

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

601-02525-26

2026480c1

A bill to be entitled

An act relating to information technology; providing for a type two transfer of the duties and functions of the Florida Digital Service from the Department of Management Services to the Division of Integrated Government Innovation and Technology; creating s. 14.205, F.S.; creating the Division of Integrated Government Innovation and Technology (DIGIT) within the Executive Office of the Governor; providing that the division is a separate budget entity and must prepare and submit a budget in accordance with specified provisions; requiring the division to be responsible for all professional, technical, and administrative support to carry out its assigned duties; providing for a director of the division; providing that the director also serves as the state chief information officer; providing for the appointment of the director; prohibiting the state chief information officer from having certain conflicts of interest; providing the qualifications for the state chief information officer; providing that the deputy director also serves as the deputy chief information officer; providing that the director will select a state chief information security officer, state chief data officer, state chief technology officer, and state chief technology procurement officer; transferring the state chief information officer of the Department of Management Services to DIGIT until the Governor appoints a

601-02525-26

2026480c1

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

601-02525-26

2026480c1

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

601-02525-26

2026480c1

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

601-02525-26

2026480c1

117 testing, best practices, and standards; specifying  
118 such best practices and standards; requiring DIGIT to  
119 produce specified reports and provide the 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

601-02525-26

2026480c1

146 the mechanism for a state agency to request such  
147 exemption; 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 the 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

601-02525-26

2026480c1

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

601-02525-26

2026480c1

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

601-02525-26

2026480c1

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

601-02525-26

2026480c1

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

601-02525-26

2026480c1

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; prohibiting state agencies from  
319 terminating services with the data center without

601-02525-26

2026480c1

320 giving written notice within a specified timeframe,  
321 procuring third-party cloud-computing services without  
322 evaluating the data center's cloud-computing services,  
323 and exceeding a specified timeframe to remit payments  
324 for services provided by the data center; specifying  
325 circumstances under which the data center's  
326 authorization to provide services may be terminated;  
327 providing that the data center has a specified  
328 timeframe to provide for the transition of state  
329 agency customers to a qualified alternative cloud-  
330 based data center that meets specified standards;  
331 providing that the data center is the lead entity  
332 responsible for creating, operating, and managing the  
333 Florida Behavioral Health Care Data Repository;  
334 providing the purpose of the repository; requiring the  
335 data center, in collaboration with the Data Analysis  
336 Committee of the Commission on Mental Health and  
337 Substance Use Disorder, to develop a specified plan;  
338 requiring, beginning on a specified date, the data  
339 center to submit a certain report annually to the  
340 Governor and the Legislature; providing for a  
341 transition to an alternative cloud-based data center  
342 under specified circumstances; revising the  
343 information the plan identifies and documents;  
344 amending s. 282.206, F.S.; requiring state agencies to  
345 submit a certain strategic plan to DIGIT and the  
346 Northwest Regional Data Center annually by a specified  
347 date; amending s. 1004.649, F.S.; creating the  
348 Northwest Regional Data Center at Florida State

601-02525-26

2026480c1

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

601-02525-26

2026480c1

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

391

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

393

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

403       Section 2. Section 14.205, Florida Statutes, is created to  
404       read:

405       14.205 Division of Integrated Government Innovation and  
406       Technology.—

601-02525-26

2026480c1

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

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

423        (b) The state chief information officer must meet the  
424 following qualifications:

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

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

430        b. Hold a master's degree in any of the fields listed in  
431 sub subparagraph a., which may be substituted for a portion of  
432 the professional experience requirements in subparagraph 2.

433        2. Professional experience requirements.—The state chief  
434 information officer must have at least 10 years of progressively  
435 responsible experience in information technology management,

601-02525-26

2026480c1

436 digital transformation, cybersecurity, or information technology  
437 governance, including:

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

442       b. Managing large-scale information technology projects,  
443 enterprise infrastructure, and implementation of emerging  
444 technologies;

445       c. Budget planning, procurement oversight, and financial  
446 management of information technology investments; and

447       d. Working with state and federal information technology  
448 regulations, digital services, and cybersecurity compliance  
449 frameworks.

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

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

457       b. Cloud and digital services with experience in cloud  
458 computing, enterprise systems modernization, digital  
459 transformation, and emerging information technology trends;

460       c. Information technology governance and policy development  
461 by demonstrating an understanding of statewide information  
462 technology governance structures, digital services, and  
463 information technology procurement policies; and

464       d. Public sector information technology management by

601-02525-26

2026480c1

465 demonstrating familiarity with government information technology  
466 funding models, procurement requirements, and legislative  
467 processes affecting information technology strategy.

468       4. Leadership and administrative competencies.—The state  
469 chief information officer must demonstrate:

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

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

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

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

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

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

491       Section 3. Until a state chief information officer is  
492 appointed pursuant to s. 14.205, Florida Statutes, the current  
493 state chief information officer of the Department of Management

601-02525-26

2026480c1

494 Services shall be transferred to the Division of Integrated  
495 Government Innovation and Technology and serve as interim state  
496 chief information officer. A state chief information officer for  
497 the Division of Integrated Government Innovation and Technology  
498 must be appointed by the Governor by June 30, 2027.

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

501       20.055 Agency inspectors general.—

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

601-02525-26

2026480c1

523 technology governance, security, and performance standards. The  
524 performance of the audits is ~~audit shall~~ be under the direction  
525 of the inspector general, except that if the inspector general  
526 does not possess the qualifications specified in subsection (4),  
527 the director of auditing must shall perform the functions listed  
528 in this subsection.

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

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

548 (c) The inspector general and the staff shall have access  
549 to any records, data, and other information of the state agency  
550 he or she deems necessary to carry out his or her duties. The  
551 inspector general may also request such information or

601-02525-26

2026480c1

552 assistance as may be necessary from the state agency or from any  
553 federal, state, or local government entity.

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

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

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

576 1. The agency information technology compliance reports  
577 must be submitted to the agency head, the Auditor General, and,  
578 for state agencies under the jurisdiction of the Governor, the  
579 Chief Inspector General by September 30 of each year.

580 2. The Chief Inspector General shall review the annual

601-02525-26

2026480c1

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

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

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

602 (h) The inspector general shall monitor the implementation  
603 of the state agency's response to any report on the state agency  
604 issued by the Auditor General or by the Office of Program Policy  
605 Analysis and Government Accountability. No later than 6 months  
606 after the Auditor General or the Office of Program Policy  
607 Analysis and Government Accountability publishes a report on the  
608 state agency, the inspector general shall provide a written  
609 response to the agency head or, for state agencies under the

601-02525-26

2026480c1

610 jurisdiction of the Governor, the Chief Inspector General on the  
611 status of corrective actions taken. The inspector general shall  
612 file a copy of such response with the Legislative Auditing  
613 Committee.

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

631 Section 5. Paragraph (b) of subsection (3) of section  
632 97.0525, Florida Statutes, is amended to read:

633 97.0525 Online voter registration.—

634 (3)

635 (b) The division shall conduct a comprehensive risk  
636 assessment of the online voter registration system every 2  
637 years. The comprehensive risk assessment must comply with the  
638 risk assessment methodology developed by the Division of

601-02525-26

2026480c1

639       Integrated Government Innovation and Technology within the  
640       Executive Office of the Governor ~~Department of Management~~  
641       Services for identifying security risks, determining the  
642       magnitude of such risks, and identifying areas that require  
643       safeguards. In addition, the comprehensive risk assessment must  
644       incorporate all of the following:

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

650       2. Screening of computers and networks used to support the  
651       online voter registration system for malware and other  
652       vulnerabilities.

653       3. Evaluation of database infrastructure, including  
654       software and operating systems, in order to fortify defenses  
655       against cyberattacks.

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

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

663       112.22 Use of applications from foreign countries of  
664       concern prohibited.—

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

666       (a) "DIGIT" means the Division of Integrated Government  
667       Innovation and Technology within the Executive Office of the

601-02525-26

2026480c1

668 Governor "Department" means the Department of Management  
669 Services.

670 (f) "Prohibited application" means an application that  
671 meets the following criteria:

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

675 a. Collecting keystrokes or sensitive personal, financial,  
676 proprietary, or other business data;

677 b. Compromising e-mail and acting as a vector for  
678 ransomware deployment;

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

680 d. Conducting surveillance and tracking of individual  
681 users; or

682 e. Using algorithmic modifications to conduct  
683 disinformation or misinformation campaigns; or

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

688 (2)

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

692 1. This paragraph does not apply to a law enforcement  
693 officer as defined in s. 943.10(1) if the use of the prohibited  
694 application is necessary to protect the public safety or conduct  
695 an investigation within the scope of his or her employment.

696 2. A public employer may request a waiver from DIGIT the

601-02525-26

2026480c1

697 ~~department~~ to allow designated employees or officers to download  
698 or access a prohibited application on a government-issued  
699 device.

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

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

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

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

714 1. A description of the activity to be conducted and the  
715 state interest furthered by the activity.

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

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

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

725 5. A description of the circumstances under which the

601-02525-26

2026480c1

726 waiver applies.

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

732 (b) DIGIT The department shall adopt rules necessary to  
733 administer this section.

734 Section 7. Paragraph (a) of subsection (5) of section  
735 119.0725, Florida Statutes, is amended to read:

736 119.0725 Agency cybersecurity information; public records  
737 exemption; public meetings exemption.—

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

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

748 216.023 Legislative budget requests to be furnished to  
749 Legislature by agencies.—

750 (4)(a) The legislative budget request for each program must  
751 contain:

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

754 2. Information on expenditures for 3 fiscal years (actual

601-02525-26

2026480c1

755 prior-year expenditures, current-year estimated expenditures,  
756 and agency budget requested expenditures for the next fiscal  
757 year) by appropriation category.

758 3. Details on trust funds and fees.

759 4. The total number of positions (authorized, fixed, and  
760 requested).

761 5. An issue narrative describing and justifying changes in  
762 amounts and positions requested for current and proposed  
763 programs for the next fiscal year.

764 6. Information resource requests.

765 7. Supporting information, including applicable cost-  
766 benefit analyses, business case analyses, performance  
767 contracting procedures, service comparisons, and impacts on  
768 performance standards for any request to outsource or privatize  
769 agency functions. The cost-benefit and business case analyses  
770 must include an assessment of the impact on each affected  
771 activity from those identified in accordance with paragraph (b).  
772 Performance standards must include standards for each affected  
773 activity and be expressed in terms of the associated unit of  
774 activity.

775 8. An evaluation of major outsourcing and privatization  
776 initiatives undertaken during the last 5 fiscal years having  
777 aggregate expenditures exceeding \$10 million during the term of  
778 the contract. The evaluation must include an assessment of  
779 contractor performance, a comparison of anticipated service  
780 levels to actual service levels, and a comparison of estimated  
781 savings to actual savings achieved. Consolidated reports issued  
782 by the Department of Management Services may be used to satisfy  
783 this requirement.

