for state agencies. DIGIT shall develop
1015 and publish information technology policy that aligns with

576-02812-26

2026480c2

1016 industry best practices for the management of the state's
1017 information technology resources. The policy must be updated as
1018 necessary to meet the requirements of this chapter and
1019 advancements in technology.

1020 (4) DIGIT shall, in coordination with state agency
1021 technology subject matter experts, develop, publish, and
1022 maintain an enterprise architecture that:

1023 (a) Acknowledges the unique needs of the entities within
1024 the enterprise in the development and publication of standards
1025 and terminologies to facilitate digital interoperability;

1026 (b) Supports the cloud-first policy as specified in s.
1027 282.206;

1028 (c) Addresses the manner in which information technology
1029 infrastructure may be modernized to achieve security,
1030 scalability, maintainability, interoperability, and improved
1031 cost-efficiency goals; and

1032 (d) Includes, at a minimum, best practices, guidelines, and
1033 standards for:

1034 1. Data models and taxonomies.

1035 2. Master data management.

1036 3. Data integration and interoperability.

1037 4. Data security and encryption.

1038 5. Bot prevention and data protection.

1039 6. Data backup and recovery.

1040 7. Application portfolio and catalog requirements.

1041 8. Application architectural patterns and principles.

1042 9. Technology and platform standards.

1043 10. Secure coding practices.

1044 11. Performance and scalability.

576-02812-26

2026480c2

- 1045 12. Cloud infrastructure and architecture.
- 1046 13. Networking, connectivity, and security protocols.
- 1047 14. Authentication, authorization, and access controls.
- 1048 15. Disaster recovery.
- 1049 16. Quality assurance.
- 1050 17. Testing methodologies and measurements.
- 1051 18. Logging and log retention.
- 1052 19. Application and use of artificial intelligence.
- 1053 (5) DIGIT shall develop open data technical standards and
- 1054 terminologies for use by state agencies. DIGIT shall develop
- 1055 enterprise technology testing and quality assurance best
- 1056 practices and standards to ensure the reliability, security, and
- 1057 performance of information technology systems. Such best
- 1058 practices and standards must include:
- 1059 (a) Functional testing to ensure software or systems meet
- 1060 required specifications.
- 1061 (b) Performance and load testing to ensure software and
- 1062 systems operate efficiently under various conditions.
- 1063 (c) Security testing to protect software and systems from
- 1064 vulnerabilities and cyber threats.
- 1065 (d) Compatibility and interoperability testing to ensure
- 1066 software and systems operate seamlessly across environments.
- 1067 (6) DIGIT shall produce and provide the following reports
- 1068 to the Governor, the President of the Senate, and the Speaker of
- 1069 the House of Representatives:
- 1070 (a) Annually by December 15, an enterprise analysis report
- 1071 for state agencies which includes all of the following:
- 1072 1. Results of the state agency needs assessments, including
- 1073 any plan to address technical debt as required by s. 282.0061

576-02812-26

2026480c2

1074 pursuant to the schedule adopted.

1075 2. Alternative standards related to federal funding adopted
1076 pursuant to s. 282.0061.

1077 3. Information technology financial data for each state
1078 agency for the previous fiscal year. This portion of the annual
1079 report must include, at a minimum, the following recurring and
1080 nonrecurring information:

1081 a. Total number of full-time equivalent positions.

1082 b. Total amount of salary.

1083 c. Total amount of benefits.

1084 d. Total number of comparable full-time equivalent
1085 positions and total amount of expenditures for information
1086 technology staff augmentation.

1087 e. Total number of contracts and purchase orders and total
1088 amount of associated expenditures for information technology
1089 managed services.

1090 f. Total amount of expenditures by state term contract as
1091 defined in s. 287.012, contracts procured using alternative
1092 purchasing methods as authorized pursuant to s. 287.042(16), and
1093 state agency procurements through request for proposal,
1094 invitation to negotiate, invitation to bid, single source, and
1095 emergency purchases.

1096 g. Total amount of expenditures for hardware.

1097 h. Total amount of expenditures for non-cloud software.

1098 i. Total amount of expenditures for cloud software licenses
1099 and services with a separate amount for expenditures for state
1100 data center services.

1101 j. Total amount of expenditures for cloud data center
1102 services with a separate amount for expenditures for state data

576-02812-26

2026480c2

1103 center services.

1104 k. Total amount of expenditures for administrative costs.

1105 4. Consolidated information for the previous fiscal year
1106 about state information technology projects, which must include,
1107 at a minimum, the following information:

1108 a. Anticipated funding requirements for information
1109 technology support over the next 5 years.

1110 b. An inventory of current information technology assets
1111 and major projects. As used in this paragraph, the term "major
1112 project" includes projects costing more than \$500,000 to
1113 implement.

1114 c. Significant unmet needs for information technology
1115 resources over the next 5 fiscal years, ranked in priority order
1116 according to their urgency.

1117 5. A review and summary of whether the information
1118 technology contract policy established pursuant to s. 282.0064
1119 is included in all solicitations and contracts.

1120 (b) Biennially by December 15 of even-numbered years, a
1121 report on the strategic direction of information technology in
1122 the state which includes recommendations for all of the
1123 following:

1124 1. Standardization and consolidation of information
1125 technology services that are identified as common across state
1126 agencies as required in s. 282.0061.

1127 2. Information technology services needed to be designed,
1128 delivered, and managed as state agency enterprise information
1129 technology services. Recommendations must include the
1130 identification of existing information technology resources
1131 associated with the services, if existing services must be

576-02812-26

2026480c2

1132 transferred as a result of being delivered and managed as
1133 enterprise information technology services, and which entity is
1134 best suited to manage the service.

1135 (c)1. When conducted as provided in this paragraph, a
1136 market analysis and accompanying strategic plan submitted by
1137 December 31 of each year that the market analysis is conducted.

1138 2. No less frequently than every 3 years, DIGIT shall
1139 conduct a market analysis to determine whether the:

1140 a. Information technology resources across state agencies
1141 are used in the most cost-effective and cost-efficient manner,
1142 while recognizing that the replacement of certain legacy
1143 information technology systems within the enterprise may be cost
1144 prohibitive or cost inefficient due to the remaining useful life
1145 of those resources; and

1146 b. State agencies are using best practices with respect to
1147 information technology, information services, and the
1148 acquisition of emerging technologies and information services.

1149 3. Each market analysis must be used to prepare a strategic
1150 plan for continued and future information technology and
1151 information services, including, but not limited to, proposed
1152 acquisitions of new services or technologies and approaches to
1153 the implementation of any new services or technologies.

1154 (7) (a) DIGIT shall develop, implement, and maintain a
1155 library to serve as the official repository for all enterprise
1156 information technology policies, standards, guidelines, and best
1157 practices applicable to state agencies. The online library must
1158 be accessible and searchable by all state agencies and the
1159 Department of Legal Affairs, the Department of Financial
1160 Services, and the Department of Agriculture and Consumer

576-02812-26

2026480c2

1161 Services through a secure authentication system. The library
1162 must include standardized checklists organized by technical
1163 subject areas to assist state agencies in measuring compliance
1164 with the information technology policies, standards, guidelines,
1165 and best practices.

1166 (b) DIGIT shall establish procedures to ensure the
1167 integrity, security, and availability of the library, including
1168 appropriate access controls, encryption, and disaster recovery
1169 measures. DIGIT shall regularly update documents and materials
1170 in the library to reflect current state and federal
1171 requirements, industry best practices, and emerging technologies
1172 and shall maintain version control and revision history for all
1173 published documents. DIGIT shall create mechanisms for state
1174 agencies to submit feedback, request clarifications, and
1175 recommend updates.

1176 (8) (a) Each state agency shall actively participate and
1177 collaborate with DIGIT to achieve the objectives set forth in
1178 this chapter. Each state agency shall also adhere to the
1179 policies, standards, guidelines, and best practices established
1180 by DIGIT in information technology planning, procurement,
1181 implementation, and operations as required by this chapter.

1182 (b)1. A state agency may request an exemption to a specific
1183 policy, standard, or guideline when compliance is not
1184 technically feasible, would cause undue hardship, or conflicts
1185 with any agency-specific statutory requirement. The state agency
1186 requesting an exemption must submit a formal justification to
1187 DIGIT detailing all of the following:

1188 a. The specific requirement for which an exemption is
1189 sought.

576-02812-26

2026480c2

1190 b. The reason compliance is not feasible or practical.

1191 c. Any compensating control or alternative measure the
1192 state agency will implement to mitigate associated risks.

1193 d. The anticipated duration of the exemption.

1194 2. DIGIT shall review all exemption requests and provide a
1195 recommendation to the state chief information officer, who shall
1196 present the compliance exemption requests to the chief
1197 information officer workgroup. Approval of exemption requests
1198 must be made by a majority vote of the workgroup. Approved
1199 exemptions must be documented and include conditions and
1200 expiration dates.

1201 3. A state agency with an approved exemption shall undergo
1202 periodic review to determine whether the exemption remains
1203 necessary or whether compliance can be achieved.

1204 (9) DIGIT may adopt rules to implement this chapter.

1205 Section 12. Section 282.0061, Florida Statutes, is created
1206 to read:

1207 282.0061 DIGIT support of state agencies; information
1208 technology procurement and projects.-

1209 (1) LEGISLATIVE INTENT.-The Legislature intends for DIGIT
1210 to support state agencies in their information technology
1211 efforts through the adoption of policies, standards, and
1212 guidance and by providing oversight that recognizes unique state
1213 agency information technology needs, environments, and goals.
1214 DIGIT assistance and support must allow for adaptability to
1215 emerging technologies and organizational needs while maintaining
1216 compliance with industry best practices. DIGIT may not prescribe
1217 specific tools, platforms, or vendors.

1218 (2) NEEDS ASSESSMENTS.-

576-02812-26

2026480c2

1219 (a) By January 1, 2029, DIGIT shall conduct full baseline
1220 needs assessments of state agencies to document their respective
1221 technical environments, existing technical debt, security risks,
1222 and compliance with all information technology standards and
1223 guidelines developed and published by DIGIT. The needs
1224 assessment must use the latest version of the Capability
1225 Maturity Model Integration to evaluate each state agency's
1226 information technology capabilities, providing a maturity level
1227 rating for each assessed domain. After completion of the initial
1228 full baseline needs assessment, such assessments must be
1229 maintained and updated on a regular schedule adopted by DIGIT.

1230 (b) In assessing the existing technical debt portion of the
1231 needs assessment, DIGIT shall analyze the state's legacy
1232 information technology systems and develop a plan to document
1233 the needs and costs for replacement systems. The plan must
1234 include an inventory of legacy applications and infrastructure;
1235 the required capabilities not available with the legacy system;
1236 the estimated process, timeline, and cost to migrate from legacy
1237 environments; and any other information necessary for fiscal or
1238 technology planning. The plan must determine and document the
1239 estimated timeframe during which the state agency can continue
1240 to efficiently use legacy information technology systems,
1241 resources, security, and data management to support operations.
1242 State agencies shall provide all necessary documentation to
1243 enable accurate reporting on legacy systems.

1244 (c) DIGIT shall develop a plan and schedule to conduct the
1245 initial full baseline needs assessments. By October 1, 2027,
1246 DIGIT shall submit the plan to the Governor, the President of
1247 the Senate, and the Speaker of the House of Representatives.

576-02812-26

2026480c2

1248 (d) DIGIT shall support state agency strategic planning
1249 efforts and assist state agencies with the production of a
1250 phased roadmap to address known technology gaps and deficiencies
1251 as identified in the needs assessments. The roadmaps must
1252 include specific strategies and initiatives aimed at advancing
1253 the state agency's maturity level in accordance with the latest
1254 version of the Capability Maturity Model Integration. State
1255 agencies shall create, maintain, and submit the roadmap on an
1256 annual basis with their legislative budget requests required
1257 under s. 216.023.

1258 (3) STANDARDIZATION.—DIGIT shall:

1259 (a) Recommend in its annual enterprise analysis report for
1260 state agencies required under s. 282.006 any potential method
1261 for standardizing data across state agencies which will promote
1262 interoperability and reduce the collection of duplicative data.

1263 (b) Identify any opportunities in such enterprise analysis
1264 report for state agencies for standardization and consolidation
1265 of information technology services that are common across all
1266 state agencies and that support:

1267 1. Improved interoperability, security, scalability,
1268 maintainability, and cost efficiency; and

1269 2. Business functions and operations, including
1270 administrative functions such as purchasing, accounting and
1271 reporting, cash management, and personnel.

1272 (c) Review all state agency information technology
1273 legislative budget requests for compliance with the enterprise
1274 architecture, project planning standards, and cybersecurity, and
1275 provide a report of the findings to the Executive Office of the
1276 Governor's Office of Policy and Budget for consideration for

576-02812-26

2026480c2

1277 funding decisions in the Governor's recommended budget.

1278 (4) DATA MANAGEMENT.—

1279 (a) DIGIT shall develop standards for use by state agencies
1280 which support best practices for master data management at the
1281 state agency level to facilitate enterprise data sharing and
1282 interoperability.

1283 (b) DIGIT shall establish a methodology and strategy for
1284 implementing statewide master data management and submit a
1285 report to the Governor, the President of the Senate, and the
1286 Speaker of the House of Representatives by December 1, 2029. The
1287 report must include the vision, goals, and benefits of
1288 implementing a statewide master data management initiative, an
1289 analysis of the current state of data management, and the
1290 recommended strategy, methodology, and estimated timeline and
1291 resources needed at a state agency and enterprise level to
1292 accomplish the initiative.

1293 (5) INFORMATION TECHNOLOGY PROJECTS.—DIGIT has the
1294 following duties and responsibilities related to state agency
1295 technology projects:

1296 (a) Provide procurement advisory and review services for
1297 information technology projects to all state agencies, including
1298 procurement and contract development assistance to meet the
1299 information technology contract policy established pursuant to
1300 s. 282.0064.

1301 (b) Establish best practices and procurement processes, and
1302 develop metrics to support these processes for the procurement
1303 of information technology products and services in order to
1304 reduce costs or improve the provision of government services.

1305 (c) Upon request, assist state agencies in the development

576-02812-26

2026480c2

1306 of information technology-related legislative budget requests.

1307 (d) Develop standards and accountability measures for
1308 information technology project planning and implementation,
1309 including criteria for effective project management and
1310 oversight. State agencies shall satisfy these standards and
1311 measures when implementing information technology projects. To
1312 support data-driven decisionmaking, the standards and measures
1313 must include, but are not limited to:

1314 1. Performance measurements and metrics that objectively
1315 assess the progress and risks of an information technology
1316 project based on a defined and documented project scope, to
1317 include the number of impacted stakeholders, cost, and schedule,
1318 to determine whether the project is performing as planned and
1319 delivering the intended outcomes.

1320 2. Methodologies for calculating and defining acceptable
1321 variances between the planned and actual scope of a technology
1322 project which provide clear thresholds for guiding corrective
1323 actions. Such methodologies must account for project complexity
1324 and scale, schedule, performance, quality, and the cost of an
1325 information technology project.

1326 3. Reporting requirements that ensure timely notifications
1327 to all defined stakeholders when an information technology
1328 project exceeds acceptable variances defined and documented in a
1329 project plan, including any variance that results in a schedule
1330 delay of 1 month or more, or a cost increase of \$1 million or
1331 more, and that establish procedures for escalating critical
1332 issues to appropriate individuals.

1333 4. Technical reporting metrics to determine if an
1334 information technology project complies with the enterprise

576-02812-26

2026480c2

1335 architecture standards.

1336 5. Minimum requirements for engaging stakeholders
1337 throughout a project's life cycle.

1338 (e) Develop a framework that provides processes,
1339 activities, and deliverables state agencies must comply with
1340 when planning an information technology project. The processes,
1341 activities, and deliverables must include, but are not limited
1342 to, all of the following:

1343 1. Business case development, including the information
1344 required by s. 287.0571(4), full life cycle cost estimates,
1345 governance structure, system interoperability goals, data
1346 management plans, scalability approach, evaluation of
1347 cybersecurity and data privacy risks, and technology-specific
1348 performance metrics and service levels.

1349 2. Market research, including the use of a request for
1350 information as defined in s. 287.012.

1351 3. Planning and scheduling.

1352 4. Stakeholder engagement.

1353 5. Risk assessment.

1354 6. Procurement strategy.

1355 7. Project governance definition.

1356 8. System design and requirements.

1357 9. Change management.

1358 10. Monitoring and reporting.

1359 11. Postimplementation review and planning.

1360 12. Solicitation documentation.

1361 (f) Develop information technology project reports for use
1362 by state agencies, including, but not limited to, operational
1363 work plans, project spending plans, and project status reports.

576-02812-26

2026480c2

1364 Reporting standards must include content, format, and frequency
1365 of project updates.

1366 (g) Develop and provide training specific to information
1367 technology project management and oversight which supplements
1368 and enhances the training offered by the department and the
1369 Chief Financial Officer under s. 287.057(15)(b). DIGIT shall
1370 evaluate such training every 2 years to assess its effectiveness
1371 and update the training curriculum. The training must address
1372 the unique requirements and risk profiles of state information
1373 technology projects, procurements, contract management, and
1374 vendor management.

1375 (h) Perform project oversight on all state agency
1376 information technology projects that have total project costs of
1377 \$10 million or more. DIGIT shall report by the 30th day after
1378 the end of each quarter to the Executive Office of the Governor,
1379 the President of the Senate, and the Speaker of the House of
1380 Representatives on any information technology project that DIGIT
1381 identifies as high-risk due to the project exceeding the
1382 acceptable project variance thresholds provided in the project
1383 management and oversight standards. The report must include a
1384 risk assessment, including fiscal risks associated with
1385 proceeding to the next stage of the project, a list of all
1386 projects with a performance deficiency, reported pursuant to s.
1387 287.057(26)(d)1., which has not been corrected as of the end of
1388 the reporting period, and a recommendation for corrective
1389 actions required, including suspension or termination of the
1390 project.

1391 (i) Establish a streamlined reporting process with clear
1392 timelines and escalation procedures for notifying a state agency

576-02812-26

2026480c2

1393 of noncompliance with the standards developed and adopted by
1394 DIGIT.

1395 (j) Develop and maintain standards, performance metrics,
1396 and evaluation tools to measure the performance of information
1397 technology vendors that provide information technology
1398 commodities or services to the state. The standards, metrics,
1399 and tools must:

1400 1. Be organized by vendor category, reflecting the
1401 different roles, services, and risk profiles of information
1402 technology vendors, including, but not limited to, software,
1403 cloud services, infrastructure, cybersecurity, systems
1404 integration, and professional services.

1405 2. Include objective, measurable criteria to assess vendor
1406 performance, which criteria may include timeliness, quality of
1407 deliverables, cost control, compliance with contract
1408 requirements, security and privacy practices, responsiveness,
1409 and customer satisfaction.

1410 3. Provide for the collection and analysis of performance
1411 data across state agencies to support consistent and comparable
1412 evaluations.

1413 4. Support a scoring mechanism that may be used in
1414 procurement and contract management processes, including the
1415 identification of vendors eligible for inclusion on a preferred
1416 vendors list established by DIGIT.

1417 5. Provide for the public availability of the preferred
1418 vendors list, including vendor rankings by category, in a manner
1419 determined by DIGIT.

1420 6. Require that, to the extent permitted by law, priority
1421 consideration in future procurements be given to vendors on the

576-02812-26

2026480c2

1422 preferred vendors list based on performance ranking and cost, as
1423 applicable to the procurement method used.

1424 7. Be periodically reviewed and updated to reflect evolving
1425 technology, market conditions, and state needs.

1426 (6) INFORMATION TECHNOLOGY FINANCIAL DATA.—

1427 (a) In consultation with state agencies, DIGIT shall create
1428 a methodology, an approach, and applicable templates and formats
1429 for identifying and collecting both current and planned
1430 information technology expenditure data at the state agency
1431 level. DIGIT shall continuously obtain, review, and maintain
1432 records of the appropriations, expenditures, and revenues for
1433 information technology for each state agency.

1434 (b) DIGIT shall prescribe the format for state agencies to
1435 provide all necessary financial information to DIGIT for
1436 inclusion in the annual report required under s. 282.006. State
1437 agencies shall provide the information to DIGIT by October 1 for
1438 the previous fiscal year.

1439 (7) FEDERAL CONFLICTS.—DIGIT must work with state agencies
1440 to provide alternative standards, policies, or requirements that
1441 do not conflict with federal regulations or requirements if
1442 adherence to standards or policies adopted by or established
1443 pursuant to this section conflict with federal regulations or
1444 requirements imposed on an entity within the enterprise and
1445 results in, or is expected to result in, adverse action against
1446 any state agency or loss of federal funding.

1447 Section 13. Section 282.0062, Florida Statutes, is created
1448 to read:

1449 282.0062 DIGIT workgroups.—The following workgroups are
1450 established within DIGIT to facilitate coordination with state

576-02812-26

2026480c2

1451 agencies:

1452 (1) CHIEF INFORMATION OFFICER WORKGROUP.—

1453 (a) The chief information officer workgroup, composed of
1454 all state agency chief information officers, shall consider and
1455 make recommendations to the state chief information officer and
1456 the state chief information architect on such matters as
1457 enterprise information technology policies, standards, services,
1458 and architecture. The workgroup may also identify and recommend
1459 opportunities for the establishment of public-private
1460 partnerships when considering technology infrastructure and
1461 services in order to accelerate project delivery and provide a
1462 source of new or increased project funding.

1463 (b) At a minimum, the state chief information officer shall
1464 consult with the workgroup on a quarterly basis with regard to
1465 executing the duties and responsibilities of the state agencies
1466 related to statewide information technology strategic planning
1467 and policy.

1468 (2) ENTERPRISE DATA AND INTEROPERABILITY WORKGROUP.—

1469 (a) The enterprise data and interoperability workgroup,
1470 composed of chief data officer representatives from all state
1471 agencies, shall consider and make recommendations to the state
1472 chief data officer on such matters as enterprise data policies,
1473 standards, services, and architecture that promote data
1474 consistency, accessibility, and seamless integration across the
1475 enterprise.

1476 (b) At a minimum, the state chief data officer shall
1477 consult with the workgroup on a quarterly basis with regard to
1478 executing the duties and responsibilities of the state agencies
1479 related to statewide data governance planning and policy.

576-02812-26

2026480c2

1480 (3) ENTERPRISE SECURITY WORKGROUP.—

1481 (a) The enterprise security workgroup, composed of chief
1482 information security officer representatives from all state
1483 agencies, shall consider and make recommendations to the state
1484 chief information security officer on such matters as
1485 cybersecurity policies, standards, services, and architecture
1486 that promote the protection of state assets.

1487 (b) At a minimum, the state chief information security
1488 officer shall consult with the workgroup on a quarterly basis
1489 with regard to executing the duties and responsibilities of the
1490 state agencies related to cybersecurity governance and policy
1491 development.

1492 (4) ENTERPRISE INFORMATION TECHNOLOGY QUALITY ASSURANCE
1493 WORKGROUP.—

1494 (a) The enterprise information technology quality assurance
1495 workgroup, composed of testing and quality assurance
1496 representatives from all state agencies, shall consider and make
1497 recommendations to the state chief technology officer on such
1498 matters as testing methodologies, tools, and best practices to
1499 reduce risks related to software defects, cybersecurity threats,
1500 and operational failures.

1501 (b) At a minimum, the state chief information officer shall
1502 consult with the workgroup on a quarterly basis with regard to
1503 executing the duties and responsibilities of the state agencies
1504 related to enterprise software testing and quality assurance
1505 standards.

1506 (5) ENTERPRISE INFORMATION TECHNOLOGY PROJECT MANAGEMENT
1507 WORKGROUP.—

1508 (a) The enterprise information technology project

576-02812-26

2026480c2

1509 management workgroup, composed of information technology project
1510 manager representatives from all state agencies, shall consider
1511 and make recommendations to the state chief technology officer
1512 on such matters as information technology project management
1513 policies, standards, accountability measures, and services that
1514 promote project governance and standardization across the
1515 enterprise.

1516 (b) At a minimum, the state chief information officer shall
1517 consult with the workgroup on a quarterly basis with regard to
1518 executing the duties and responsibilities of the state agencies
1519 related to project management and oversight.

1520 (6) ENTERPRISE INFORMATION TECHNOLOGY PURCHASING
1521 WORKGROUP.—

1522 (a) The enterprise information technology purchasing
1523 workgroup, composed of information technology procurement
1524 representatives from all state agencies, shall consider and make
1525 recommendations to the state chief technology procurement
1526 officer on such matters as information technology procurement
1527 policies, standards, and purchasing strategy and optimization
1528 that promote best practices for contract negotiation,
1529 consolidation, and effective service-level agreement
1530 implementation across the enterprise.

1531 (b) At a minimum, the state chief information officer shall
1532 consult with the workgroup on a quarterly basis with regard to
1533 executing the duties and responsibilities of the state agencies
1534 related to technology evaluation, purchasing, and cost savings.