601-02525-26

2026480c1

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

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

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

810        ~~(a) The name of the technology system.~~  
811        ~~(b) A brief description of the purpose and function of the  
812 system.~~

601-02525-26

2026480c1

- (c) A brief description of the goals of the project.
- (d) The initiation date of the project.
- (e) The key performance indicators for the project.
- (f) Any other metrics for the project evaluating the health status of the project.

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

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

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

For purposes of this subsection, an ongoing technology-related project is one which has been funded or has had or is expected to have expenditures in more than one fiscal year. An ongoing technology-related project does not include the continuance of existing hardware and software maintenance agreements, the renewal of existing software licensing agreements, or the replacement of desktop units with new technology that is substantially similar to the technology being replaced. This subsection expires July 1, 2026.

Section 9. Present subsections (36), (37), and (38) of section 282.0041, Florida Statutes, are redesignated as subsections (37), (38), and (39), respectively, new subsections (11) and (36) are added to that section, and subsection (1), present subsection (7), and subsections (27) and (29) of that section are amended, to read:

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

(1) "Agency assessment" means the amount each customer

601-02525-26

2026480c1

entity must pay annually for services from the Department of Management Services and includes administrative and data center services costs.

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

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

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

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

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

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

282.00515 Duties of Cabinet agencies.—

(1) (a) The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services shall adopt the standards, best practices,

601-02525-26

2026480c1

processes, and methodologies established in s. 282.0061(4) and (5)(b) and (d). However, such departments may s. 282.0051(1)(b), (e), and (r) and (3)(e) or adopt alternative standards, best practices, and methodologies that must be based on industry-recognized best practices and industry standards that enable allow for open data exchange, interoperability, and vendor-neutral integration. Such departments shall evaluate the adoption of alternative standards on a case-by-case basis for each standard, project, or system and reevaluate such alternative standards periodically.

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

(2) If the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services adopts alternative standards, best practices, processes, and methodologies in lieu of the enterprise architecture standards, best practices, processes, and methodologies adopted pursuant to s. 282.0061(4) and (5)(b) and (d) s. 282.0051, such department must notify DIGIT, the Governor, the President of the Senate, and the Speaker of the House of Representatives in writing of the adoption of the alternative standards and provide a justification for adoption of the alternative standards and explain the manner in which how

601-02525-26

2026480c1

900 the agency will achieve the policy, standard, guideline, or best  
901 practice while promoting open data interoperability.

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

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

924 (5) The Department of Legal Affairs, the Department of  
925 Financial Services, and the Department of Agriculture and  
926 Consumer Services may, but are not required to, contract with  
927 DIGIT the department to provide procurement advisory and review  
928 services for information technology projects as provided in s.

601-02525-26

2026480c1

282.0061(5)(a) ~~or perform any of the services and functions described in s. 282.0051.~~

(6) The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services shall use the information technology reports developed by DIGIT pursuant to s. 282.0061(5)(f) and follow the streamlined reporting process pursuant to s. 282.0061(5)(i). The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services shall report annually to the President of the Senate and the Speaker of the House of Representatives by December 15 information related to the respective department similar to the information required under s. 282.006(6)(a) and the information technology financial data methodology and reporting required by s. 282.0061(6). The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services may provide the report required under this subsection collectively with DIGIT or shall report separately to the Governor, the President of the Senate, and the Speaker of the House of Representatives.

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

(b) ~~DIGIT~~ The department, ~~acting through the Florida Digital Service~~, may not retrieve or disclose any data without a shared-data agreement in place between DIGIT ~~the department~~ and

601-02525-26

2026480c1

958 the Department of Legal Affairs, the Department of Financial  
959 Services, or the Department of Agriculture and Consumer  
960 Services.

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

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

601-02525-26

2026480c1

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

991       Section 11. Section 282.006, Florida Statutes, is created  
992 to read:

993       282.006 Division of Integrated Government Innovation and  
994 Technology; enterprise responsibilities; reporting.—

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

1003       (2) The Legislature intends for DIGIT policy, standards,  
1004 guidance, and oversight to allow for adaptability to emerging  
1005 technology and organizational needs while maintaining compliance  
1006 with industry best practices. All policies, standards, and  
1007 guidelines established pursuant to this chapter must be  
1008 technology-agnostic and may not prescribe specific tools,  
1009 platforms, or vendors.

1010       (3) DIGIT shall establish the strategic direction of  
1011 information technology for state agencies. DIGIT shall develop  
1012 and publish information technology policy that aligns with  
1013 industry best practices for the management of the state's  
1014 information technology resources. The policy must be updated as  
1015 necessary to meet the requirements of this chapter and

601-02525-26

2026480c1

1016 advancements in technology.

1017 (4) DIGIT shall, in coordination with state agency  
1018 technology subject matter experts, develop, publish, and  
1019 maintain an enterprise architecture that:

1020 (a) Acknowledges the unique needs of the entities within  
1021 the enterprise in the development and publication of standards  
1022 and terminologies to facilitate digital interoperability;

1023 (b) Supports the cloud-first policy as specified in s.

1024 282.206;

1025 (c) Addresses the manner in which information technology  
1026 infrastructure may be modernized to achieve security,  
1027 scalability, maintainability, interoperability, and improved  
1028 cost-efficiency goals; and

1029 (d) Includes, at a minimum, best practices, guidelines, and  
1030 standards for:

1031 1. Data models and taxonomies.

1032 2. Master data management.

1033 3. Data integration and interoperability.

1034 4. Data security and encryption.

1035 5. Bot prevention and data protection.

1036 6. Data backup and recovery.

1037 7. Application portfolio and catalog requirements.

1038 8. Application architectural patterns and principles.

1039 9. Technology and platform standards.

1040 10. Secure coding practices.

1041 11. Performance and scalability.

1042 12. Cloud infrastructure and architecture.

1043 13. Networking, connectivity, and security protocols.

1044 14. Authentication, authorization, and access controls.

601-02525-26

2026480c1

1045        15. Disaster recovery.

1046        16. Quality assurance.

1047        17. Testing methodologies and measurements.

1048        18. Logging and log retention.

1049        19. Application and use of artificial intelligence.

1050        (5) DIGIT shall develop open data technical standards and  
1051 terminologies for use by state agencies. DIGIT shall develop  
1052 enterprise technology testing and quality assurance best  
1053 practices and standards to ensure the reliability, security, and  
1054 performance of information technology systems. Such best  
1055 practices and standards must include:

1056        (a) Functional testing to ensure software or systems meet  
1057 required specifications.

1058        (b) Performance and load testing to ensure software and  
1059 systems operate efficiently under various conditions.

1060        (c) Security testing to protect software and systems from  
1061 vulnerabilities and cyber threats.

1062        (d) Compatibility and interoperability testing to ensure  
1063 software and systems operate seamlessly across environments.

1064        (6) DIGIT shall produce and provide the following reports  
1065 to the Governor, the President of the Senate, and the Speaker of  
1066 the House of Representatives:

1067        (a) Annually by December 15, an enterprise analysis report  
1068 for state agencies which includes all of the following:

1069        1. Results of the state agency needs assessments, including  
1070 any plan to address technical debt as required by s. 282.0061  
1071 pursuant to the schedule adopted.

1072        2. Alternative standards related to federal funding adopted  
1073 pursuant to s. 282.0061.

601-02525-26

2026480c1

1074       3. Information technology financial data for each state  
1075       agency for the previous fiscal year. This portion of the annual  
1076       report must include, at a minimum, the following recurring and  
1077       nonrecurring information:

1078       a. Total number of full-time equivalent positions.  
1079       b. Total amount of salary.  
1080       c. Total amount of benefits.  
1081       d. Total number of comparable full-time equivalent  
1082       positions and total amount of expenditures for information  
1083       technology staff augmentation.

1084       e. Total number of contracts and purchase orders and total  
1085       amount of associated expenditures for information technology  
1086       managed services.

1087       f. Total amount of expenditures by state term contract as  
1088       defined in s. 287.012, contracts procured using alternative  
1089       purchasing methods as authorized pursuant to s. 287.042(16), and  
1090       state agency procurements through request for proposal,  
1091       invitation to negotiate, invitation to bid, single source, and  
1092       emergency purchases.

1093       g. Total amount of expenditures for hardware.  
1094       h. Total amount of expenditures for non-cloud software.  
1095       i. Total amount of expenditures for cloud software licenses  
1096       and services with a separate amount for expenditures for state  
1097       data center services.

1098       j. Total amount of expenditures for cloud data center  
1099       services with a separate amount for expenditures for state data  
1100       center services.

1101       k. Total amount of expenditures for administrative costs.  
1102       4. Consolidated information for the previous fiscal year

601-02525-26

2026480c1

1103 about state information technology projects, which must include,  
1104 at a minimum, the following information:

1105 a. Anticipated funding requirements for information  
1106 technology support over the next 5 years.

1107 b. An inventory of current information technology assets  
1108 and major projects. As used in this paragraph, the term "major  
1109 project" includes projects costing more than \$500,000 to  
1110 implement.

1111 c. Significant unmet needs for information technology  
1112 resources over the next 5 fiscal years, ranked in priority order  
1113 according to their urgency.

1114 5. A review and summary of whether the information  
1115 technology contract policy established pursuant to s. 282.0064  
1116 is included in all solicitations and contracts.

1117 (b) Biennially by December 15 of even-numbered years, a  
1118 report on the strategic direction of information technology in  
1119 the state which includes recommendations for all of the  
1120 following:

1121 1. Standardization and consolidation of information  
1122 technology services that are identified as common across state  
1123 agencies as required in s. 282.0061.

1124 2. Information technology services needed to be designed,  
1125 delivered, and managed as state agency enterprise information  
1126 technology services. Recommendations must include the  
1127 identification of existing information technology resources  
1128 associated with the services, if existing services must be  
1129 transferred as a result of being delivered and managed as  
1130 enterprise information technology services, and which entity is  
1131 best suited to manage the service.

601-02525-26

2026480c1

1132        (c)1. When conducted as provided in this paragraph, a  
1133        market analysis and accompanying strategic plan submitted by  
1134        December 31 of each year that the market analysis is conducted.

1135        2. No less frequently than every 3 years, DIGIT shall  
1136        conduct a market analysis to determine whether the:

1137        a. Information technology resources across state agencies  
1138        are used in the most cost-effective and cost-efficient manner,  
1139        while recognizing that the replacement of certain legacy  
1140        information technology systems within the enterprise may be cost  
1141        prohibitive or cost inefficient due to the remaining useful life  
1142        of those resources; and

1143        b. State agencies are using best practices with respect to  
1144        information technology, information services, and the  
1145        acquisition of emerging technologies and information services.

1146        3. Each market analysis must be used to prepare a strategic  
1147        plan for continued and future information technology and  
1148        information services, including, but not limited to, proposed  
1149        acquisition of new services or technologies and approaches to  
1150        the implementation of any new services or technologies.

1151        (7) (a) DIGIT shall develop, implement, and maintain a  
1152        library to serve as the official repository for all enterprise  
1153        information technology policies, standards, guidelines, and best  
1154        practices applicable to state agencies. The online library must  
1155        be accessible and searchable by all state agencies and the  
1156        Department of Legal Affairs, the Department of Financial  
1157        Services, and the Department of Agriculture and Consumer  
1158        Services through a secure authentication system. The library  
1159        must include standardized checklists organized by technical  
1160        subject areas to assist state agencies in measuring compliance

601-02525-26

2026480c1

1161 with the information technology policies, standards, guidelines,  
1162 and best practices.

1163 (b) DIGIT shall establish procedures to ensure the  
1164 integrity, security, and availability of the library, including  
1165 appropriate access controls, encryption, and disaster recovery  
1166 measures. DIGIT shall regularly update documents and materials  
1167 in the library to reflect current state and federal  
1168 requirements, industry best practices, and emerging technologies  
1169 and shall maintain version control and revision history for all  
1170 published documents. DIGIT shall create mechanisms for state  
1171 agencies to submit feedback, request clarifications, and  
1172 recommend updates.

1173 (8) (a) Each state agency shall actively participate and  
1174 collaborate with DIGIT to achieve the objectives set forth in  
1175 this chapter. Each state agency shall also adhere to the  
1176 policies, standards, guidelines, and best practices established  
1177 by DIGIT in information technology planning, procurement,  
1178 implementation, and operations as required by this chapter.

1179 (b) 1. A state agency may request an exemption to a specific  
1180 policy, standard, or guideline when compliance is not  
1181 technically feasible, would cause undue hardship, or conflicts  
1182 with any agency-specific statutory requirement. The state agency  
1183 requesting an exception must submit a formal justification to  
1184 DIGIT detailing all of the following:

1185 a. The specific requirement for which an exemption is  
1186 sought.

1187 b. The reason compliance is not feasible or practical.

1188 c. Any compensating control or alternative measure the  
1189 state agency will implement to mitigate associated risks.

601-02525-26

2026480c1

1190                   d. The anticipated duration of the exemption.

1191                   2. DIGIT shall review all exemption requests and provide a  
1192                   recommendation to the state chief information officer, who shall  
1193                   present the compliance exemption requests to the chief  
1194                   information officer workgroup. Approval of exemption requests  
1195                   must be made by a majority vote of the workgroup. Approved  
1196                   exemptions must be documented and include conditions and  
1197                   expiration dates.

1198                   3. A state agency with an approved exemption shall undergo  
1199                   periodic review to determine whether the exemption remains  
1200                   necessary or whether compliance can be achieved.

1201                   (9) DIGIT may adopt rules to implement this chapter.

1202                   Section 12. Section 282.0061, Florida Statutes, is created  
1203                   to read:

1204                   282.0061 DIGIT support of state agencies; information  
1205                   technology procurement and projects.—

1206                   (1) LEGISLATIVE INTENT.—The Legislature intends for DIGIT  
1207                   to support state agencies in their information technology  
1208                   efforts through the adoption of policies, standards, and  
1209                   guidance and by providing oversight that recognizes unique state  
1210                   agency information technology needs, environments, and goals.  
1211                   DIGIT assistance and support must allow for adaptability to  
1212                   emerging technologies and organizational needs while maintaining  
1213                   compliance with industry best practices. DIGIT may not prescribe  
1214                   specific tools, platforms, or vendors.

1215                   (2) NEEDS ASSESSMENTS.—

1216                   (a) By January 1, 2029, DIGIT shall conduct full baseline  
1217                   needs assessments of state agencies to document their respective  
1218                   technical environments, existing technical debt, security risks,

601-02525-26

2026480c1

1219 and compliance with all information technology standards and  
1220 guidelines developed and published by DIGIT. The needs  
1221 assessment must use the latest version of the Capability  
1222 Maturity Model Integration to evaluate each state agency's  
1223 information technology capabilities, providing a maturity level  
1224 rating for each assessed domain. After completion of the initial  
1225 full baseline needs assessment, such assessments must be  
1226 maintained and updated on a regular schedule adopted by DIGIT.

1227 (b) In assessing the existing technical debt portion of the  
1228 needs assessment, DIGIT shall analyze the state's legacy  
1229 information technology systems and develop a plan to document  
1230 the needs and costs for replacement systems. The plan must  
1231 include an inventory of legacy applications and infrastructure;  
1232 the required capabilities not available with the legacy system;  
1233 the estimated process, timeline, and cost to migrate from legacy  
1234 environments; and any other information necessary for fiscal or  
1235 technology planning. The plan must determine and document the  
1236 estimated timeframe during which the state agency can continue  
1237 to efficiently use legacy information technology systems,  
1238 resources, security, and data management to support operations.  
1239 State agencies shall provide all necessary documentation to  
1240 enable accurate reporting on legacy systems.

1241 (c) DIGIT shall develop a plan and schedule to conduct the  
1242 initial full baseline needs assessments. By October 1, 2027,  
1243 DIGIT shall submit the plan to the Governor, the President of  
1244 the Senate, and the Speaker of the House of Representatives.

1245 (d) DIGIT shall support state agency strategic planning  
1246 efforts and assist state agencies with the production of a  
1247 phased roadmap to address known technology gaps and deficiencies

601-02525-26

2026480c1

1248 as identified in the needs assessments. The roadmaps must  
1249 include specific strategies and initiatives aimed at advancing  
1250 the state agency's maturity level in accordance with the latest  
1251 version of the Capability Maturity Model Integration. State  
1252 agencies shall create, maintain, and submit the roadmap on an  
1253 annual basis with their legislative budget requests required  
1254 under s. 216.023.

1255 (3) STANDARDIZATION.—DIGIT shall:

1256 (a) Recommend in its annual enterprise analysis report for  
1257 state agencies required under s. 282.006 any potential method  
1258 for standardizing data across state agencies which will promote  
1259 interoperability and reduce the collection of duplicative data.

1260 (b) Identify any opportunities in such enterprise analysis  
1261 report for state agencies for standardization and consolidation  
1262 of information technology services that are common across all  
1263 state agencies and that support:

1264 1. Improved interoperability, security, scalability,  
1265 maintainability, and cost efficiency; and

1266 2. Business functions and operations, including  
1267 administrative functions such as purchasing, accounting and  
1268 reporting, cash management, and personnel.

1269 (c) Review all state agency information technology  
1270 legislative budget requests for compliance with the enterprise  
1271 architecture, project planning standards, and cybersecurity and  
1272 provide a report of the findings to the Executive Office of the  
1273 Governor's Office of Policy and Budget for consideration for  
1274 funding decisions in the Governor's recommended budget.

1275 (4) DATA MANAGEMENT.—

1276 (a) DIGIT shall develop standards for use by state agencies

601-02525-26

2026480c1

1277 which support best practices for master data management at the  
1278 state agency level to facilitate enterprise data sharing and  
1279 interoperability.

1280 (b) DIGIT shall establish a methodology and strategy for  
1281 implementing statewide master data management and submit a  
1282 report to the Governor, the President of the Senate, and the  
1283 Speaker of the House of Representatives by December 1, 2029. The  
1284 report must include the vision, goals, and benefits of  
1285 implementing a statewide master data management initiative, an  
1286 analysis of the current state of data management, and the  
1287 recommended strategy, methodology, and estimated timeline and  
1288 resources needed at a state agency and enterprise level to  
1289 accomplish the initiative.

1290 (5) INFORMATION TECHNOLOGY PROJECTS.—DIGIT has the  
1291 following duties and responsibilities related to state agency  
1292 technology projects:

1293 (a) Provide procurement advisory and review services for  
1294 information technology projects to all state agencies, including  
1295 procurement and contract development assistance to meet the  
1296 information technology contract policy established pursuant to  
1297 s. 282.0064.

1298 (b) Establish best practices and procurement processes and  
1299 develop metrics to support these processes for the procurement  
1300 of information technology products and services in order to  
1301 reduce costs or improve the provision of government services.

1302 (c) Upon request, assist state agencies in the development  
1303 of information technology-related legislative budget requests.

1304 (d) Develop standards and accountability measures for  
1305 information technology project planning and implementation,

601-02525-26

2026480c1

1306 including criteria for effective project management and  
1307 oversight. State agencies shall satisfy these standards and  
1308 measures when implementing information technology projects. To  
1309 support data-driven decisionmaking, the standards and measures  
1310 must include, but are not limited to:

1311 1. Performance measurements and metrics that objectively  
1312 assess the progress and risks of an information technology  
1313 project based on a defined and documented project scope, to  
1314 include the number of impacted stakeholders, cost, and schedule,  
1315 to determine whether the project is performing as planned and  
1316 delivering the intended outcomes.

1317 2. Methodologies for calculating and defining acceptable  
1318 variances between the planned and actual scope of a technology  
1319 project which provide clear thresholds for guiding corrective  
1320 actions. Such methodologies must account for project complexity  
1321 and scale, schedule, performance, quality, and the cost of an  
1322 information technology project.

1323 3. Reporting requirements that ensure timely notifications  
1324 to all defined stakeholders when an information technology  
1325 project exceeds acceptable variances defined and documented in a  
1326 project plan, including any variance that results in a schedule  
1327 delay of 1 month or more or a cost increase of \$1 million or  
1328 more, and that establish procedures for escalating critical  
1329 issues to appropriate individuals.

1330 4. Technical reporting metrics to determine if an  
1331 information technology project complies with the enterprise  
1332 architecture standards.

1333 5. Minimum requirements for engaging stakeholders  
1334 throughout a project's life cycle.

601-02525-26

2026480c1

1335                   (e) Develop a framework that provides processes,  
1336 activities, and deliverables state agencies must comply with  
1337 when planning an information technology project. The processes,  
1338 activities, and deliverables must include, but are not limited  
1339 to, all of the following:

1340                   1. Business case development, including the information  
1341 required by s. 287.0571(4), full life cycle cost estimates,  
1342 governance structure, system interoperability goals, data  
1343 management plans, scalability approach, evaluation of  
1344 cybersecurity and data privacy risks, and technology-specific  
1345 performance metrics and service levels.

1346                   2. Market research, including the use of a request for  
1347 information as defined in s. 287.012.

1348                   3. Planning and scheduling.

1349                   4. Stakeholder engagement.

1350                   5. Risk assessment.

1351                   6. Procurement strategy.

1352                   7. Project governance definition.

1353                   8. System design and requirements.

1354                   9. Change management.

1355                   10. Monitoring and reporting.

1356                   11. Postimplementation review and planning.

1357                   12. Solicitation documentation.

1358                   (f) Develop information technology project reports for use  
1359 by state agencies, including, but not limited to, operational  
1360 work plans, project spending plans, and project status reports.  
1361 Reporting standards must include content, format, and frequency  
1362 of project updates.