1535 (7) DEPARTMENT OF LEGAL AFFAIRS, DEPARTMENT OF FINANCIAL
1536 SERVICES, AND DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES
1537 INFORMATION TECHNOLOGY STAFF.—Appropriate information technology

576-02812-26

2026480c2

1538 staff of the Department of Legal Affairs, the Department of
1539 Financial Services, and the Department of Agriculture and
1540 Consumer Services shall participate in the workgroups created
1541 under subsections (1), (2), and (3) and may participate in any
1542 other workgroups as authorized by their respective elected
1543 official.

1544 Section 14. Section 282.0063, Florida Statutes, is created
1545 to read:

1546 282.0063 State information technology professionals career
1547 paths and training.—

1548 (1) DIGIT shall develop standardized frameworks for, and
1549 career paths, progressions, and training programs for, the
1550 benefit of state agency information technology personnel. To
1551 meet that goal, DIGIT shall:

1552 (a) Assess current and future information technology
1553 workforce needs across state agencies, identify skill gaps, and
1554 develop strategies to address them.

1555 (b) Develop and establish a training program for state
1556 agencies to support the understanding and implementation of each
1557 element of the enterprise architecture.

1558 (c) Establish training programs, certifications, and
1559 continuing education opportunities to enhance information
1560 technology competencies, including cybersecurity, cloud
1561 computing, and emerging technologies.

1562 (d) Support initiatives to provide existing employees with
1563 training or other opportunities to develop skills in emerging
1564 technologies and automation, ensuring that state agencies remain
1565 competitive and innovative.

1566 (e) Develop strategies to recruit and retain information

576-02812-26

2026480c2

1567 technology professionals, including internship programs,
1568 apprenticeships, partnerships with educational institutions,
1569 scholarships for service, and initiatives to attract diverse
1570 talent.

1571 (2) DIGIT shall consult with CareerSource Florida, Inc.,
1572 the Department of Commerce, and the Department of Education in
1573 the implementation of this section.

1574 Section 15. Section 282.0064, Florida Statutes, is created
1575 to read:

1576 282.0064 Information technology contract policy.-

1577 (1) In coordination with the Department of Management
1578 Services, DIGIT shall establish a policy for all information
1579 technology-related solicitations and contracts, including state
1580 term contracts; contracts sourced using alternative purchasing
1581 methods as authorized pursuant to s. 287.042(16); sole source
1582 and emergency procurements; and contracts for commodities,
1583 consultant services, and staff augmentation services.

1584 (2) Related to state term contracts, the information
1585 technology policy must include:

1586 (a) Identification of the information technology product
1587 and service categories to be included in state term contracts.

1588 (b) The term of each information technology-related state
1589 term contract.

1590 (c) The maximum number of vendors authorized on each state
1591 term contract.

1592 (3) For all contracts, the information technology policy
1593 must include:

1594 (a) Evaluation criteria for the award of information
1595 technology-related contracts.

576-02812-26

2026480c2

1596 (b) Requirements to be included in solicitations.

1597 (c) At a minimum, a requirement that any contract for
1598 information technology commodities or services meet the
1599 requirements of the enterprise architecture and National
1600 Institute of Standards and Technology Cybersecurity Framework.

1601 (4) The policy must include the following requirements for
1602 any information technology project that requires project
1603 oversight through independent verification and validation:

1604 (a) An entity providing independent verification and
1605 validation may not have any:

1606 1. Technical, managerial, or financial interest in the
1607 project; or

1608 2. Responsibility for or participation in any other aspect
1609 of the project.

1610 (b) The primary objective of independent verification and
1611 validation must be to provide an objective assessment throughout
1612 the entire project life cycle, reporting directly to all
1613 relevant stakeholders. An independent verification and
1614 validation entity shall independently verify and validate
1615 whether:

1616 1. The project is being built and implemented in accordance
1617 with defined technical architecture, specifications, and
1618 requirements.

1619 2. The project is adhering to established project
1620 management processes.

1621 3. The procurement of products, tools, and services and
1622 resulting contracts aligns with current statutory and regulatory
1623 requirements.

1624 4. The value of services delivered is commensurate with

576-02812-26

2026480c2

1625 project costs.

1626 5. The completed project meets the actual needs of the
1627 intended users.

1628 (c) The entity performing independent verification and
1629 validation shall provide regular reports and assessments
1630 directly to the designated oversight body, identifying risks,
1631 deficiencies, and recommendations for corrective actions to
1632 ensure project success and compliance with statutory
1633 requirements.

1634 (5) The Division of State Purchasing in the Department of
1635 Management Services shall coordinate with DIGIT on state term
1636 contract solicitations and invitations to negotiate related to
1637 information technology. Such coordination must include reviewing
1638 the solicitation specifications to verify compliance with
1639 enterprise architecture and cybersecurity standards, evaluating
1640 vendor responses under established criteria, answering vendor
1641 questions, and providing any other technical expertise
1642 necessary.

1643 (6) The Department of Legal Affairs, the Department of
1644 Financial Services, and the Department of Agriculture and
1645 Consumer Services may adopt alternatives to the information
1646 technology policy established by DIGIT pursuant to this section.
1647 If alternatives to the policy are adopted, such department must
1648 notify DIGIT, the Governor, the President of the Senate, and the
1649 Speaker of the House of Representatives in writing of the
1650 adoption of the alternatives and provide a justification for
1651 adoption of the alternatives, including whether the alternatives
1652 were necessary to meet alternatives adopted pursuant to s.
1653 282.00515, and explain the manner in which the department will

576-02812-26

2026480c2

1654 achieve the information technology policy.

1655 Section 16. Subsections (3), (4), (7), and (10) of section
1656 282.318, Florida Statutes, are amended to read:

1657 282.318 Cybersecurity.—

1658 (3) DIGIT ~~The department, acting through the Florida~~
1659 ~~Digital Service,~~ is the lead entity responsible for establishing
1660 standards and processes for assessing state agency cybersecurity
1661 risks and determining appropriate security measures that comply
1662 with the latest national and state data compliance security
1663 standards. Such standards and processes must be consistent with
1664 generally accepted technology best practices, including the
1665 National Institute for Standards and Technology Cybersecurity
1666 Framework, for cybersecurity. DIGIT ~~The department, acting~~
1667 ~~through the Florida Digital Service,~~ shall adopt rules that
1668 mitigate risks; safeguard state agency digital assets, data,
1669 information, and information technology resources to ensure
1670 availability, confidentiality, and integrity; and support a
1671 security governance framework. DIGIT ~~The department, acting~~
1672 ~~through the Florida Digital Service,~~ shall also:

1673 (a) Designate an employee ~~of the Florida Digital Service~~ as
1674 the state chief information security officer. The state chief
1675 information security officer must have experience and expertise
1676 in security and risk management for communications and
1677 information technology resources. The state chief information
1678 security officer is responsible for the development of
1679 enterprise cybersecurity policy, standards, operation, and
1680 security architecture oversight ~~of cybersecurity~~ for state
1681 technology systems. The state chief information security officer
1682 must ~~shall~~ be notified of all confirmed or suspected incidents

576-02812-26

2026480c2

1683 or threats of state agency information technology resources and
1684 must report such incidents or threats to the state chief
1685 information officer ~~and the Governor.~~

1686 (b) Develop, and annually update by February 1, a statewide
1687 cybersecurity strategic plan that includes security goals and
1688 objectives for cybersecurity, including the identification and
1689 mitigation of risk, proactive protections against threats,
1690 tactical risk detection, threat reporting, and response and
1691 recovery protocols for a cyber incident.

1692 (c) Develop and publish for use by state agencies a
1693 cybersecurity governance framework that, at a minimum, includes
1694 guidelines and processes for:

1695 1. Establishing asset management procedures to ensure that
1696 an agency's information technology resources are identified and
1697 managed consistent with their relative importance to the
1698 agency's business objectives.

1699 2. Using a standard risk assessment methodology that
1700 includes the identification of an agency's priorities,
1701 constraints, risk tolerances, and assumptions necessary to
1702 support operational risk decisions and that is aligned with
1703 generally accepted technology best practices, including the
1704 National Institute for Standards and Technology Cybersecurity
1705 Framework.

1706 3. Completing comprehensive risk assessments and
1707 cybersecurity audits, which may be completed by an independent
1708 third party ~~a private sector vendor~~, and submitting completed
1709 assessments and audits to DIGIT ~~the department.~~

1710 4. Identifying protection procedures to manage the
1711 protection of an agency's information, data, and information

576-02812-26

2026480c2

1712 technology resources.

1713 5. Establishing procedures for accessing information and
1714 data to ensure the confidentiality, integrity, and availability
1715 of such information and data.

1716 6. Detecting threats through proactive monitoring of
1717 events, continuous security monitoring, and defined detection
1718 processes.

1719 7. Establishing agency cybersecurity incident response
1720 teams and describing their responsibilities for responding to
1721 cybersecurity incidents, including breaches of personal
1722 information containing confidential or exempt data.

1723 8. Recovering information and data in response to a
1724 cybersecurity incident. The recovery may include recommended
1725 improvements to the agency processes, policies, or guidelines.

1726 9. Establishing a cybersecurity incident reporting process
1727 that includes procedures for notifying DIGIT ~~the department~~ and
1728 the Department of Law Enforcement of cybersecurity incidents.

1729 a. The level of severity of the cybersecurity incident is
1730 defined by the National Cyber Incident Response Plan of the
1731 United States Department of Homeland Security as follows:

1732 (I) Level 5 is an emergency-level incident within the
1733 specified jurisdiction that poses an imminent threat to the
1734 provision of wide-scale critical infrastructure services;
1735 national, state, or local government security; or the lives of
1736 the country's, state's, or local government's residents.

1737 (II) Level 4 is a severe-level incident that is likely to
1738 result in a significant impact in the affected jurisdiction to
1739 public health or safety; national, state, or local security;
1740 economic security; or civil liberties.

576-02812-26

2026480c2

1741 (III) Level 3 is a high-level incident that is likely to
1742 result in a demonstrable impact in the affected jurisdiction to
1743 public health or safety; national, state, or local security;
1744 economic security; civil liberties; or public confidence.

1745 (IV) Level 2 is a medium-level incident that may impact
1746 public health or safety; national, state, or local security;
1747 economic security; civil liberties; or public confidence.

1748 (V) Level 1 is a low-level incident that is unlikely to
1749 impact public health or safety; national, state, or local
1750 security; economic security; civil liberties; or public
1751 confidence.

1752 b. The cybersecurity incident reporting process must
1753 specify the information that must be reported by a state agency
1754 following a cybersecurity incident or ransomware incident,
1755 which, at a minimum, must include the following:

1756 (I) A summary of the facts surrounding the cybersecurity
1757 incident or ransomware incident.

1758 (II) The date on which the state agency most recently
1759 backed up its data; the physical location of the backup, if the
1760 backup was affected; and if the backup was created using cloud
1761 computing.

1762 (III) The types of data compromised by the cybersecurity
1763 incident or ransomware incident.

1764 (IV) The estimated fiscal impact of the cybersecurity
1765 incident or ransomware incident.

1766 (V) In the case of a ransomware incident, the details of
1767 the ransom demanded.

1768 c.(I) A state agency shall report all ransomware incidents
1769 and any cybersecurity incident determined by the state agency to

576-02812-26

2026480c2

1770 be of severity level 3, 4, or 5 to the state chief information
1771 security officer ~~Cybersecurity Operations Center~~ and the
1772 Cybercrime Office of the Department of Law Enforcement as soon
1773 as possible but no later than 48 hours after discovery of the
1774 cybersecurity incident and no later than 12 hours after
1775 discovery of the ransomware incident. The report must contain
1776 the information required in sub-subparagraph b. If the event
1777 involves services housed or procured through the Northwest
1778 Regional Data Center, the state agency must also notify the
1779 Northwest Regional Data Center.

1780 (II) The state chief information security officer
1781 ~~Cybersecurity Operations Center~~ shall notify the President of
1782 the Senate and the Speaker of the House of Representatives of
1783 any severity level 3, 4, or 5 incident as soon as possible but
1784 no later than 12 hours after receiving a state agency's incident
1785 report. The notification must include a high-level description
1786 of the incident and the likely effects.

1787 d. A state agency shall report a cybersecurity incident
1788 determined by the state agency to be of severity level 1 or 2 to
1789 the state chief information security officer ~~Cybersecurity~~
1790 ~~Operations Center~~ and the Cybercrime Office of the Department of
1791 Law Enforcement as soon as possible, but no later than 96 hours
1792 after the discovery of the cybersecurity incident and no later
1793 than 72 hours after the discovery of the ransomware incident.

1794 The report must contain the information required in sub-
1795 subparagraph b. If the event involves services housed or
1796 procured through the Northwest Regional Data Center, the state
1797 agency must also notify the Northwest Regional Data Center.

1798 e. The state chief information security officer

576-02812-26

2026480c2

1799 ~~Cybersecurity Operations Center~~ shall provide a consolidated
1800 incident report on a quarterly basis to the President of the
1801 Senate and, the Speaker of the House of Representatives, ~~and the~~
1802 ~~Florida Cybersecurity Advisory Council. The report provided to~~
1803 ~~the Florida Cybersecurity Advisory Council may not contain the~~
1804 ~~name of any agency, network information, or system identifying~~
1805 ~~information but must contain sufficient relevant information to~~
1806 ~~allow the Florida Cybersecurity Advisory Council to fulfill its~~
1807 ~~responsibilities as required in s. 282.319(9).~~

1808 10. Incorporating information obtained through detection
1809 and response activities into the agency's cybersecurity incident
1810 response plans.

1811 11. Developing agency strategic and operational
1812 cybersecurity plans required pursuant to this section.

1813 12. Establishing the managerial, operational, and technical
1814 safeguards for protecting state government data and information
1815 technology resources that align with the state agency risk
1816 management strategy and that protect the confidentiality,
1817 integrity, and availability of information and data.

1818 13. Establishing procedures for procuring information
1819 technology commodities and services that require the commodity
1820 or service to meet the National Institute of Standards and
1821 Technology Cybersecurity Framework.

1822 14. Submitting after-action reports following a
1823 cybersecurity incident or ransomware incident. ~~Such guidelines~~
1824 ~~and processes for submitting after-action reports must be~~
1825 ~~developed and published by December 1, 2022.~~

1826 (d) Assist state agencies in complying with this section.

1827 (e) In collaboration with the Cybercrime Office of the

576-02812-26

2026480c2

1828 Department of Law Enforcement, annually provide training for
1829 state agency information security managers and computer security
1830 incident response team members that contains training on
1831 cybersecurity, including cybersecurity threats, trends, and best
1832 practices.

1833 (f) Annually review the strategic and operational
1834 cybersecurity plans of state agencies.

1835 (g) Annually provide cybersecurity training to all state
1836 agency technology professionals and employees with access to
1837 highly sensitive information which develops, assesses, and
1838 documents competencies by role and skill level. The
1839 cybersecurity training curriculum must include training on the
1840 identification of each cybersecurity incident severity level
1841 referenced in sub-subparagraph (c)9.a. The training may be
1842 provided in collaboration with the Cybercrime Office of the
1843 Department of Law Enforcement, a private sector entity, or an
1844 institution of the State University System.

1845 ~~(h) Operate and maintain a Cybersecurity Operations Center~~
1846 ~~led by the state chief information security officer, which must~~
1847 ~~be primarily virtual and staffed with tactical detection and~~
1848 ~~incident response personnel. The Cybersecurity Operations Center~~
1849 ~~shall serve as a clearinghouse for threat information and~~
1850 ~~coordinate with the Department of Law Enforcement to support~~
1851 ~~state agencies and their response to any confirmed or suspected~~
1852 ~~cybersecurity incident.~~

1853 ~~(i) Lead an Emergency Support Function, ESF CYBER, under~~
1854 ~~the state comprehensive emergency management plan as described~~
1855 ~~in s. 252.35.~~

1856 (4) Each state agency head shall, at a minimum:

576-02812-26

2026480c2

1857 (a) Designate an information security manager to administer
1858 the cybersecurity program of the state agency. This designation
1859 must be provided annually in writing to DIGIT ~~the department~~ by
1860 January 1. A state agency's information security manager, for
1861 purposes of these information security duties, shall report
1862 directly to the agency head.

1863 (b) In consultation with the state chief information
1864 security officer ~~department, through the Florida Digital~~
1865 ~~Service,~~ and the Cybercrime Office of the Department of Law
1866 Enforcement, establish an agency cybersecurity response team to
1867 respond to a cybersecurity incident. The agency cybersecurity
1868 response team shall convene upon notification of a cybersecurity
1869 incident and shall ~~must~~ immediately report all confirmed or
1870 suspected incidents to the state chief information security
1871 officer, or his or her designee, and comply with all applicable
1872 guidelines and processes established pursuant to paragraph

1873 (3) (c).

1874 (c) Submit to the state chief information security officer
1875 ~~department~~ annually by July 31, the state agency's strategic and
1876 operational cybersecurity plans developed pursuant to rules and
1877 guidelines established by the state chief information security
1878 officer ~~department, through the Florida Digital Service.~~

1879 1. The state agency strategic cybersecurity plan must cover
1880 a 2-year ~~3-year~~ period and, at a minimum, define security goals,
1881 intermediate objectives, and projected agency costs for the
1882 strategic issues of agency information security policy, risk
1883 management, security training, security incident response, and
1884 disaster recovery. The plan must be based on the statewide
1885 cybersecurity strategic plan created by the state chief

576-02812-26

2026480c2

1886 information security officer department and include performance
1887 metrics that can be objectively measured to reflect the status
1888 of the state agency's progress in meeting security goals and
1889 objectives identified in the agency's strategic information
1890 security plan.

1891 2. The state agency operational cybersecurity plan must
1892 include a set of measures that objectively assess the
1893 performance of the agency's cybersecurity program in accordance
1894 with its risk management plan ~~progress report that objectively~~
1895 ~~measures progress made towards the prior operational~~
1896 ~~cybersecurity plan and a project plan that includes activities,~~
1897 ~~timelines, and deliverables for security objectives that the~~
1898 ~~state agency will implement during the current fiscal year.~~

1899 (d) Conduct, and update every 2 ~~3~~ years, a comprehensive
1900 risk assessment, which may be completed by an independent third
1901 party ~~a private sector vendor~~, to determine the security threats
1902 to the data, information, and information technology resources,
1903 including mobile devices and print environments, of the agency.
1904 The risk assessment must comply with the risk assessment
1905 methodology developed by the state chief information security
1906 officer department and is confidential and exempt from s.
1907 119.07(1), except that such information shall be available to
1908 the Auditor General, the state chief information security
1909 officer Florida Digital Service within the department, the
1910 Cybercrime Office of the Department of Law Enforcement, and, for
1911 state agencies under the jurisdiction of the Governor, the Chief
1912 Inspector General. If an independent third party ~~a private~~
1913 ~~sector vendor~~ is used to complete a comprehensive risk
1914 assessment, it must attest to the validity of the risk

576-02812-26

2026480c2

1915 assessment findings. The comprehensive risk assessment must
1916 include all of the following:

1917 1. The results of vulnerability and penetration tests on
1918 any Internet website or mobile application that processes any
1919 sensitive personal information or confidential information, and
1920 a plan to address any vulnerability identified in the tests.

1921 2. A written acknowledgment that the executive director or
1922 the secretary of the agency, the chief financial officer of the
1923 agency, and each executive manager as designated by the state
1924 agency, have been made aware of the risks revealed during the
1925 preparation of the agency's operations cybersecurity plan and
1926 the comprehensive risk assessment.

1927 (e) Develop, and periodically update, written internal
1928 policies and procedures, which include procedures for reporting
1929 cybersecurity incidents and breaches to the Cybercrime Office of
1930 the Department of Law Enforcement and the state chief
1931 information security officer ~~Florida Digital Service within the~~
1932 ~~department~~. Such policies and procedures must be consistent with
1933 the rules, guidelines, and processes established by DIGIT ~~the~~
1934 ~~department~~ to ensure the security of the data, information, and
1935 information technology resources of the agency. The internal
1936 policies and procedures that, if disclosed, could facilitate the
1937 unauthorized modification, disclosure, or destruction of data or
1938 information technology resources are confidential information
1939 and exempt from s. 119.07(1), except that such information must
1940 ~~shall~~ be available to the Auditor General, the Cybercrime Office
1941 of the Department of Law Enforcement, the state chief
1942 information security officer ~~the Florida Digital Service within~~
1943 ~~the department~~, and, for state agencies under the jurisdiction

576-02812-26

2026480c2

1944 of the Governor, the Chief Inspector General.

1945 (f) Implement managerial, operational, and technical
1946 safeguards and risk assessment remediation plans recommended by
1947 DIGIT ~~the department~~ to address identified risks to the data,
1948 information, and information technology resources of the agency.
1949 The state chief information security officer ~~department, through~~
1950 ~~the Florida Digital Service,~~ shall track implementation by state
1951 agencies upon development of such remediation plans in
1952 coordination with agency inspectors general.

1953 (g) Ensure that periodic internal audits and evaluations of
1954 the agency's cybersecurity program for the data, information,
1955 and information technology resources of the agency are
1956 conducted. The results of such audits and evaluations are
1957 confidential information and exempt from s. 119.07(1), except
1958 that such information must ~~shall~~ be available to the Auditor
1959 General, the Cybercrime Office of the Department of Law
1960 Enforcement, the state chief information security officer
1961 ~~Florida Digital Service within the department,~~ and, for agencies
1962 under the jurisdiction of the Governor, the Chief Inspector
1963 General.

1964 (h) Ensure that the cybersecurity requirements in the
1965 written specifications for the solicitation, contracts, and
1966 service-level agreement of information technology and
1967 information technology resources and services meet or exceed the
1968 applicable state and federal laws, regulations, and standards
1969 for cybersecurity, including the National Institute of Standards
1970 and Technology Cybersecurity Framework. Service-level agreements
1971 must identify service provider and state agency responsibilities
1972 for privacy and security, protection of government data,

576-02812-26

2026480c2

1973 personnel background screening, and security deliverables with
1974 associated frequencies.

1975 (i) Provide cybersecurity awareness training to all state
1976 agency employees within 30 days after commencing employment, and
1977 annually thereafter, concerning cybersecurity risks and the
1978 responsibility of employees to comply with policies, standards,
1979 guidelines, and operating procedures adopted by the state agency
1980 to reduce those risks. The training may be provided in
1981 collaboration with the Cybercrime Office of the Department of
1982 Law Enforcement, a private sector entity, or an institution of
1983 the State University System.

1984 (j) Develop a process for detecting, reporting, and
1985 responding to threats, breaches, or cybersecurity incidents
1986 which is consistent with the security rules, guidelines, and
1987 processes established by DIGIT ~~the department~~ through the state
1988 chief information security officer ~~Florida Digital Service~~.

1989 1. All cybersecurity incidents and ransomware incidents
1990 must be reported by state agencies. Such reports must comply
1991 with the notification procedures and reporting timeframes
1992 established pursuant to paragraph (3)(c).

1993 2. For cybersecurity breaches, state agencies shall provide
1994 notice in accordance with s. 501.171.

1995 (k) Submit to the state chief information security officer
1996 ~~Florida Digital Service~~, within 1 week after the remediation of
1997 a cybersecurity incident or ransomware incident, an after-action
1998 report that summarizes the incident, the incident's resolution,
1999 and any insights gained as a result of the incident.

2000 (7) The portions of records made confidential and exempt in
2001 subsections (5) and (6) must ~~shall~~ be available to the Auditor

576-02812-26

2026480c2

2002 General, the Cybercrime Office of the Department of Law
 2003 Enforcement, the state chief information security officer, the
 2004 Legislature ~~Florida Digital Service within the department~~, and,
 2005 for agencies under the jurisdiction of the Governor, the Chief
 2006 Inspector General. Such portions of records may be made
 2007 available to a local government, another state agency, or a
 2008 federal agency for cybersecurity purposes or in furtherance of
 2009 the state agency's official duties.

2010 (10) DIGIT ~~The department~~ shall adopt rules relating to
 2011 cybersecurity and to administer this section.

2012 Section 17. Subsections (3) through (6) of section
 2013 282.3185, Florida Statutes, are amended to read:

2014 282.3185 Local government cybersecurity.—

2015 (3) CYBERSECURITY TRAINING.—

2016 (a) The state chief information security officer ~~Florida~~
 2017 ~~Digital Service~~ shall:

2018 1. Develop a basic cybersecurity training curriculum for
 2019 local government employees. All local government employees with
 2020 access to the local government's network must complete the basic
 2021 cybersecurity training within 30 days after commencing
 2022 employment and annually thereafter.

2023 2. Develop an advanced cybersecurity training curriculum
 2024 for local governments which is consistent with the cybersecurity
 2025 training required under s. 282.318(3)(g). All local government
 2026 technology professionals and employees with access to highly
 2027 sensitive information must complete the advanced cybersecurity
 2028 training within 30 days after commencing employment and annually
 2029 thereafter.