1363                   (g) Develop and provide training specific to information

601-02525-26

2026480c1

1364 technology project management and oversight which supplements  
1365 and enhances the training offered by the department and the  
1366 Chief Financial Officer under s. 287.057(15) (b) . DIGIT shall  
1367 evaluate such training every 2 years to assess its effectiveness  
1368 and update the training curriculum. The training must address  
1369 the unique requirements and risk profiles of state information  
1370 technology projects, procurements, contract management, and  
1371 vendor management.

1372 (h) Perform project oversight on all state agency  
1373 information technology projects that have total project costs of  
1374 \$10 million or more. DIGIT shall report by the 30th day after  
1375 the end of each quarter to the Executive Office of the Governor,  
1376 the President of the Senate, and the Speaker of the House of  
1377 Representatives on any information technology project that DIGIT  
1378 identifies as high-risk due to the project exceeding the  
1379 acceptable project variance thresholds provided in the project  
1380 management and oversight standards. The report must include a  
1381 risk assessment, including fiscal risks associated with  
1382 proceeding to the next stage of the project, a list of all  
1383 projects with a performance deficiency, reported pursuant to s.  
1384 287.057(26) (d)1., which has not been corrected as of the end of  
1385 the reporting period, and a recommendation for corrective  
1386 actions required, including suspension or termination of the  
1387 project.

1388 (i) Establish a streamlined reporting process with clear  
1389 timelines and escalation procedures for notifying a state agency  
1390 of noncompliance with the standards developed and adopted by  
1391 DIGIT.

1392 (6) INFORMATION TECHNOLOGY FINANCIAL DATA.—

601-02525-26

2026480c1

1393       (a) In consultation with state agencies, DIGIT shall create  
1394       a methodology, an approach, and applicable templates and formats  
1395       for identifying and collecting both current and planned  
1396       information technology expenditure data at the state agency  
1397       level. DIGIT shall continuously obtain, review, and maintain  
1398       records of the appropriations, expenditures, and revenues for  
1399       information technology for each state agency.

1400       (b) DIGIT shall prescribe the format for state agencies to  
1401       provide all necessary financial information to DIGIT for  
1402       inclusion in the annual report required under s. 282.006. State  
1403       agencies shall provide the information to DIGIT by October 1 for  
1404       the previous fiscal year.

1405       (7) FEDERAL CONFLICTS.—DIGIT must work with state agencies  
1406       to provide alternative standards, policies, or requirements that  
1407       do not conflict with federal regulations or requirements if  
1408       adherence to standards or policies adopted by or established  
1409       pursuant to this section conflict with federal regulations or  
1410       requirements imposed on an entity within the enterprise and  
1411       results in, or is expected to result in, adverse action against  
1412       any state agency or loss of federal funding.

1413       Section 13. Section 282.0062, Florida Statutes, is created  
1414       to read:

1415       282.0062 DIGIT workgroups.—The following workgroups are  
1416       established within DIGIT to facilitate coordination with state  
1417       agencies:

1418       (1) CHIEF INFORMATION OFFICER WORKGROUP.—

1419       (a) The chief information officer workgroup, composed of  
1420       all state agency chief information officers, shall consider and  
1421       make recommendations to the state chief information officer and

601-02525-26

2026480c1

1422 the state chief information architect on such matters as  
1423 enterprise information technology policies, standards, services,  
1424 and architecture. The workgroup may also identify and recommend  
1425 opportunities for the establishment of public-private  
1426 partnerships when considering technology infrastructure and  
1427 services in order to accelerate project delivery and provide a  
1428 source of new or increased project funding.

1429 (b) At a minimum, the state chief information officer shall  
1430 consult with the workgroup on a quarterly basis with regard to  
1431 executing the duties and responsibilities of the state agencies  
1432 related to statewide information technology strategic planning  
1433 and policy.

1434 (2) ENTERPRISE DATA AND INTEROPERABILITY WORKGROUP.—

1435 (a) The enterprise data and interoperability workgroup,  
1436 composed of chief data officer representatives from all state  
1437 agencies, shall consider and make recommendations to the state  
1438 chief data officer on such matters as enterprise data policies,  
1439 standards, services, and architecture that promote data  
1440 consistency, accessibility, and seamless integration across the  
1441 enterprise.

1442 (b) At a minimum, the state chief data officer shall  
1443 consult with the workgroup on a quarterly basis with regard to  
1444 executing the duties and responsibilities of the state agencies  
1445 related to statewide data governance planning and policy.

1446 (3) ENTERPRISE SECURITY WORKGROUP.—

1447 (a) The enterprise security workgroup, composed of chief  
1448 information security officer representatives from all state  
1449 agencies, shall consider and make recommendations to the state  
1450 chief information security officer on such matters as

601-02525-26

2026480c1

1451 cybersecurity policies, standards, services, and architecture  
1452 that promote the protection of state assets.

1453 (b) At a minimum, the state chief information security  
1454 officer shall consult with the workgroup on a quarterly basis  
1455 with regard to executing the duties and responsibilities of the  
1456 state agencies related to cybersecurity governance and policy  
1457 development.

1458 (4) ENTERPRISE INFORMATION TECHNOLOGY QUALITY ASSURANCE  
1459 WORKGROUP.—

1460 (a) The enterprise information technology quality assurance  
1461 workgroup, composed of testing and quality assurance  
1462 representatives from all state agencies, shall consider and make  
1463 recommendations to the state chief technology officer on such  
1464 matters as testing methodologies, tools, and best practices to  
1465 reduce risks related to software defects, cybersecurity threats,  
1466 and operational failures.

1467 (b) At a minimum, the state chief information officer shall  
1468 consult with the workgroup on a quarterly basis with regard to  
1469 executing the duties and responsibilities of the state agencies  
1470 related to enterprise software testing and quality assurance  
1471 standards.

1472 (5) ENTERPRISE INFORMATION TECHNOLOGY PROJECT MANAGEMENT  
1473 WORKGROUP.—

1474 (a) The enterprise information technology project  
1475 management workgroup, composed of information technology project  
1476 manager representatives from all state agencies, shall consider  
1477 and make recommendations to the state chief technology officer  
1478 on such matters as information technology project management  
1479 policies, standards, accountability measures, and services that

601-02525-26

2026480c1

1480 promote project governance and standardization across the  
1481 enterprise.

1482 (b) At a minimum, the state chief information officer shall  
1483 consult with the workgroup on a quarterly basis with regard to  
1484 executing the duties and responsibilities of the state agencies  
1485 related to project management and oversight.

1486 (6) ENTERPRISE INFORMATION TECHNOLOGY PURCHASING  
1487 WORKGROUP.—

1488 (a) The enterprise information technology purchasing  
1489 workgroup, composed of information technology procurement  
1490 representatives from all state agencies, shall consider and make  
1491 recommendations to the state chief technology procurement  
1492 officer on such matters as information technology procurement  
1493 policies, standards, and purchasing strategy and optimization  
1494 that promote best practices for contract negotiation,  
1495 consolidation, and effective service-level agreement  
1496 implementation across the enterprise.

1497 (b) At a minimum, the state chief information officer shall  
1498 consult with the workgroup on a quarterly basis with regard to  
1499 executing the duties and responsibilities of the state agencies  
1500 related to technology evaluation, purchasing, and cost savings.

1501 (7) DEPARTMENT OF LEGAL AFFAIRS, DEPARTMENT OF FINANCIAL  
1502 SERVICES, AND DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES  
1503 INFORMATION TECHNOLOGY STAFF.—Appropriate information technology  
1504 staff of the Department of Legal Affairs, the Department of  
1505 Financial Services, and the Department of Agriculture and  
1506 Consumer Services shall participate in the workgroups created  
1507 under subsections (1), (2), and (3) and may participate in any  
1508 other workgroups as authorized by their respective elected

601-02525-26

2026480c1

1509 official.1510 Section 14. Section 282.0063, Florida Statutes, is created  
1511 to read:1512 282.0063 State information technology professionals career  
1513 paths and training.-1514 (1) DIGIT shall develop standardized frameworks for, and  
1515 career paths, progressions, and training programs for, the  
1516 benefit of state agency information technology personnel. To  
1517 meet that goal, DIGIT shall:1518 (a) Assess current and future information technology  
1519 workforce needs across state agencies, identify skill gaps, and  
1520 develop strategies to address them.1521 (b) Develop and establish a training program for state  
1522 agencies to support the understanding and implementation of each  
1523 element of the enterprise architecture.1524 (c) Establish training programs, certifications, and  
1525 continuing education opportunities to enhance information  
1526 technology competencies, including cybersecurity, cloud  
1527 computing, and emerging technologies.1528 (d) Support initiatives to provide existing employees with  
1529 training or other opportunities to develop skills in emerging  
1530 technologies and automation, ensuring that state agencies remain  
1531 competitive and innovative.1532 (e) Develop strategies to recruit and retain information  
1533 technology professionals, including internship programs,  
1534 apprenticeships, partnerships with educational institutions,  
1535 scholarships for service, and initiatives to attract diverse  
1536 talent.1537 (2) DIGIT shall consult with CareerSource Florida, Inc.,

601-02525-26

2026480c1

1538 the Department of Commerce, and the Department of Education in  
1539 the implementation of this section.

1540 Section 15. Section 282.0064, Florida Statutes, is created  
1541 to read:

1542 282.0064 Information technology contract policy.—

1543 (1) In coordination with the Department of Management

1544 Services, DIGIT shall establish a policy for all information  
1545 technology-related solicitations and contracts, including state  
1546 term contracts; contracts sourced using alternative purchasing  
1547 methods as authorized pursuant to s. 287.042(16); sole source  
1548 and emergency procurements; and contracts for commodities,  
1549 consultant services, and staff augmentation services.

1550 (2) Related to state term contracts, the information

1551 technology policy must include:

1552 (a) Identification of the information technology product  
1553 and service categories to be included in state term contracts.

1554 (b) The term of each information technology-related state  
1555 term contract.

1556 (c) The maximum number of vendors authorized on each state  
1557 term contract.

1558 (3) For all contracts, the information technology policy  
1559 must include:

1560 (a) Evaluation criteria for the award of information  
1561 technology-related contracts.

1562 (b) Requirements to be included in solicitations.

1563 (c) At a minimum, a requirement that any contract for  
1564 information technology commodities or services meet the  
1565 requirements of the enterprise architecture and National  
1566 Institute of Standards and Technology Cybersecurity Framework.

601-02525-26

2026480c1

1567        (4) The policy must include the following requirements for  
1568 any information technology project that requires project  
1569 oversight through independent verification and validation:

1570        (a) An entity providing independent verification and  
1571 validation may not have any:

1572        1. Technical, managerial, or financial interest in the  
1573 project; or

1574        2. Responsibility for or participation in any other aspect  
1575 of the project.