2030 (b) The state chief information security officer ~~Florida~~

576-02812-26

2026480c2

2031 ~~Digital Service~~ may provide the cybersecurity training required
2032 by this subsection in collaboration with the Cybercrime Office
2033 of the Department of Law Enforcement, a private sector entity,
2034 or an institution of the State University System.

2035 (4) CYBERSECURITY STANDARDS.—

2036 (a) Each local government shall adopt cybersecurity
2037 standards that safeguard its data, information technology, and
2038 information technology resources to ensure availability,
2039 confidentiality, and integrity. The cybersecurity standards must
2040 be consistent with generally accepted best practices for
2041 cybersecurity, including the National Institute of Standards and
2042 Technology Cybersecurity Framework.

2043 (b) ~~Each county with a population of 75,000 or more must~~
2044 ~~adopt the cybersecurity standards required by this subsection by~~
2045 ~~January 1, 2024. Each county with a population of less than~~
2046 ~~75,000 must adopt the cybersecurity standards required by this~~
2047 ~~subsection by January 1, 2025.~~

2048 (c) ~~Each municipality with a population of 25,000 or more~~
2049 ~~must adopt the cybersecurity standards required by this~~
2050 ~~subsection by January 1, 2024. Each municipality with a~~
2051 ~~population of less than 25,000 must adopt the cybersecurity~~
2052 ~~standards required by this subsection by January 1, 2025.~~

2053 (d) Each local government shall notify the state chief
2054 information security officer ~~Florida Digital Service~~ of its
2055 compliance with this subsection as soon as possible.

2056 (5) INCIDENT NOTIFICATION.—

2057 (a) A local government shall provide notification of a
2058 cybersecurity incident or ransomware incident to the state chief
2059 information security officer ~~Cybersecurity Operations Center,~~

576-02812-26

2026480c2

2060 the Cybercrime Office of the Department of Law Enforcement, and
2061 the sheriff who has jurisdiction over the local government in
2062 accordance with paragraph (b). The notification must include, at
2063 a minimum, the following information:

2064 1. A summary of the facts surrounding the cybersecurity
2065 incident or ransomware incident.

2066 2. The date on which the local government most recently
2067 backed up its data; the physical location of the backup, if the
2068 backup was affected; and if the backup was created using cloud
2069 computing.

2070 3. The types of data compromised by the cybersecurity
2071 incident or ransomware incident.

2072 4. The estimated fiscal impact of the cybersecurity
2073 incident or ransomware incident.

2074 5. In the case of a ransomware incident, the details of the
2075 ransom demanded.

2076 6. A statement requesting or declining assistance from ~~the~~
2077 ~~Cybersecurity Operations Center~~, the Cybercrime Office of the
2078 Department of Law Enforcement, or the sheriff who has
2079 jurisdiction over the local government.

2080 (b)1. A local government shall report all ransomware
2081 incidents and any cybersecurity incident determined by the local
2082 government to be of severity level 3, 4, or 5 as provided in s.
2083 282.318(3)(c) to the state chief information security officer
2084 ~~Cybersecurity Operations Center~~, the Cybercrime Office of the
2085 Department of Law Enforcement, and the sheriff who has
2086 jurisdiction over the local government as soon as possible but
2087 no later than 12 ~~48~~ hours after discovery of the cybersecurity
2088 incident and no later than 6 ~~12~~ hours after discovery of the

576-02812-26

2026480c2

2089 ransomware incident. The report must contain the information
2090 required in paragraph (a).

2091 2. The state chief information security officer
2092 ~~Cybersecurity Operations Center~~ shall notify the President of
2093 the Senate and the Speaker of the House of Representatives of
2094 any severity level 3, 4, or 5 incident as soon as possible but
2095 no later than 12 hours after receiving a local government's
2096 incident report. The notification must include a high-level
2097 description of the incident and the likely effects.

2098 (c) A local government may report a cybersecurity incident
2099 determined by the local government to be of severity level 1 or
2100 2 as provided in s. 282.318(3)(c) to the state chief information
2101 security officer ~~Cybersecurity Operations Center~~, the Cybercrime
2102 Office of the Department of Law Enforcement, and the sheriff who
2103 has jurisdiction over the local government. The report must
2104 ~~shall~~ contain the information required in paragraph (a).

2105 (d) The state chief information security officer
2106 ~~Cybersecurity Operations Center~~ shall provide a consolidated
2107 incident report by the 30th day after the end of each quarter ~~on~~
2108 ~~a quarterly basis~~ to the President of the Senate and~~7~~ the
2109 Speaker of the House of Representatives, ~~and the Florida~~
2110 ~~Cybersecurity Advisory Council~~. ~~The report provided to the~~
2111 ~~Florida Cybersecurity Advisory Council may not contain the name~~
2112 ~~of any local government, network information, or system~~
2113 ~~identifying information but must contain sufficient relevant~~
2114 ~~information to allow the Florida Cybersecurity Advisory Council~~
2115 ~~to fulfill its responsibilities as required in s. 282.319(9).~~

2116 (6) AFTER-ACTION REPORT.—A local government shall ~~must~~
2117 submit to the state chief information security officer ~~Florida~~

576-02812-26

2026480c2

2118 ~~Digital Service~~, within 1 week after the remediation of a
2119 cybersecurity incident or ransomware incident, an after-action
2120 report that summarizes the incident, the incident's resolution,
2121 and any insights gained as a result of the incident. ~~By December~~
2122 ~~1, 2022, the Florida Digital Service shall establish guidelines~~
2123 ~~and processes for submitting an after-action report.~~

2124 Section 18. Section 282.319, Florida Statutes, is repealed.

2125 Section 19. Section 282.201, Florida Statutes, is amended
2126 to read:

2127 282.201 State data center.—The state data center is
2128 established within the Northwest Regional Data Center pursuant
2129 to s. 282.2011 and shall meet or exceed the information
2130 technology standards specified in ss. 282.006 and 282.318 ~~the~~
2131 ~~department. The provision of data center services must comply~~
2132 ~~with applicable state and federal laws, regulations, and~~
2133 ~~policies, including all applicable security, privacy, and~~
2134 ~~auditing requirements. The department shall appoint a director~~
2135 ~~of the state data center who has experience in leading data~~
2136 ~~center facilities and has expertise in cloud-computing~~
2137 ~~management.~~

2138 ~~(1) STATE DATA CENTER DUTIES. The state data center shall:~~

2139 ~~(a) Offer, develop, and support the services and~~
2140 ~~applications defined in service-level agreements executed with~~
2141 ~~its customer entities.~~

2142 ~~(b) Maintain performance of the state data center by~~
2143 ~~ensuring proper data backup; data backup recovery; disaster~~
2144 ~~recovery; and appropriate security, power, cooling, fire~~
2145 ~~suppression, and capacity.~~

2146 ~~(c) Develop and implement business continuity and disaster~~

576-02812-26

2026480c2

2147 ~~recovery plans, and annually conduct a live exercise of each~~
2148 ~~plan.~~

2149 ~~(d) Enter into a service-level agreement with each customer~~
2150 ~~entity to provide the required type and level of service or~~
2151 ~~services. If a customer entity fails to execute an agreement~~
2152 ~~within 60 days after commencement of a service, the state data~~
2153 ~~center may cease service. A service-level agreement may not have~~
2154 ~~a term exceeding 3 years and at a minimum must:~~

2155 ~~1. Identify the parties and their roles, duties, and~~
2156 ~~responsibilities under the agreement.~~

2157 ~~2. State the duration of the contract term and specify the~~
2158 ~~conditions for renewal.~~

2159 ~~3. Identify the scope of work.~~

2160 ~~4. Identify the products or services to be delivered with~~
2161 ~~sufficient specificity to permit an external financial or~~
2162 ~~performance audit.~~

2163 ~~5. Establish the services to be provided, the business~~
2164 ~~standards that must be met for each service, the cost of each~~
2165 ~~service by agency application, and the metrics and processes by~~
2166 ~~which the business standards for each service are to be~~
2167 ~~objectively measured and reported.~~

2168 ~~6. Provide a timely billing methodology to recover the~~
2169 ~~costs of services provided to the customer entity pursuant to s.~~
2170 ~~215.422.~~

2171 ~~7. Provide a procedure for modifying the service-level~~
2172 ~~agreement based on changes in the type, level, and cost of a~~
2173 ~~service.~~

2174 ~~8. Include a right-to-audit clause to ensure that the~~
2175 ~~parties to the agreement have access to records for audit~~

576-02812-26

2026480c2

2176 ~~purposes during the term of the service level agreement.~~

2177 ~~9. Provide that a service level agreement may be terminated~~
2178 ~~by either party for cause only after giving the other party and~~
2179 ~~the department notice in writing of the cause for termination~~
2180 ~~and an opportunity for the other party to resolve the identified~~
2181 ~~cause within a reasonable period.~~

2182 ~~10. Provide for mediation of disputes by the Division of~~
2183 ~~Administrative Hearings pursuant to s. 120.573.~~

2184 ~~(e) For purposes of chapter 273, be the custodian of~~
2185 ~~resources and equipment located in and operated, supported, and~~
2186 ~~managed by the state data center.~~

2187 ~~(f) Assume administrative access rights to resources and~~
2188 ~~equipment, including servers, network components, and other~~
2189 ~~devices, consolidated into the state data center.~~

2190 ~~1. Upon consolidation, a state agency shall relinquish~~
2191 ~~administrative rights to consolidated resources and equipment.~~
2192 ~~State agencies required to comply with federal and state~~
2193 ~~criminal justice information security rules and policies shall~~
2194 ~~retain administrative access rights sufficient to comply with~~
2195 ~~the management control provisions of those rules and policies;~~
2196 ~~however, the state data center shall have the appropriate type~~
2197 ~~or level of rights to allow the center to comply with its duties~~
2198 ~~pursuant to this section. The Department of Law Enforcement~~
2199 ~~shall serve as the arbiter of disputes pertaining to the~~
2200 ~~appropriate type and level of administrative access rights~~
2201 ~~pertaining to the provision of management control in accordance~~
2202 ~~with the federal criminal justice information guidelines.~~

2203 ~~2. The state data center shall provide customer entities~~
2204 ~~with access to applications, servers, network components, and~~

576-02812-26

2026480c2

2205 ~~other devices necessary for entities to perform business~~
2206 ~~activities and functions, and as defined and documented in a~~
2207 ~~service-level agreement.~~

2208 ~~(g) In its procurement process, show preference for cloud-~~
2209 ~~computing solutions that minimize or do not require the~~
2210 ~~purchasing, financing, or leasing of state data center~~
2211 ~~infrastructure, and that meet the needs of customer agencies,~~
2212 ~~that reduce costs, and that meet or exceed the applicable state~~
2213 ~~and federal laws, regulations, and standards for cybersecurity.~~

2214 ~~(h) Assist customer entities in transitioning from state~~
2215 ~~data center services to the Northwest Regional Data Center or~~
2216 ~~other third party cloud computing services procured by a~~
2217 ~~customer entity or by the Northwest Regional Data Center on~~
2218 ~~behalf of a customer entity.~~

2219 (1)(2) USE OF THE STATE DATA CENTER.—

2220 ~~(a)~~ The following are exempt from the use of the state data
2221 center: the Department of Law Enforcement, the Department of the
2222 Lottery's Gaming System, Systems Design and Development in the
2223 Office of Policy and Budget, the regional traffic management
2224 centers as described in s. 335.14(2) and the Office of Toll
2225 Operations of the Department of Transportation, the State Board
2226 of Administration, state attorneys, public defenders, criminal
2227 conflict and civil regional counsel, capital collateral regional
2228 counsel, ~~and~~ the Florida Housing Finance Corporation, and the
2229 Division of Emergency Management within the Executive Office of
2230 the Governor.

2231 ~~(b) The Division of Emergency Management is exempt from the~~
2232 ~~use of the state data center. This paragraph expires July 1,~~
2233 ~~2026.~~

576-02812-26

2026480c2

2234 (2)~~(3)~~ AGENCY LIMITATIONS.—Unless exempt from the use of
2235 the state data center pursuant to this section or authorized by
2236 the Legislature, a state agency may not:

2237 (a) Create a new agency computing facility or data center,
2238 or expand the capability to support additional computer
2239 equipment in an existing agency computing facility or data
2240 center; or

2241 (b) Terminate services with the state data center without
2242 giving written notice of intent to terminate services 180 days
2243 before such termination.