1576        (b) The primary objective of independent verification and  
1577 validation must be to provide an objective assessment throughout  
1578 the entire project life cycle, reporting directly to all  
1579 relevant stakeholders. An independent verification and  
1580 validation entity shall independently verify and validate  
1581 whether:

1582        1. The project is being built and implemented in accordance  
1583 with defined technical architecture, specifications, and  
1584 requirements.

1585        2. The project is adhering to established project  
1586 management processes.

1587        3. The procurement of products, tools, and services and  
1588 resulting contracts aligns with current statutory and regulatory  
1589 requirements.

1590        4. The value of services delivered is commensurate with  
1591 project costs.

1592        5. The completed project meets the actual needs of the  
1593 intended users.

1594        (c) The entity performing independent verification and  
1595 validation shall provide regular reports and assessments

601-02525-26

2026480c1

1596 directly to the designated oversight body, identifying risks,  
1597 deficiencies, and recommendations for corrective actions to  
1598 ensure project success and compliance with statutory  
1599 requirements.

1600 (5) The Division of State Purchasing in the Department of  
1601 Management Services shall coordinate with DIGIT on state term  
1602 contract solicitations and invitations to negotiate related to  
1603 information technology. Such coordination must include reviewing  
1604 the solicitation specifications to verify compliance with  
1605 enterprise architecture and cybersecurity standards, evaluating  
1606 vendor responses under established criteria, answering vendor  
1607 questions, and providing any other technical expertise  
1608 necessary.

1609 (6) The Department of Legal Affairs, the Department of  
1610 Financial Services, and the Department of Agriculture and  
1611 Consumer Services may adopt alternatives to the information  
1612 technology policy established by DIGIT pursuant to this section.  
1613 If alternatives to the policy are adopted, such department must  
1614 notify DIGIT, the Governor, the President of the Senate, and the  
1615 Speaker of the House of Representatives in writing of the  
1616 adoption of the alternatives and provide a justification for  
1617 adoption of the alternatives, including whether the alternatives  
1618 were necessary to meet alternatives adopted pursuant to s.  
1619 282.00515, and explain the manner in which the department will  
1620 achieve the information technology policy.

1621 Section 16. Subsections (3), (4), (7), and (10) of section  
1622 282.318, Florida Statutes, are amended to read:

1623 282.318 Cybersecurity.—

1624 (3) DIGIT The department, acting through the Florida

601-02525-26

2026480c1

1625 ~~Digital Service~~, is the lead entity responsible for establishing  
1626 standards and processes for assessing state agency cybersecurity  
1627 risks and determining appropriate security measures that comply  
1628 with the latest national and state data compliance security  
1629 standards. Such standards and processes must be consistent with  
1630 generally accepted technology best practices, including the  
1631 National Institute for Standards and Technology Cybersecurity  
1632 Framework, for cybersecurity. DIGIT ~~The department, acting~~  
1633 ~~through the Florida Digital Service~~, shall adopt rules that  
1634 mitigate risks; safeguard state agency digital assets, data,  
1635 information, and information technology resources to ensure  
1636 availability, confidentiality, and integrity; and support a  
1637 security governance framework. DIGIT ~~The department, acting~~  
1638 ~~through the Florida Digital Service~~, shall also:

1639 (a) Designate an employee ~~of the Florida Digital Service~~ as  
1640 the state chief information security officer. The state chief  
1641 information security officer must have experience and expertise  
1642 in security and risk management for communications and  
1643 information technology resources. The state chief information  
1644 security officer is responsible for the development of  
1645 enterprise cybersecurity policy, standards, operation, and  
1646 security architecture ~~oversight of cybersecurity~~ for state  
1647 technology systems. The state chief information security officer  
1648 must ~~shall~~ be notified of all confirmed or suspected incidents  
1649 or threats of state agency information technology resources and  
1650 must report such incidents or threats to the state chief  
1651 information officer ~~and the Governor~~.

1652 (b) Develop, and annually update by February 1, a statewide  
1653 cybersecurity strategic plan that includes security goals and

601-02525-26

2026480c1

1654 objectives for cybersecurity, including the identification and  
1655 mitigation of risk, proactive protections against threats,  
1656 tactical risk detection, threat reporting, and response and  
1657 recovery protocols for a cyber incident.

1658 (c) Develop and publish for use by state agencies a  
1659 cybersecurity governance framework that, at a minimum, includes  
1660 guidelines and processes for:

1661 1. Establishing asset management procedures to ensure that  
1662 an agency's information technology resources are identified and  
1663 managed consistent with their relative importance to the  
1664 agency's business objectives.

1665 2. Using a standard risk assessment methodology that  
1666 includes the identification of an agency's priorities,  
1667 constraints, risk tolerances, and assumptions necessary to  
1668 support operational risk decisions and that is aligned with  
1669 generally accepted technology best practices, including the  
1670 National Institute for Standards and Technology Cybersecurity  
1671 Framework.

1672 3. Completing comprehensive risk assessments and  
1673 cybersecurity audits, which may be completed by an independent  
1674 third party ~~a private sector vendor~~, and submitting completed  
1675 assessments and audits to DIGIT ~~the department~~.

1676 4. Identifying protection procedures to manage the  
1677 protection of an agency's information, data, and information  
1678 technology resources.

1679 5. Establishing procedures for accessing information and  
1680 data to ensure the confidentiality, integrity, and availability  
1681 of such information and data.

1682 6. Detecting threats through proactive monitoring of

601-02525-26

2026480c1

1683 events, continuous security monitoring, and defined detection  
1684 processes.

1685 7. Establishing agency cybersecurity incident response  
1686 teams and describing their responsibilities for responding to  
1687 cybersecurity incidents, including breaches of personal  
1688 information containing confidential or exempt data.

1689 8. Recovering information and data in response to a  
1690 cybersecurity incident. The recovery may include recommended  
1691 improvements to the agency processes, policies, or guidelines.

1692 9. Establishing a cybersecurity incident reporting process  
1693 that includes procedures for notifying DIGIT the department and  
1694 the Department of Law Enforcement of cybersecurity incidents.

1695 a. The level of severity of the cybersecurity incident is  
1696 defined by the National Cyber Incident Response Plan of the  
1697 United States Department of Homeland Security as follows:

1698 (I) Level 5 is an emergency-level incident within the  
1699 specified jurisdiction that poses an imminent threat to the  
1700 provision of wide-scale critical infrastructure services;  
1701 national, state, or local government security; or the lives of  
1702 the country's, state's, or local government's residents.

1703 (II) Level 4 is a severe-level incident that is likely to  
1704 result in a significant impact in the affected jurisdiction to  
1705 public health or safety; national, state, or local security;  
1706 economic security; or civil liberties.

1707 (III) Level 3 is a high-level incident that is likely to  
1708 result in a demonstrable impact in the affected jurisdiction to  
1709 public health or safety; national, state, or local security;  
1710 economic security; civil liberties; or public confidence.

1711 (IV) Level 2 is a medium-level incident that may impact

601-02525-26

2026480c1

1712 public health or safety; national, state, or local security;  
1713 economic security; civil liberties; or public confidence.

1714 (V) Level 1 is a low-level incident that is unlikely to  
1715 impact public health or safety; national, state, or local  
1716 security; economic security; civil liberties; or public  
1717 confidence.

1718 b. The cybersecurity incident reporting process must  
1719 specify the information that must be reported by a state agency  
1720 following a cybersecurity incident or ransomware incident,  
1721 which, at a minimum, must include the following:

1722 (I) A summary of the facts surrounding the cybersecurity  
1723 incident or ransomware incident.

1724 (II) The date on which the state agency most recently  
1725 backed up its data; the physical location of the backup, if the  
1726 backup was affected; and if the backup was created using cloud  
1727 computing.

1728 (III) The types of data compromised by the cybersecurity  
1729 incident or ransomware incident.

1730 (IV) The estimated fiscal impact of the cybersecurity  
1731 incident or ransomware incident.

1732 (V) In the case of a ransomware incident, the details of  
1733 the ransom demanded.

1734 c. (I) A state agency shall report all ransomware incidents  
1735 and any cybersecurity incident determined by the state agency to  
1736 be of severity level 3, 4, or 5 to the state chief information  
1737 security officer ~~Cybersecurity Operations Center~~ and the  
1738 Cybercrime Office of the Department of Law Enforcement as soon  
1739 as possible but no later than 48 hours after discovery of the  
1740 cybersecurity incident and no later than 12 hours after

601-02525-26

2026480c1

1741 discovery of the ransomware incident. The report must contain  
1742 the information required in sub-subparagraph b. If the event  
1743 involves services housed or procured through the Northwest  
1744 Regional Data Center, the state agency must also notify the  
1745 Northwest Regional Data Center.

1746 (II) The state chief information security officer  
1747 ~~Cybersecurity Operations Center~~ shall notify the President of  
1748 the Senate and the Speaker of the House of Representatives of  
1749 any severity level 3, 4, or 5 incident as soon as possible but  
1750 no later than 12 hours after receiving a state agency's incident  
1751 report. The notification must include a high-level description  
1752 of the incident and the likely effects.

1753 d. A state agency shall report a cybersecurity incident  
1754 determined by the state agency to be of severity level 1 or 2 to  
1755 the state chief information security officer ~~Cybersecurity~~  
1756 ~~Operations Center~~ and the Cybercrime Office of the Department of  
1757 Law Enforcement as soon as possible, but no later than 96 hours  
1758 after the discovery of the cybersecurity incident and no later  
1759 than 72 hours after the discovery of the ransomware incident.  
1760 The report must contain the information required in sub-  
1761 subparagraph b. If the event involves services housed or  
1762 procured through the Northwest Regional Data Center, the state  
1763 agency must also notify the Northwest Regional Data Center.

1764 e. The state chief information security officer  
1765 ~~Cybersecurity Operations Center~~ shall provide a consolidated  
1766 incident report on a quarterly basis to the President of the  
1767 Senate ~~and,~~ the Speaker of the House of Representatives, ~~and the~~ the  
1768 ~~Florida Cybersecurity Advisory Council.~~ The report provided to  
1769 ~~the Florida Cybersecurity Advisory Council~~ may not contain the

601-02525-26

2026480c1

1770 ~~name of any agency, network information, or system identifying~~  
1771 ~~information but must contain sufficient relevant information to~~  
1772 ~~allow the Florida Cybersecurity Advisory Council to fulfill its~~  
1773 ~~responsibilities as required in s. 282.319(9).~~

1774 10. Incorporating information obtained through detection  
1775 and response activities into the agency's cybersecurity incident  
1776 response plans.

1777 11. Developing agency strategic and operational  
1778 cybersecurity plans required pursuant to this section.

1779 12. Establishing the managerial, operational, and technical  
1780 safeguards for protecting state government data and information  
1781 technology resources that align with the state agency risk  
1782 management strategy and that protect the confidentiality,  
1783 integrity, and availability of information and data.

1784 13. Establishing procedures for procuring information  
1785 technology commodities and services that require the commodity  
1786 or service to meet the National Institute of Standards and  
1787 Technology Cybersecurity Framework.

1788 14. Submitting after-action reports following a  
1789 cybersecurity incident or ransomware incident. ~~Such guidelines~~  
1790 ~~and processes for submitting after-action reports must be~~  
1791 ~~developed and published by December 1, 2022.~~

1792 (d) Assist state agencies in complying with this section.

1793 (e) In collaboration with the Cybercrime Office of the  
1794 Department of Law Enforcement, annually provide training for  
1795 state agency information security managers and computer security  
1796 incident response team members that contains training on  
1797 cybersecurity, including cybersecurity threats, trends, and best  
1798 practices.

601-02525-26

2026480c1

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

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

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

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

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

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

601-02525-26

2026480c1

1828 directly to the agency head.

1829 (b) In consultation with the state chief information  
1830 security officer department, through the Florida Digital  
1831 Service, and the Cybercrime Office of the Department of Law  
1832 Enforcement, establish an agency cybersecurity response team to  
1833 respond to a cybersecurity incident. The agency cybersecurity  
1834 response team shall convene upon notification of a cybersecurity  
1835 incident and shall must immediately report all confirmed or  
1836 suspected incidents to the state chief information security  
1837 officer, or his or her designee, and comply with all applicable  
1838 guidelines and processes established pursuant to paragraph  
1839 (3) (c) .

1840 (c) Submit to the state chief information security officer  
1841 department annually by July 31, the state agency's strategic and  
1842 operational cybersecurity plans developed pursuant to rules and  
1843 guidelines established by the state chief information security  
1844 officer department, through the Florida Digital Service.

1845 1. The state agency strategic cybersecurity plan must cover  
1846 a 2-year ~~3-year~~ period and, at a minimum, define security goals,  
1847 intermediate objectives, and projected agency costs for the  
1848 strategic issues of agency information security policy, risk  
1849 management, security training, security incident response, and  
1850 disaster recovery. The plan must be based on the statewide  
1851 cybersecurity strategic plan created by the state chief  
1852 information security officer department and include performance  
1853 metrics that can be objectively measured to reflect the status  
1854 of the state agency's progress in meeting security goals and  
1855 objectives identified in the agency's strategic information  
1856 security plan.

601-02525-26

2026480c1

1857        2. The state agency operational cybersecurity plan must  
1858        include a set of measures that objectively assess the  
1859        performance of the agency's cybersecurity program in accordance  
1860        with its risk management plan progress report that objectively  
1861        measures progress made towards the prior operational  
1862        cybersecurity plan and a project plan that includes activities,  
1863        timelines, and deliverables for security objectives that the  
1864        state agency will implement during the current fiscal year.

1865        (d) Conduct, and update every 2 3 years, a comprehensive  
1866        risk assessment, which may be completed by an independent third  
1867        party a private sector vendor, to determine the security threats  
1868        to the data, information, and information technology resources,  
1869        including mobile devices and print environments, of the agency.  
1870        The risk assessment must comply with the risk assessment  
1871        methodology developed by the state chief information security  
1872        officer department and is confidential and exempt from s.  
1873        119.07(1), except that such information shall be available to  
1874        the Auditor General, the state chief information security  
1875        officer Florida Digital Service within the department, the  
1876        Cybercrime Office of the Department of Law Enforcement, and, for  
1877        state agencies under the jurisdiction of the Governor, the Chief  
1878        Inspector General. If an independent third party a private  
1879        sector vendor is used to complete a comprehensive risk  
1880        assessment, it must attest to the validity of the risk  
1881        assessment findings. The comprehensive risk assessment must  
1882        include all of the following:

1883        1. The results of vulnerability and penetration tests on  
1884        any Internet website or mobile application that processes any  
1885        sensitive personal information or confidential information and a

601-02525-26

2026480c1

1886 plan to address any vulnerability identified in the tests.

1887 2. A written acknowledgment that the executive director or  
1888 the secretary of the agency, the chief financial officer of the  
1889 agency, and each executive manager as designated by the state  
1890 agency have been made aware of the risks revealed during the  
1891 preparation of the agency's operations cybersecurity plan and  
1892 the comprehensive risk assessment.

1893 (e) Develop, and periodically update, written internal  
1894 policies and procedures, which include procedures for reporting  
1895 cybersecurity incidents and breaches to the Cybercrime Office of  
1896 the Department of Law Enforcement and the state chief  
1897 information security officer ~~Florida Digital Service within the~~  
1898 ~~department~~. Such policies and procedures must be consistent with  
1899 the rules, guidelines, and processes established by DIGIT ~~the~~  
1900 ~~department~~ to ensure the security of the data, information, and  
1901 information technology resources of the agency. The internal  
1902 policies and procedures that, if disclosed, could facilitate the  
1903 unauthorized modification, disclosure, or destruction of data or  
1904 information technology resources are confidential information  
1905 and exempt from s. 119.07(1), except that such information must  
1906 shall be available to the Auditor General, the Cybercrime Office  
1907 of the Department of Law Enforcement, the state chief  
1908 information security officer ~~the Florida Digital Service within~~  
1909 ~~the department~~, and, for state agencies under the jurisdiction  
1910 of the Governor, the Chief Inspector General.

1911 (f) Implement managerial, operational, and technical  
1912 safeguards and risk assessment remediation plans recommended by  
1913 DIGIT ~~the department~~ to address identified risks to the data,  
1914 information, and information technology resources of the agency.

601-02525-26

2026480c1

1915 The state chief information security officer department, through  
1916 ~~the Florida Digital Service~~, shall track implementation by state  
1917 agencies upon development of such remediation plans in  
1918 coordination with agency inspectors general.

1919 (g) Ensure that periodic internal audits and evaluations of  
1920 the agency's cybersecurity program for the data, information,  
1921 and information technology resources of the agency are  
1922 conducted. The results of such audits and evaluations are  
1923 confidential information and exempt from s. 119.07(1), except  
1924 that such information must ~~shall~~ be available to the Auditor  
1925 General, the Cybercrime Office of the Department of Law  
1926 Enforcement, the state chief information security officer  
1927 ~~Florida Digital Service within the department~~, and, for agencies  
1928 under the jurisdiction of the Governor, the Chief Inspector  
1929 General.

1930 (h) Ensure that the cybersecurity requirements in the  
1931 written specifications for the solicitation, contracts, and  
1932 service-level agreement of information technology and  
1933 information technology resources and services meet or exceed the  
1934 applicable state and federal laws, regulations, and standards  
1935 for cybersecurity, including the National Institute of Standards  
1936 and Technology Cybersecurity Framework. Service-level agreements  
1937 must identify service provider and state agency responsibilities  
1938 for privacy and security, protection of government data,  
1939 personnel background screening, and security deliverables with  
1940 associated frequencies.

1941 (i) Provide cybersecurity awareness training to all state  
1942 agency employees within 30 days after commencing employment, and  
1943 annually thereafter, concerning cybersecurity risks and the

601-02525-26

2026480c1

1944 responsibility of employees to comply with policies, standards,  
1945 guidelines, and operating procedures adopted by the state agency  
1946 to reduce those risks. The training may be provided in  
1947 collaboration with the Cybercrime Office of the Department of  
1948 Law Enforcement, a private sector entity, or an institution of  
1949 the State University System.

1950 (j) Develop a process for detecting, reporting, and  
1951 responding to threats, breaches, or cybersecurity incidents  
1952 which is consistent with the security rules, guidelines, and  
1953 processes established by DIGIT the department through the state  
1954 chief information security officer Florida Digital Service.

1955 1. All cybersecurity incidents and ransomware incidents  
1956 must be reported by state agencies. Such reports must comply  
1957 with the notification procedures and reporting timeframes  
1958 established pursuant to paragraph (3)(c).

1959 2. For cybersecurity breaches, state agencies shall provide  
1960 notice in accordance with s. 501.171.

1961 (k) Submit to the state chief information security officer  
1962 Florida Digital Service, within 1 week after the remediation of  
1963 a cybersecurity incident or ransomware incident, an after-action  
1964 report that summarizes the incident, the incident's resolution,  
1965 and any insights gained as a result of the incident.

1966 (7) The portions of records made confidential and exempt in  
1967 subsections (5) and (6) must shall be available to the Auditor  
1968 General, the Cybercrime Office of the Department of Law  
1969 Enforcement, the state chief information security officer, the  
1970 Legislature Florida Digital Service within the department, and,  
1971 for agencies under the jurisdiction of the Governor, the Chief  
1972 Inspector General. Such portions of records may be made

601-02525-26

2026480c1

1973 available to a local government, another state agency, or a  
1974 federal agency for cybersecurity purposes or in furtherance of  
1975 the state agency's official duties.

1976 (10) DIGIT The department shall adopt rules relating to  
1977 cybersecurity and to administer this section.

1978 Section 17. Subsections (3) through (6) of section  
1979 282.3185, Florida Statutes, are amended to read:

1980 282.3185 Local government cybersecurity.—

1981 (3) CYBERSECURITY TRAINING.—

1982 (a) The state chief information security officer Florida  
1983 ~~Digital Service~~ shall:

1984 1. Develop a basic cybersecurity training curriculum for  
1985 local government employees. All local government employees with  
1986 access to the local government's network must complete the basic  
1987 cybersecurity training within 30 days after commencing  
1988 employment and annually thereafter.

1989 2. Develop an advanced cybersecurity training curriculum  
1990 for local governments which is consistent with the cybersecurity  
1991 training required under s. 282.318(3)(g). All local government  
1992 technology professionals and employees with access to highly  
1993 sensitive information must complete the advanced cybersecurity  
1994 training within 30 days after commencing employment and annually  
1995 thereafter.

1996 (b) The state chief information security officer Florida  
1997 ~~Digital Service~~ may provide the cybersecurity training required  
1998 by this subsection in collaboration with the Cybercrime Office  
1999 of the Department of Law Enforcement, a private sector entity,  
2000 or an institution of the State University System.

2001 (4) CYBERSECURITY STANDARDS.—

601-02525-26

2026480c1

2002                   (a) Each local government shall adopt cybersecurity  
2003 standards that safeguard its data, information technology, and  
2004 information technology resources to ensure availability,  
2005 confidentiality, and integrity. The cybersecurity standards must  
2006 be consistent with generally accepted best practices for  
2007 cybersecurity, including the National Institute of Standards and  
2008 Technology Cybersecurity Framework.

2009                   (b) ~~Each county with a population of 75,000 or more must~~  
2010 ~~adopt the cybersecurity standards required by this subsection by~~  
2011 ~~January 1, 2024. Each county with a population of less than~~  
2012 ~~75,000 must adopt the cybersecurity standards required by this~~  
2013 ~~subsection by January 1, 2025.~~

2014                   (c) ~~Each municipality with a population of 25,000 or more~~  
2015 ~~must adopt the cybersecurity standards required by this~~  
2016 ~~subsection by January 1, 2024. Each municipality with a~~  
2017 ~~population of less than 25,000 must adopt the cybersecurity~~  
2018 ~~standards required by this subsection by January 1, 2025.~~

2019                   (d) Each local government shall notify the state chief  
2020 information security officer ~~Florida Digital Service~~ of its  
2021 compliance with this subsection as soon as possible.