2244 ~~(4) DEPARTMENT RESPONSIBILITIES. The department shall
2245 provide operational management and oversight of the state data
2246 center, which includes:~~

2247 ~~(a) Implementing industry standards and best practices for
2248 the state data center's facilities, operations, maintenance,
2249 planning, and management processes.~~

2250 ~~(b) Developing and implementing cost recovery mechanisms
2251 that recover the full direct and indirect cost of services
2252 through charges to applicable customer entities. Such cost-
2253 recovery mechanisms must comply with applicable state and
2254 federal regulations concerning distribution and use of funds and
2255 must ensure that, for any fiscal year, no service or customer
2256 entity subsidizes another service or customer entity. The
2257 department may recommend other payment mechanisms to the
2258 Executive Office of the Governor, the President of the Senate,
2259 and the Speaker of the House of Representatives. Such mechanisms
2260 may be implemented only if specifically authorized by the
2261 Legislature.~~

2262 ~~(c) Developing and implementing appropriate operating~~

576-02812-26

2026480c2

2263 ~~guidelines and procedures necessary for the state data center to~~
2264 ~~perform its duties pursuant to subsection (1). The guidelines~~
2265 ~~and procedures must comply with applicable state and federal~~
2266 ~~laws, regulations, and policies and conform to generally~~
2267 ~~accepted governmental accounting and auditing standards. The~~
2268 ~~guidelines and procedures must include, but need not be limited~~
2269 ~~to:~~

2270 ~~1. Implementing a consolidated administrative support~~
2271 ~~structure responsible for providing financial management,~~
2272 ~~procurement, transactions involving real or personal property,~~
2273 ~~human resources, and operational support.~~

2274 ~~2. Implementing an annual reconciliation process to ensure~~
2275 ~~that each customer entity is paying for the full direct and~~
2276 ~~indirect cost of each service as determined by the customer~~
2277 ~~entity's use of each service.~~

2278 ~~3. Providing rebates that may be credited against future~~
2279 ~~billings to customer entities when revenues exceed costs.~~

2280 ~~4. Requiring customer entities to validate that sufficient~~
2281 ~~funds exist before implementation of a customer entity's request~~
2282 ~~for a change in the type or level of service provided, if such~~
2283 ~~change results in a net increase to the customer entity's cost~~
2284 ~~for that fiscal year.~~

2285 ~~5. By November 15 of each year, providing to the Office of~~
2286 ~~Policy and Budget in the Executive Office of the Governor and to~~
2287 ~~the chairs of the legislative appropriations committees the~~
2288 ~~projected costs of providing data center services for the~~
2289 ~~following fiscal year.~~

2290 ~~6. Providing a plan for consideration by the Legislative~~
2291 ~~Budget Commission if the cost of a service is increased for a~~

576-02812-26

2026480c2

2292 ~~reason other than a customer entity's request made pursuant to~~
2293 ~~subparagraph 4. Such a plan is required only if the service cost~~
2294 ~~increase results in a net increase to a customer entity for that~~
2295 ~~fiscal year.~~

2296 ~~7. Standardizing and consolidating procurement and~~
2297 ~~contracting practices.~~

2298 ~~(d) In collaboration with the Department of Law Enforcement~~
2299 ~~and the Florida Digital Service, developing and implementing a~~
2300 ~~process for detecting, reporting, and responding to~~
2301 ~~cybersecurity incidents, breaches, and threats.~~

2302 ~~(e) Adopting rules relating to the operation of the state~~
2303 ~~data center, including, but not limited to, budgeting and~~
2304 ~~accounting procedures, cost-recovery methodologies, and~~
2305 ~~operating procedures.~~

2306 ~~(5) NORTHWEST REGIONAL DATA CENTER CONTRACT. In order for~~
2307 ~~the department to carry out its duties and responsibilities~~
2308 ~~relating to the state data center, the secretary of the~~
2309 ~~department shall contract by July 1, 2022, with the Northwest~~
2310 ~~Regional Data Center pursuant to s. 287.057(11). The contract~~
2311 ~~shall provide that the Northwest Regional Data Center will~~
2312 ~~manage the operations of the state data center and provide data~~
2313 ~~center services to state agencies.~~

2314 ~~(a) The department shall provide contract oversight,~~
2315 ~~including, but not limited to, reviewing invoices provided by~~
2316 ~~the Northwest Regional Data Center for services provided to~~
2317 ~~state agency customers.~~

2318 ~~(b) The department shall approve or request updates to~~
2319 ~~invoices within 10 business days after receipt. If the~~
2320 ~~department does not respond to the Northwest Regional Data~~

576-02812-26

2026480c2

2321 ~~Center, the invoice will be approved by default. The Northwest~~
2322 ~~Regional Data Center must submit approved invoices directly to~~
2323 ~~state agency customers.~~

2324 Section 20. Section 282.2011, Florida Statutes, is created
2325 to read:

2326 282.2011 Northwest Regional Data Center.—

2327 (1) For the purpose of providing data center services to
2328 its state agency customers, the Northwest Regional Data Center
2329 is designated as the state data center for all state agencies,
2330 except as otherwise provided by law, and shall:

2331 (a) Operate under a governance structure that represents
2332 its customers proportionally.

2333 (b) Maintain an appropriate cost-allocation methodology
2334 that accurately bills state agency customers based solely on the
2335 actual direct and indirect costs of the services provided to
2336 state agency customers and ensures that, for any fiscal year,
2337 state agency customers are not subsidizing other customers of
2338 the data center. Such cost-allocation methodology must comply
2339 with applicable state and federal regulations concerning the
2340 distribution and use of state and federal funds.

2341 (c) Enter into a service-level agreement with each state
2342 agency customer to provide services as defined and approved by
2343 the governing board of the center. At a minimum, such service-
2344 level agreements must:

2345 1. Identify the parties and their roles, duties, and
2346 responsibilities under the agreement;

2347 2. State the duration of the agreement term, which may not
2348 exceed 3 years, and specify the conditions for up to two
2349 optional 1-year renewals of the agreement before execution of a

576-02812-26

2026480c2

2350 new agreement;

2351 3. Identify the scope of work;

2352 4. Establish the services to be provided, the business
2353 standards that must be met for each service, the cost of each
2354 service, and the process by which the business standards for
2355 each service are to be objectively measured and reported;

2356 5. Provide a timely billing methodology for recovering the
2357 cost of services provided pursuant to s. 215.422;

2358 6. Provide a procedure for modifying the service-level
2359 agreement to address any changes in projected costs of service;

2360 7. Include a right-to-audit clause to ensure that the
2361 parties to the agreement have access to records for audit
2362 purposes during the term of the service-level agreement;

2363 8. Identify the products or services to be delivered with
2364 sufficient specificity to permit an external financial or
2365 performance audit;

2366 9. Provide that the service-level agreement may be
2367 terminated by either party for cause only after giving the other
2368 party notice in writing of the cause for termination and an
2369 opportunity for the other party to resolve the identified cause
2370 within a reasonable period; and

2371 10. Provide state agency customer entities with access to
2372 applications, servers, network components, and other devices
2373 necessary for entities to perform business activities and
2374 functions and as defined and documented in a service-level
2375 agreement.

2376 (d) For purposes of chapter 273, be the custodian of
2377 resources and equipment located in and operated, supported, and
2378 managed by the state data center.

576-02812-26

2026480c2

2379 (e) Assume administrative access rights to resources and
2380 equipment, including servers, network components, and other
2381 devices, consolidated into the state data center.

2382 1. Upon consolidation, a state agency shall relinquish
2383 administrative rights to consolidated resources and equipment.
2384 State agencies required to comply with federal and state
2385 criminal justice information security rules and policies shall
2386 retain administrative access rights sufficient to comply with
2387 the management control provisions of those rules and policies;
2388 however, the state data center shall have the appropriate type
2389 or level of rights to allow the center to comply with its duties
2390 pursuant to this section. The Department of Law Enforcement
2391 shall serve as the arbiter of disputes pertaining to the
2392 appropriate type and level of administrative access rights
2393 pertaining to the provision of management control in accordance
2394 with the federal criminal justice information guidelines.

2395 2. The state data center shall provide customer entities
2396 with access to applications, servers, network components, and
2397 other devices necessary for entities to perform business
2398 activities and functions, and as defined and documented in a
2399 service-level agreement.

2400 (f) In its procurement process, show preference for cloud-
2401 computing solutions that minimize or do not require the
2402 purchasing or financing of state data center infrastructure,
2403 that meet the needs of state agency customer entities, that
2404 reduce costs, and that meet or exceed the applicable state and
2405 federal laws, regulations, and standards for cybersecurity.

2406 (g) Assist state agency customer entities in transitioning
2407 from state data center services to other third-party cloud-

576-02812-26

2026480c2

2408 computing services procured by a customer entity or by the
2409 Northwest Regional Data Center on behalf of the customer entity.

2410 (h) Provide to the Board of Governors the total annual
2411 budget by major expenditure category, including, but not limited
2412 to, salaries, expenses, operating capital outlay, contracted
2413 services, or other personnel services, by July 30 each fiscal
2414 year.

2415 (i) Provide to each state agency customer its projected
2416 annual cost for providing the agreed-upon data center services
2417 by September 1 each fiscal year.

2418 (j) By November 15 of each year, provide to the Office of
2419 Policy and Budget in the Executive Office of the Governor and to
2420 the chairs of the legislative appropriations committees the
2421 projected costs of providing data center services for the
2422 following fiscal year for each state agency customer. The
2423 projections must include prior-year comparisons, identification
2424 of new services, and documentation of changes to billing
2425 methodologies or service cost allocation.

2426 (k) Provide a plan for consideration by the Legislative
2427 Budget Commission if the governing body of the center approves
2428 the use of a billing rate schedule after the start of the fiscal
2429 year which increases any state agency customer's costs for that
2430 fiscal year.

2431 (l) Provide data center services that comply with
2432 applicable state and federal laws, regulations, and policies,
2433 including all applicable security, privacy, and auditing
2434 requirements.

2435 (m) Maintain performance of the data center facilities by
2436 ensuring proper data backup; data backup recovery; disaster

576-02812-26

2026480c2

2437 recovery; and appropriate security, power, cooling, fire
2438 suppression, and capacity.

2439 (n) Submit invoices to state agency customers.

2440 (o) As funded in the General Appropriations Act, provide
2441 data center services to state agencies from multiple facilities.

2442 (2) Unless exempt from the requirement to use the state
2443 data center pursuant to s. 282.201(1) or as authorized by the
2444 Legislature, a state agency may not do any of the following:

2445 (a) Terminate services with the Northwest Regional Data
2446 Center without giving written notice of intent to terminate
2447 services 180 days before such termination.

2448 (b) Procure third-party cloud-computing services without
2449 evaluating the cloud-computing services provided by the
2450 Northwest Regional Data Center.

2451 (c) Exceed 30 days from receipt of approved invoices to
2452 remit payment for state data center services provided by the
2453 Northwest Regional Data Center.

2454 (3) The Northwest Regional Data Center's authority to
2455 provide data center services to its state agency customers may
2456 be terminated if:

2457 (a) The center requests such termination to the Board of
2458 Governors, the President of the Senate, and the Speaker of the
2459 House of Representatives; or

2460 (b) The center fails to comply with the provisions of this
2461 section.

2462 (4) The Northwest Regional Data Center is the lead entity
2463 responsible for creating, operating, and managing, including the
2464 research conducted by, the Florida Behavioral Health Care Data
2465 Repository as established by this subsection.

576-02812-26

2026480c2

2466 (a) The purpose of the data repository is to create a
2467 centralized system for:

2468 1. Collecting and analyzing existing statewide behavioral
2469 health care data to:

2470 a. Better understand the scope of and trends in behavioral
2471 health services, spending, and outcomes to improve patient care
2472 and enhance the efficiency and effectiveness of behavioral
2473 health services;

2474 b. Better understand the scope of, trends in, and
2475 relationship between behavioral health, criminal justice,
2476 incarceration, and the use of behavioral health services as a
2477 diversion from incarceration for individuals with mental
2478 illness; and

2479 c. Enhance the collection and coordination of treatment and
2480 outcome information as an ongoing evidence base for research and
2481 education related to behavioral health.

2482 2. Developing useful data analytics, economic metrics, and
2483 visual representations of such analytics and metrics to inform
2484 relevant state agencies and the Legislature of data and trends
2485 in behavioral health.

2486 (b) The Northwest Regional Data Center shall develop, in
2487 collaboration with the Data Analysis Committee of the Commission
2488 on Mental Health and Substance Use Disorder created under s.
2489 394.9086 and with relevant stakeholders, a plan that includes
2490 all of the following:

2491 1. A project plan that describes the technology,
2492 methodology, timeline, cost, and resources necessary to create a
2493 centralized, integrated, and coordinated data system.

2494 2. A proposed governance structure to oversee the

576-02812-26

2026480c2

2495 implementation and operations of the repository.

2496 3. An integration strategy to incorporate existing data
2497 from relevant state agencies, including, but not limited to, the
2498 Agency for Health Care Administration, the Department of
2499 Children and Families, the Department of Juvenile Justice, the
2500 Office of the State Courts Administrator, and the Department of
2501 Corrections.

2502 4. Identification of relevant data and metrics to support
2503 actionable information and ensure the efficient and responsible
2504 use of taxpayer dollars within behavioral health systems of
2505 care.

2506 5. Data security requirements for the repository.

2507 6. The structure and process that will be used to create an
2508 annual analysis and report that gives state agencies and the
2509 Legislature a better general understanding of trends and issues
2510 in the state's behavioral health systems of care and the trends
2511 and issues in behavioral health systems related to criminal
2512 justice treatment, diversion, and incarceration.

2513 (c) Beginning December 1, 2026, and annually thereafter,
2514 the Northwest Regional Data Center shall submit the developed
2515 trends and issues report under subparagraph (b)6. to the
2516 Governor, the President of the Senate, and the Speaker of the
2517 House of Representatives.

2518 (5) If such authority is terminated, the center has 1 year
2519 to provide for the transition of its state agency customers to a
2520 qualified alternative cloud-based data center that meets the
2521 enterprise architecture standards established pursuant to this
2522 chapter.

2523 Section 21. Subsection (4) of section 282.206, Florida

576-02812-26

2026480c2

2524 Statutes, is amended to read:

2525 282.206 Cloud-first policy in state agencies.—

2526 (4) Each state agency shall develop a strategic plan to be
2527 updated annually to address its inventory of applications
2528 located at the state data center. Each agency shall submit the
2529 plan by October 15 of each year to DIGIT, the Office of Policy
2530 and Budget in the Executive Office of the Governor, ~~and~~ the
2531 chairs of the legislative appropriations committees, and the
2532 Northwest Regional Data Center. For each application, the plan
2533 must identify and document the feasibility, appropriateness,
2534 readiness, appropriate strategy, and high-level timeline for
2535 transition to a cloud-computing service based on the
2536 application's quality, cost, and resource requirements. This
2537 information must be used to assist the state data center in
2538 making adjustments to its service offerings.

2539 Section 22. Section 1004.649, Florida Statutes, is amended
2540 to read:

2541 1004.649 Northwest Regional Data Center.—There is created
2542 at Florida State University the Northwest Regional Data Center.
2543 The data center shall serve as the state data center as
2544 designated in s. 282.201

2545 ~~(1) For the purpose of providing data center services to~~
2546 ~~its state agency customers, the Northwest Regional Data Center~~
2547 ~~is designated as a state data center for all state agencies and~~
2548 ~~shall:~~

2549 ~~(a) Operate under a governance structure that represents~~
2550 ~~its customers proportionally.~~

2551 ~~(b) Maintain an appropriate cost-allocation methodology~~
2552 ~~that accurately bills state agency customers based solely on the~~

576-02812-26

2026480c2

2553 ~~actual direct and indirect costs of the services provided to~~
2554 ~~state agency customers and ensures that, for any fiscal year,~~
2555 ~~state agency customers are not subsidizing other customers of~~
2556 ~~the data center. Such cost-allocation methodology must comply~~
2557 ~~with applicable state and federal regulations concerning the~~
2558 ~~distribution and use of state and federal funds.~~

2559 ~~(c) Enter into a service-level agreement with each state~~
2560 ~~agency customer to provide services as defined and approved by~~
2561 ~~the governing board of the center. At a minimum, such service-~~
2562 ~~level agreements must:~~

- 2563 ~~1. Identify the parties and their roles, duties, and~~
2564 ~~responsibilities under the agreement;~~
- 2565 ~~2. State the duration of the agreement term, which may not~~
2566 ~~exceed 3 years, and specify the conditions for up to two~~
2567 ~~optional 1-year renewals of the agreement before execution of a~~
2568 ~~new agreement;~~
- 2569 ~~3. Identify the scope of work;~~
- 2570 ~~4. Establish the services to be provided, the business~~
2571 ~~standards that must be met for each service, the cost of each~~
2572 ~~service, and the process by which the business standards for~~
2573 ~~each service are to be objectively measured and reported;~~
- 2574 ~~5. Provide a timely billing methodology for recovering the~~
2575 ~~cost of services provided pursuant to s. 215.422;~~
- 2576 ~~6. Provide a procedure for modifying the service-level~~
2577 ~~agreement to address any changes in projected costs of service;~~
- 2578 ~~7. Include a right-to-audit clause to ensure that the~~
2579 ~~parties to the agreement have access to records for audit~~
2580 ~~purposes during the term of the service-level agreement;~~
- 2581 ~~8. Identify the products or services to be delivered with~~

576-02812-26

2026480c2

2582 ~~sufficient specificity to permit an external financial or~~
2583 ~~performance audit;~~

2584 ~~9. Provide that the service-level agreement may be~~
2585 ~~terminated by either party for cause only after giving the other~~
2586 ~~party notice in writing of the cause for termination and an~~
2587 ~~opportunity for the other party to resolve the identified cause~~
2588 ~~within a reasonable period; and~~

2589 ~~10. Provide state agency customer entities with access to~~
2590 ~~applications, servers, network components, and other devices~~
2591 ~~necessary for entities to perform business activities and~~
2592 ~~functions and as defined and documented in a service-level~~
2593 ~~agreement.~~

2594 ~~(d) In its procurement process, show preference for cloud-~~
2595 ~~computing solutions that minimize or do not require the~~
2596 ~~purchasing or financing of state data center infrastructure,~~
2597 ~~that meet the needs of state agency customer entities, that~~
2598 ~~reduce costs, and that meet or exceed the applicable state and~~
2599 ~~federal laws, regulations, and standards for cybersecurity.~~

2600 ~~(e) Assist state agency customer entities in transitioning~~
2601 ~~from state data center services to other third-party cloud-~~
2602 ~~computing services procured by a customer entity or by the~~
2603 ~~Northwest Regional Data Center on behalf of the customer entity.~~

2604 ~~(f) Provide to the Board of Governors the total annual~~
2605 ~~budget by major expenditure category, including, but not limited~~
2606 ~~to, salaries, expenses, operating capital outlay, contracted~~
2607 ~~services, or other personnel services by July 30 each fiscal~~
2608 ~~year.~~

2609 ~~(g) Provide to each state agency customer its projected~~
2610 ~~annual cost for providing the agreed-upon data center services~~

576-02812-26

2026480c2

2611 ~~by September 1 each fiscal year.~~

2612 ~~(h) Provide a plan for consideration by the Legislative~~
2613 ~~Budget Commission if the governing body of the center approves~~
2614 ~~the use of a billing rate schedule after the start of the fiscal~~
2615 ~~year that increases any state agency customer's costs for that~~
2616 ~~fiscal year.~~

2617 ~~(i) Provide data center services that comply with~~
2618 ~~applicable state and federal laws, regulations, and policies,~~
2619 ~~including all applicable security, privacy, and auditing~~
2620 ~~requirements.~~

2621 ~~(j) Maintain performance of the data center facilities by~~
2622 ~~ensuring proper data backup; data backup recovery; disaster~~
2623 ~~recovery; and appropriate security, power, cooling, fire~~
2624 ~~suppression, and capacity.~~

2625 ~~(k) Prepare and submit state agency customer invoices to~~
2626 ~~the Department of Management Services for approval. Upon~~
2627 ~~approval or by default pursuant to s. 282.201(5), submit~~
2628 ~~invoices to state agency customers.~~

2629 ~~(l) As funded in the General Appropriations Act, provide~~
2630 ~~data center services to state agencies from multiple facilities.~~

2631 ~~(2) Unless exempt from the requirement to use the state~~
2632 ~~data center pursuant to s. 282.201(2) or as authorized by the~~
2633 ~~Legislature, a state agency may not do any of the following:~~

2634 ~~(a) Terminate services with the Northwest Regional Data~~
2635 ~~Center without giving written notice of intent to terminate~~
2636 ~~services 180 days before such termination.~~

2637 ~~(b) Procure third party cloud computing services without~~
2638 ~~evaluating the cloud computing services provided by the~~
2639 ~~Northwest Regional Data Center.~~

576-02812-26

2026480c2

2640 ~~(c) Exceed 30 days from receipt of approved invoices to~~
2641 ~~remit payment for state data center services provided by the~~
2642 ~~Northwest Regional Data Center.~~

2643 ~~(3) The Northwest Regional Data Center's authority to~~
2644 ~~provide data center services to its state agency customers may~~
2645 ~~be terminated if:~~

2646 ~~(a) The center requests such termination to the Board of~~
2647 ~~Governors, the President of the Senate, and the Speaker of the~~
2648 ~~House of Representatives; or~~

2649 ~~(b) The center fails to comply with the provisions of this~~
2650 ~~section.~~

2651 ~~(4) The Northwest Regional Data Center is the lead entity~~
2652 ~~responsible for creating, operating, and managing, including the~~
2653 ~~research conducted by, the Florida Behavioral Health Care Data~~
2654 ~~Repository as established by this subsection.~~

2655 ~~(a) The purpose of the data repository is to create a~~
2656 ~~centralized system for:~~

2657 ~~1. Collecting and analyzing existing statewide behavioral~~
2658 ~~health care data to:~~

2659 ~~a. Better understand the scope of and trends in behavioral~~
2660 ~~health services, spending, and outcomes to improve patient care~~
2661 ~~and enhance the efficiency and effectiveness of behavioral~~
2662 ~~health services;~~

2663 ~~b. Better understand the scope of, trends in, and~~
2664 ~~relationship between behavioral health, criminal justice,~~
2665 ~~incarceration, and the use of behavioral health services as a~~
2666 ~~diversion from incarceration for individuals with mental~~
2667 ~~illness; and~~

2668 ~~e. Enhance the collection and coordination of treatment and~~

576-02812-26

2026480c2

2669 ~~outcome information as an ongoing evidence base for research and~~
2670 ~~education related to behavioral health.~~

2671 ~~2. Developing useful data analytics, economic metrics, and~~
2672 ~~visual representations of such analytics and metrics to inform~~
2673 ~~relevant state agencies and the Legislature of data and trends~~
2674 ~~in behavioral health.~~

2675 ~~(b) The Northwest Regional Data Center shall develop, in~~
2676 ~~collaboration with the Data Analysis Committee of the Commission~~
2677 ~~on Mental Health and Substance Use Disorder created under s.~~
2678 ~~394.9086 and with relevant stakeholders, a plan that includes~~
2679 ~~all of the following:~~

2680 ~~1. A project plan that describes the technology,~~
2681 ~~methodology, timeline, cost, and resources necessary to create a~~
2682 ~~centralized, integrated, and coordinated data system.~~

2683 ~~2. A proposed governance structure to oversee the~~
2684 ~~implementation and operations of the repository.~~

2685 ~~3. An integration strategy to incorporate existing data~~
2686 ~~from relevant state agencies, including, but not limited to, the~~
2687 ~~Agency for Health Care Administration, the Department of~~
2688 ~~Children and Families, the Department of Juvenile Justice, the~~
2689 ~~Office of the State Courts Administrator, and the Department of~~
2690 ~~Corrections.~~

2691 ~~4. Identification of relevant data and metrics to support~~
2692 ~~actionable information and ensure the efficient and responsible~~
2693 ~~use of taxpayer dollars within behavioral health systems of~~
2694 ~~care.~~

2695 ~~5. Data security requirements for the repository.~~

2696 ~~6. The structure and process that will be used to create an~~
2697 ~~annual analysis and report that gives state agencies and the~~

576-02812-26

2026480c2

2698 ~~Legislature a better general understanding of trends and issues~~
2699 ~~in the state's behavioral health systems of care and the trends~~
2700 ~~and issues in behavioral health systems related to criminal~~
2701 ~~justice treatment, diversion, and incarceration.~~

2702 ~~(c) By December 1, 2025, the Northwest Regional Data~~
2703 ~~Center, in collaboration with the Data Analysis Committee of the~~
2704 ~~Commission on Mental Health and Substance Use Disorder, shall~~
2705 ~~submit the developed plan for implementation and ongoing~~
2706 ~~operation with a proposed budget to the Governor, the President~~
2707 ~~of the Senate, and the Speaker of the House of Representatives~~
2708 ~~for review.~~

2709 ~~(d) Beginning December 1, 2026, and annually thereafter,~~
2710 ~~the Northwest Regional Data Center shall submit the developed~~
2711 ~~trends and issues report under subparagraph (b)6. to the~~
2712 ~~Governor, the President of the Senate, and the Speaker of the~~
2713 ~~House of Representatives.~~

2714 ~~(5) If such authority is terminated, the center has 1 year~~
2715 ~~to provide for the transition of its state agency customers to a~~
2716 ~~qualified alternative cloud-based data center that meets the~~
2717 ~~enterprise architecture standards established by the Florida~~
2718 ~~Digital Service.~~

2719 Section 23. Section 287.0583, Florida Statutes, is created
2720 to read:

2721 287.0583 Contract requirements for information technology
2722 commodities or services.—A contract for information technology
2723 commodities or services involving the development,
2724 customization, implementation, integration, support, or
2725 maintenance of software systems, applications, platforms, or
2726 related services must include provisions ensuring all of the

576-02812-26

2026480c2

2727 following:

2728 (1) Any data created, processed, or maintained under the
2729 contract is portable and can be extracted in a machine-readable
2730 format upon request.