2022                   (5) INCIDENT NOTIFICATION.—

2023                   (a) A local government shall provide notification of a  
2024 cybersecurity incident or ransomware incident to the state chief  
2025 information security officer ~~Cybersecurity Operations Center,~~  
2026 ~~the~~ Cybercrime Office of the Department of Law Enforcement, and  
2027 ~~the~~ sheriff who has jurisdiction over the local government in  
2028 accordance with paragraph (b). The notification must include, at  
2029 a minimum, the following information:

2030                   1. A summary of the facts surrounding the cybersecurity

601-02525-26

2026480c1

2031 incident or ransomware incident.

2032 2. The date on which the local government most recently  
2033 backed up its data; the physical location of the backup, if the  
2034 backup was affected; and if the backup was created using cloud  
2035 computing.

2036 3. The types of data compromised by the cybersecurity  
2037 incident or ransomware incident.

2038 4. The estimated fiscal impact of the cybersecurity  
2039 incident or ransomware incident.

2040 5. In the case of a ransomware incident, the details of the  
2041 ransom demanded.

2042 6. A statement requesting or declining assistance from ~~the~~  
2043 ~~Cybersecurity Operations Center~~, the Cybercrime Office of the  
2044 Department of Law Enforcement, or the sheriff who has  
2045 jurisdiction over the local government.

2046 (b)1. A local government shall report all ransomware  
2047 incidents and any cybersecurity incident determined by the local  
2048 government to be of severity level 3, 4, or 5 as provided in s.  
2049 282.318(3)(c) to the state chief information security officer  
2050 ~~Cybersecurity Operations Center~~, the Cybercrime Office of the  
2051 Department of Law Enforcement, and the sheriff who has  
2052 jurisdiction over the local government as soon as possible but  
2053 no later than 12 48 hours after discovery of the cybersecurity  
2054 incident and no later than 6 12 hours after discovery of the  
2055 ransomware incident. The report must contain the information  
2056 required in paragraph (a).

2057 2. The state chief information security officer  
2058 ~~Cybersecurity Operations Center~~ shall notify the President of  
2059 the Senate and the Speaker of the House of Representatives of

601-02525-26

2026480c1

2060 any severity level 3, 4, or 5 incident as soon as possible but  
2061 no later than 12 hours after receiving a local government's  
2062 incident report. The notification must include a high-level  
2063 description of the incident and the likely effects.

2064 (c) A local government may report a cybersecurity incident  
2065 determined by the local government to be of severity level 1 or  
2066 2 as provided in s. 282.318(3)(c) to the state chief information  
2067 security officer Cybersecurity Operations Center, the Cybercrime  
2068 Office of the Department of Law Enforcement, and the sheriff who  
2069 has jurisdiction over the local government. The report must  
2070 shall contain the information required in paragraph (a).

2071 (d) The state chief information security officer  
2072 Cybersecurity Operations Center shall provide a consolidated  
2073 incident report by the 30th day after the end of each quarter on  
2074 a quarterly basis to the President of the Senate and, the  
2075 Speaker of the House of Representatives, and the Florida  
2076 Cybersecurity Advisory Council. The report provided to the  
2077 Florida Cybersecurity Advisory Council may not contain the name  
2078 of any local government, network information, or system  
2079 identifying information but must contain sufficient relevant  
2080 information to allow the Florida Cybersecurity Advisory Council  
2081 to fulfill its responsibilities as required in s. 282.319(9).

2082 (6) AFTER-ACTION REPORT.—A local government shall must  
2083 submit to the state chief information security officer Florida  
2084 Digital Service, within 1 week after the remediation of a  
2085 cybersecurity incident or ransomware incident, an after-action  
2086 report that summarizes the incident, the incident's resolution,  
2087 and any insights gained as a result of the incident. By December  
2088 1, 2022, the Florida Digital Service shall establish guidelines

601-02525-26

2026480c1

2089 and processes for submitting an after action report.

2090 Section 18. Section 282.319, Florida Statutes, is repealed.

2091 Section 19. Section 282.201, Florida Statutes, is amended  
2092 to read:

2093 282.201 State data center.—The state data center is  
2094 established within the Northwest Regional Data Center pursuant  
2095 to s. 282.2011 and shall meet or exceed the information  
2096 technology standards specified in ss. 282.006 and 282.318 the  
2097 department. The provision of data center services must comply  
2098 with applicable state and federal laws, regulations, and  
2099 policies, including all applicable security, privacy, and  
2100 auditing requirements. The department shall appoint a director  
2101 of the state data center who has experience in leading data  
2102 center facilities and has expertise in cloud computing  
2103 management.

2104 (1) STATE DATA CENTER DUTIES.—The state data center shall:

2105 (a) Offer, develop, and support the services and  
2106 applications defined in service level agreements executed with  
2107 its customer entities.

2108 (b) Maintain performance of the state data center by  
2109 ensuring proper data backup; data backup recovery; disaster  
2110 recovery; and appropriate security, power, cooling, fire  
2111 suppression, and capacity.

2112 (c) Develop and implement business continuity and disaster  
2113 recovery plans, and annually conduct a live exercise of each  
2114 plan.

2115 (d) Enter into a service level agreement with each customer  
2116 entity to provide the required type and level of service or  
2117 services. If a customer entity fails to execute an agreement

601-02525-26

2026480c1

2118 ~~within 60 days after commencement of a service, the state data~~  
2119 ~~center may cease service. A service level agreement may not have~~  
2120 ~~a term exceeding 3 years and at a minimum must:~~

2121 ~~1. Identify the parties and their roles, duties, and~~  
2122 ~~responsibilities under the agreement.~~

2123 ~~2. State the duration of the contract term and specify the~~  
2124 ~~conditions for renewal.~~

2125 ~~3. Identify the scope of work.~~

2126 ~~4. Identify the products or services to be delivered with~~  
2127 ~~sufficient specificity to permit an external financial or~~  
2128 ~~performance audit.~~

2129 ~~5. Establish the services to be provided, the business~~  
2130 ~~standards that must be met for each service, the cost of each~~  
2131 ~~service by agency application, and the metrics and processes by~~  
2132 ~~which the business standards for each service are to be~~  
2133 ~~objectively measured and reported.~~

2134 ~~6. Provide a timely billing methodology to recover the~~  
2135 ~~costs of services provided to the customer entity pursuant to s.~~  
2136 ~~215.422.~~

2137 ~~7. Provide a procedure for modifying the service level~~  
2138 ~~agreement based on changes in the type, level, and cost of a~~  
2139 ~~service.~~

2140 ~~8. Include a right to audit clause to ensure that the~~  
2141 ~~parties to the agreement have access to records for audit~~  
2142 ~~purposes during the term of the service level agreement.~~

2143 ~~9. Provide that a service level agreement may be terminated~~  
2144 ~~by either party for cause only after giving the other party and~~  
2145 ~~the department notice in writing of the cause for termination~~  
2146 ~~and an opportunity for the other party to resolve the identified~~

601-02525-26

2026480c1

2147 cause within a reasonable period.

2148 10. Provide for mediation of disputes by the Division of  
2149 Administrative Hearings pursuant to s. 120.573.

2150 (e) For purposes of chapter 273, be the custodian of  
2151 resources and equipment located in and operated, supported, and  
2152 managed by the state data center.

2153 (f) Assume administrative access rights to resources and  
2154 equipment, including servers, network components, and other  
2155 devices, consolidated into the state data center.

2156 1. Upon consolidation, a state agency shall relinquish  
2157 administrative rights to consolidated resources and equipment.  
2158 State agencies required to comply with federal and state  
2159 criminal justice information security rules and policies shall  
2160 retain administrative access rights sufficient to comply with  
2161 the management control provisions of those rules and policies;  
2162 however, the state data center shall have the appropriate type  
2163 or level of rights to allow the center to comply with its duties  
2164 pursuant to this section. The Department of Law Enforcement  
2165 shall serve as the arbiter of disputes pertaining to the  
2166 appropriate type and level of administrative access rights  
2167 pertaining to the provision of management control in accordance  
2168 with the federal criminal justice information guidelines.

2169 2. The state data center shall provide customer entities  
2170 with access to applications, servers, network components, and  
2171 other devices necessary for entities to perform business  
2172 activities and functions, and as defined and documented in a  
2173 service level agreement.

2174 (g) In its procurement process, show preference for cloud-  
2175 computing solutions that minimize or do not require the

601-02525-26

2026480c1

2176 ~~purchasing, financing, or leasing of state data center~~  
2177 ~~infrastructure, and that meet the needs of customer agencies,~~  
2178 ~~that reduce costs, and that meet or exceed the applicable state~~  
2179 ~~and federal laws, regulations, and standards for cybersecurity.~~

2180 ~~(h) Assist customer entities in transitioning from state~~  
2181 ~~data center services to the Northwest Regional Data Center or~~  
2182 ~~other third-party cloud computing services procured by a~~  
2183 ~~customer entity or by the Northwest Regional Data Center on~~  
2184 ~~behalf of a customer entity.~~

2185 (1) (2) USE OF THE STATE DATA CENTER.

2186 ~~(a) The following are exempt from the use of the state data~~  
2187 ~~center: the Department of Law Enforcement, the Department of the~~  
2188 ~~Lottery's Gaming System, Systems Design and Development in the~~  
2189 ~~Office of Policy and Budget, the regional traffic management~~  
2190 ~~centers as described in s. 335.14(2) and the Office of Toll~~  
2191 ~~Operations of the Department of Transportation, the State Board~~  
2192 ~~of Administration, state attorneys, public defenders, criminal~~  
2193 ~~conflict and civil regional counsel, capital collateral regional~~  
2194 ~~counsel, and the Florida Housing Finance Corporation, and the~~  
2195 ~~Division of Emergency Management within the Executive Office of~~  
2196 ~~the Governor.~~

2197 ~~(b) The Division of Emergency Management is exempt from the~~  
2198 ~~use of the state data center. This paragraph expires July 1,~~  
2199 ~~2026.~~

2200 (2) (3) AGENCY LIMITATIONS.—Unless exempt from the use of  
2201 the state data center pursuant to this section or authorized by  
2202 the Legislature, a state agency may not:

2203 (a) Create a new agency computing facility or data center,  
2204 or expand the capability to support additional computer

601-02525-26

2026480c1

2205 equipment in an existing agency computing facility or data  
2206 center; or

2207 (b) Terminate services with the state data center without  
2208 giving written notice of intent to terminate services 180 days  
2209 before such termination.