2731 (2) The vendor will provide, upon request, comprehensive
2732 operational documentation sufficient to allow continued
2733 operation and maintenance by the agency or a new vendor.

2734 (3) The vendor will provide, upon request, reasonable
2735 assistance and support during a transition to the agency or to a
2736 new vendor.

2737 (4) All anticipated software license fees, license renewal
2738 fees, and operation and maintenance costs are documented in
2739 detail. If exact figures are not feasible, the vendor must
2740 provide a reasonable cost range.

2741 Section 24. Section 287.0591, Florida Statutes, is amended
2742 to read:

2743 287.0591 Information technology; vendor disqualification.-

2744 (1) (a) Any competitive solicitation issued by the
2745 department for a state term contract for information technology
2746 commodities must include a term that does not exceed 48 months.

2747 (b) ~~(2)~~ Any competitive solicitation issued by the
2748 department for a state term contract for information technology
2749 consultant services or information technology staff augmentation
2750 contractual services must include a term that does not exceed 48
2751 months.

2752 (c) ~~(3)~~ The department may execute a state term contract for
2753 information technology commodities, consultant services, or
2754 staff augmentation contractual services that exceeds the 48-
2755 month requirement if the Secretary of Management Services and

576-02812-26

2026480c2

2756 the state chief information officer certify in writing to the
2757 Executive Office of the Governor that a longer contract term is
2758 in the best interest of the state.

2759 (2)~~(4)~~ If the department issues a competitive solicitation
2760 for information technology commodities, consultant services, or
2761 staff augmentation contractual services, the department shall
2762 coordinate with the Division of Integrated Government Innovation
2763 and Technology within the Executive Office of the Governor
2764 ~~Florida Digital Service within the department shall participate~~
2765 in such solicitations. Such coordination must include reviewing
2766 the solicitation specifications to verify compliance with
2767 enterprise architecture and cybersecurity standards, evaluating
2768 vendor responses under established criteria, answering vendor
2769 questions, and providing any other technical expertise
2770 necessary.

2771 (3) (a)~~(5)~~ If an agency issues a request for quote to
2772 purchase information technology commodities, information
2773 technology consultant services, or information technology staff
2774 augmentation contractual services from the state term contract
2775 which meets the CATEGORY TWO threshold amount, but is less than
2776 the CATEGORY FOUR threshold amount:

2777 1. For any contract with 25 approved vendors or fewer, the
2778 agency must issue a request for quote to all vendors approved to
2779 provide such commodity or service.

2780 2. For any contract with more than 25 approved vendors, the
2781 agency must issue a request for quote to at least 25 of the
2782 vendors approved to provide such commodity or contractual
2783 service.

2784 (b) The agency shall maintain a copy of the request for

576-02812-26

2026480c2

2785 quote, the identity of the vendors that were sent the request
2786 for quote, and any vendor response to the request for quote for
2787 2 years after the date of issuance of the purchase order.

2788 (c) Use of a request for quote does not constitute a
2789 decision or intended decision that is subject to protest under
2790 s. 120.57(3).

2791 (4) (a) An agency issuing a request for quote to purchase
2792 information technology commodities, information technology
2793 consultant services, or information technology staff
2794 augmentation contractual services from the state term contract
2795 which exceeds the CATEGORY FOUR threshold amount is subject to
2796 public records requirements pursuant to s. 287.057.

2797 Additionally, an agency shall publish:

2798 1. The request for quote for a minimum of 10 days before
2799 executing the purchase order; and

2800 2. The name of the vendor awarded the purchase order.

2801 (b) The agency shall maintain a copy of the request for
2802 quote, the identity of the vendors that were sent the request
2803 for quote, and all vendor responses to the request for quote for
2804 2 years after the date of issuance of the purchase order.

2805 (c) Use of a request for quote does not constitute a
2806 decision or intended decision that is subject to protest under
2807 s. 120.57(3).

2808 (5) A state agency may request the Division of Integrated
2809 Government Innovation and Technology within the Executive Office
2810 of the Governor for procurement advisory and review services
2811 pursuant to s. 282.0061.

2812 (6) (a) ~~Beginning October 1, 2021, and~~ Each October 1
2813 ~~thereafter,~~ the department shall prequalify firms and

576-02812-26

2026480c2

2814 individuals to provide information technology staff augmentation
 2815 contractual services and information technology commodities on
 2816 state term contract.

2817 (b) In order to prequalify a firm or individual for
 2818 participation on the state term contract, the department must
 2819 consider, at a minimum, the capability, experience, and past
 2820 performance record of the firm or individual.

2821 (c) A firm or individual removed from the source of supply
 2822 pursuant to s. 287.042(1)(b) or placed on a disqualified vendor
 2823 list pursuant to s. 287.133 or s. 287.134 is immediately
 2824 disqualified from state term contract eligibility.

2825 (d) Once a firm or individual has been prequalified to
 2826 provide information technology staff augmentation contractual
 2827 services or information technology commodities on state term
 2828 contract, the firm or individual may respond to requests for
 2829 quotes from an agency to provide such services.

2830 Section 25. Subsection (2) of section 20.22, Florida
 2831 Statutes, is amended to read:

2832 20.22 Department of Management Services.—There is created a
 2833 Department of Management Services.

2834 (2) The following divisions, programs, and services within
 2835 the Department of Management Services are established:

2836 (a) Facilities Program.

2837 (b) ~~The Florida Digital Service.~~

2838 ~~(c)~~ Workforce Program.

2839 (c)1.~~(d)1.~~ Support Program.

2840 2. Federal Property Assistance Program.

2841 (d)~~(e)~~ Administration Program.

2842 (e)~~(f)~~ Division of Administrative Hearings.

576-02812-26

2026480c2

2843 ~~(f)(g)~~ Division of Retirement.

2844 ~~(g)(h)~~ Division of State Group Insurance.

2845 ~~(h)(i)~~ Division of Telecommunications.

2846 Section 26. Subsections (1), (5), (7), and (8) of section

2847 282.802, Florida Statutes, are amended to read:

2848 282.802 Government Technology Modernization Council.—

2849 (1) The Government Technology Modernization Council, an

2850 advisory council as defined in s. 20.03(7), is located ~~created~~

2851 within DIGIT ~~the department~~. Except as otherwise provided in

2852 this section, the advisory council shall operate in a manner

2853 consistent with s. 20.052.

2854 (5) The state chief information officer ~~Secretary of~~

2855 ~~Management Services~~, or his or her designee, shall serve as the

2856 ex officio, nonvoting executive director of the council.

2857 (7)~~(a)~~ The council shall meet at least quarterly to:

2858 (a)1. ~~(a)1.~~ Recommend legislative and administrative actions that

2859 the Legislature and state agencies as defined in s. 282.0041 ~~s.~~

2860 ~~282.318(2)~~ may take to promote the development of data

2861 modernization in this state.

2862 (b)2. ~~(b)2.~~ Assess and provide guidance on necessary legislative

2863 reforms and the creation of a state code of ethics for

2864 artificial intelligence systems in state government.

2865 (c)3. ~~(c)3.~~ Assess the effect of automated decision systems or

2866 identity management on constitutional and other legal rights,

2867 duties, and privileges of residents of this state.

2868 (d)4. ~~(d)4.~~ Evaluate common standards for artificial intelligence

2869 safety and security measures, including the benefits of

2870 requiring disclosure of the digital provenance for all images

2871 and audio created using generative artificial intelligence as a

576-02812-26

2026480c2

2872 means of revealing the origin and edit of the image or audio, as
2873 well as the best methods for such disclosure.

2874 (e)5. Assess the manner in which governmental entities and
2875 the private sector are using artificial intelligence with a
2876 focus on opportunity areas for deployments in systems across
2877 this state.

2878 (f)6. Determine the manner in which artificial intelligence
2879 is being exploited by bad actors, including foreign countries of
2880 concern as defined in s. 287.138(1).

2881 (g)7. Evaluate the need for curriculum to prepare school-
2882 age audiences with the digital media and visual literacy skills
2883 needed to navigate the digital information landscape.

2884 ~~(b) At least one quarterly meeting of the council must be a~~
2885 ~~joint meeting with the Florida Cybersecurity Advisory Council.~~

2886 (8) ~~By December 31, 2024, and~~ Each December 31 thereafter,
2887 the council shall submit to the Governor, the President of the
2888 Senate, and the Speaker of the House of Representatives any
2889 legislative recommendations considered necessary by the council
2890 to modernize government technology, including:

2891 (a) Recommendations for policies necessary to:

2892 1. Accelerate adoption of technologies that will increase
2893 productivity of state enterprise information technology systems,
2894 improve customer service levels of government, and reduce
2895 administrative or operating costs.

2896 2. Promote the development and deployment of artificial
2897 intelligence systems, financial technology, education
2898 technology, or other enterprise management software in this
2899 state.

2900 3. Protect Floridians from bad actors who use artificial

576-02812-26

2026480c2

2901 intelligence.

2902 (b) Any other information the council considers relevant.

2903 Section 27. Section 282.604, Florida Statutes, is amended
2904 to read:

2905 282.604 Adoption of rules.—DIGIT ~~The Department of~~
2906 ~~Management Services~~ shall, with input from stakeholders, adopt
2907 rules pursuant to ss. 120.536(1) and 120.54 for the development,
2908 procurement, maintenance, and use of accessible electronic
2909 information technology by governmental units.

2910 Section 28. Paragraph (b) of subsection (4) of section
2911 443.1113, Florida Statutes, is amended to read:

2912 443.1113 Reemployment Assistance Claims and Benefits
2913 Information System.—

2914 (4)

2915 (b) The department shall seek input on recommended
2916 enhancements from, at a minimum, the following entities:

2917 1. The Division of Integrated Government Innovation and
2918 Technology within the Executive Office of the Governor ~~Florida~~
2919 ~~Digital Service within the Department of Management Services.~~

2920 2. The General Tax Administration Program Office within the
2921 Department of Revenue.

2922 3. The Division of Accounting and Auditing within the
2923 Department of Financial Services.

2924 Section 29. Subsection (5) of section 943.0415, Florida
2925 Statutes, is amended to read:

2926 943.0415 Cybercrime Office.—There is created within the
2927 Department of Law Enforcement the Cybercrime Office. The office
2928 may:

2929 (5) Consult with the state chief information security

576-02812-26

2026480c2

2930 officer of the Division of Integrated Government Innovation and
2931 Technology within the Executive Office of the Governor ~~Florida~~
2932 ~~Digital Service within the Department of Management Services~~ in
2933 the adoption of rules relating to the information technology
2934 security provisions in s. 282.318.

2935 Section 30. Subsection (3) of section 1004.444, Florida
2936 Statutes, is amended to read:

2937 1004.444 Florida Center for Cybersecurity.—

2938 (3) Upon receiving a request for assistance from a ~~the~~
2939 ~~Department of Management Services, the Florida Digital Service,~~
2940 ~~or another~~ state agency, the center is authorized, but may not
2941 be compelled by the agency, to conduct, consult on, or otherwise
2942 assist any state-funded initiatives related to:

2943 (a) Cybersecurity training, professional development, and
2944 education for state and local government employees, including
2945 school districts and the judicial branch; and

2946 (b) Increasing the cybersecurity effectiveness of the
2947 state's and local governments' technology platforms and
2948 infrastructure, including school districts and the judicial
2949 branch.

2950 Section 31. This act shall take effect January 5, 2027.