2210 ~~(4) DEPARTMENT RESPONSIBILITIES. The department shall~~  
2211 ~~provide operational management and oversight of the state data~~  
2212 ~~center, which includes:~~

2213 ~~(a) Implementing industry standards and best practices for~~  
2214 ~~the state data center's facilities, operations, maintenance,~~  
2215 ~~planning, and management processes.~~

2216 ~~(b) Developing and implementing cost recovery mechanisms~~  
2217 ~~that recover the full direct and indirect cost of services~~  
2218 ~~through charges to applicable customer entities. Such cost~~  
2219 ~~recovery mechanisms must comply with applicable state and~~  
2220 ~~federal regulations concerning distribution and use of funds and~~  
2221 ~~must ensure that, for any fiscal year, no service or customer~~  
2222 ~~entity subsidizes another service or customer entity. The~~  
2223 ~~department may recommend other payment mechanisms to the~~  
2224 ~~Executive Office of the Governor, the President of the Senate,~~  
2225 ~~and the Speaker of the House of Representatives. Such mechanisms~~  
2226 ~~may be implemented only if specifically authorized by the~~  
2227 ~~Legislature.~~

2228 ~~(c) Developing and implementing appropriate operating~~  
2229 ~~guidelines and procedures necessary for the state data center to~~  
2230 ~~perform its duties pursuant to subsection (1). The guidelines~~  
2231 ~~and procedures must comply with applicable state and federal~~  
2232 ~~laws, regulations, and policies and conform to generally~~  
2233 ~~accepted governmental accounting and auditing standards. The~~

601-02525-26

2026480c1

2234 guidelines and procedures must include, but need not be limited  
2235 to:

2236 1. ~~Implementing a consolidated administrative support~~  
2237 ~~structure responsible for providing financial management,~~  
2238 ~~procurement, transactions involving real or personal property,~~  
2239 ~~human resources, and operational support.~~

2240 2. ~~Implementing an annual reconciliation process to ensure~~  
2241 ~~that each customer entity is paying for the full direct and~~  
2242 ~~indirect cost of each service as determined by the customer~~  
2243 ~~entity's use of each service.~~

2244 3. ~~Providing rebates that may be credited against future~~  
2245 ~~billings to customer entities when revenues exceed costs.~~

2246 4. ~~Requiring customer entities to validate that sufficient~~  
2247 ~~funds exist before implementation of a customer entity's request~~  
2248 ~~for a change in the type or level of service provided, if such~~  
2249 ~~change results in a net increase to the customer entity's cost~~  
2250 ~~for that fiscal year.~~

2251 5. ~~By November 15 of each year, providing to the Office of~~  
2252 ~~Policy and Budget in the Executive Office of the Governor and to~~  
2253 ~~the chairs of the legislative appropriations committees the~~  
2254 ~~projected costs of providing data center services for the~~  
2255 ~~following fiscal year.~~

2256 6. ~~Providing a plan for consideration by the Legislative~~  
2257 ~~Budget Commission if the cost of a service is increased for a~~  
2258 ~~reason other than a customer entity's request made pursuant to~~  
2259 ~~subparagraph 4. Such a plan is required only if the service cost~~  
2260 ~~increase results in a net increase to a customer entity for that~~  
2261 ~~fiscal year.~~

2262 7. ~~Standardizing and consolidating procurement and~~

601-02525-26

2026480c1

2263 ~~contracting practices.~~2264 ~~(d) In collaboration with the Department of Law Enforcement~~  
2265 ~~and the Florida Digital Service, developing and implementing a~~  
2266 ~~process for detecting, reporting, and responding to~~  
2267 ~~cybersecurity incidents, breaches, and threats.~~2268 ~~(e) Adopting rules relating to the operation of the state~~  
2269 ~~data center, including, but not limited to, budgeting and~~  
2270 ~~accounting procedures, cost-recovery methodologies, and~~  
2271 ~~operating procedures.~~2272 ~~(5) NORTHWEST REGIONAL DATA CENTER CONTRACT. In order for~~  
2273 ~~the department to carry out its duties and responsibilities~~  
2274 ~~relating to the state data center, the secretary of the~~  
2275 ~~department shall contract by July 1, 2022, with the Northwest~~  
2276 ~~Regional Data Center pursuant to s. 287.057(11). The contract~~  
2277 ~~shall provide that the Northwest Regional Data Center will~~  
2278 ~~manage the operations of the state data center and provide data~~  
2279 ~~center services to state agencies.~~2280 ~~(a) The department shall provide contract oversight,~~  
2281 ~~including, but not limited to, reviewing invoices provided by~~  
2282 ~~the Northwest Regional Data Center for services provided to~~  
2283 ~~state agency customers.~~2284 ~~(b) The department shall approve or request updates to~~  
2285 ~~invoices within 10 business days after receipt. If the~~  
2286 ~~department does not respond to the Northwest Regional Data~~  
2287 ~~Center, the invoice will be approved by default. The Northwest~~  
2288 ~~Regional Data Center must submit approved invoices directly to~~  
2289 ~~state agency customers.~~2290 Section 20. Section 282.2011, Florida Statutes, is created  
2291 to read:

601-02525-26

2026480c1

282.2011 Northwest Regional Data Center.—

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

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

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

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

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

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

3. Identify the scope of work;

4. Establish the services to be provided, the business standards that must be met for each service, the cost of each service, and the process by which the business standards for

601-02525-26

2026480c1

2321 each service are to be objectively measured and reported;

2322 5. Provide a timely billing methodology for recovering the  
2323 cost of services provided pursuant to s. 215.422;

2324 6. Provide a procedure for modifying the service-level  
2325 agreement to address any changes in projected costs of service;

2326 7. Include a right-to-audit clause to ensure that the  
2327 parties to the agreement have access to records for audit  
2328 purposes during the term of the service-level agreement;

2329 8. Identify the products or services to be delivered with  
2330 sufficient specificity to permit an external financial or  
2331 performance audit;

2332 9. Provide that the service-level agreement may be  
2333 terminated by either party for cause only after giving the other  
2334 party notice in writing of the cause for termination and an  
2335 opportunity for the other party to resolve the identified cause  
2336 within a reasonable period; and

2337 10. Provide state agency customer entities with access to  
2338 applications, servers, network components, and other devices  
2339 necessary for entities to perform business activities and  
2340 functions and as defined and documented in a service-level  
2341 agreement.

2342 (d) In its procurement process, show preference for cloud-  
2343 computing solutions that minimize or do not require the  
2344 purchasing or financing of state data center infrastructure,  
2345 that meet the needs of state agency customer entities, that  
2346 reduce costs, and that meet or exceed the applicable state and  
2347 federal laws, regulations, and standards for cybersecurity.

2348 (e) Assist state agency customer entities in transitioning  
2349 from state data center services to other third-party cloud-

601-02525-26

2026480c1

2350 computing services procured by a customer entity or by the  
2351 Northwest Regional Data Center on behalf of the customer entity.

2352 (f) Provide to the Board of Governors the total annual  
2353 budget by major expenditure category, including, but not limited  
2354 to, salaries, expenses, operating capital outlay, contracted  
2355 services, or other personnel services, by July 30 each fiscal  
2356 year.

2357 (g) Provide to each state agency customer its projected  
2358 annual cost for providing the agreed-upon data center services  
2359 by September 1 each fiscal year.

2360 (h) By November 15 of each year, provide to the Office of  
2361 Policy and Budget in the Executive Office of the Governor and to  
2362 the chairs of the legislative appropriations committees the  
2363 projected costs of providing data center services for the  
2364 following fiscal year for each state agency customer. The  
2365 projections must include prior-year comparisons, identification  
2366 of new services, and documentation of changes to billing  
2367 methodologies or service cost allocation.

2368 (i) Provide a plan for consideration by the Legislative  
2369 Budget Commission if the governing body of the center approves  
2370 the use of a billing rate schedule after the start of the fiscal  
2371 year which increases any state agency customer's costs for that  
2372 fiscal year.

2373 (j) Provide data center services that comply with  
2374 applicable state and federal laws, regulations, and policies,  
2375 including all applicable security, privacy, and auditing  
2376 requirements.

2377 (k) Maintain performance of the data center facilities by  
2378 ensuring proper data backup; data backup recovery; disaster

601-02525-26

2026480c1

2379 recovery; and appropriate security, power, cooling, fire  
2380 suppression, and capacity.

2381 (1) Submit invoices to state agency customers.

2382 (m) As funded in the General Appropriations Act, provide  
2383 data center services to state agencies from multiple facilities.

2384 (2) Unless exempt from the requirement to use the state  
2385 data center pursuant to s. 282.201(1) or as authorized by the  
2386 Legislature, a state agency may not do any of the following:

2387 (a) Terminate services with the Northwest Regional Data  
2388 Center without giving written notice of intent to terminate  
2389 services 180 days before such termination.

2390 (b) Procure third-party cloud-computing services without  
2391 evaluating the cloud-computing services provided by the  
2392 Northwest Regional Data Center.

2393 (c) Exceed 30 days from receipt of approved invoices to  
2394 remit payment for state data center services provided by the  
2395 Northwest Regional Data Center.

2396 (3) The Northwest Regional Data Center's authority to  
2397 provide data center services to its state agency customers may  
2398 be terminated if:

2399 (a) The center requests such termination to the Board of  
2400 Governors, the President of the Senate, and the Speaker of the  
2401 House of Representatives; or

2402 (b) The center fails to comply with the provisions of this  
2403 section.

2404 (4) The Northwest Regional Data Center is the lead entity  
2405 responsible for creating, operating, and managing, including the  
2406 research conducted by, the Florida Behavioral Health Care Data  
2407 Repository as established by this subsection.

601-02525-26

2026480c1

2408       (a) The purpose of the data repository is to create a  
2409 centralized system for:

2410       1. Collecting and analyzing existing statewide behavioral  
2411 health care data to:

2412       a. Better understand the scope of and trends in behavioral  
2413 health services, spending, and outcomes to improve patient care  
2414 and enhance the efficiency and effectiveness of behavioral  
2415 health services;

2416       b. Better understand the scope of, trends in, and  
2417 relationship between behavioral health, criminal justice,  
2418 incarceration, and the use of behavioral health services as a  
2419 diversion from incarceration for individuals with mental  
2420 illness; and

2421       c. Enhance the collection and coordination of treatment and  
2422 outcome information as an ongoing evidence base for research and  
2423 education related to behavioral health.

2424       2. Developing useful data analytics, economic metrics, and  
2425 visual representations of such analytics and metrics to inform  
2426 relevant state agencies and the Legislature of data and trends  
2427 in behavioral health.

2428       (b) The Northwest Regional Data Center shall develop, in  
2429 collaboration with the Data Analysis Committee of the Commission  
2430 on Mental Health and Substance Use Disorder created under s.  
2431 394.9086 and with relevant stakeholders, a plan that includes  
2432 all of the following:

2433       1. A project plan that describes the technology,  
2434 methodology, timeline, cost, and resources necessary to create a  
2435 centralized, integrated, and coordinated data system.

2436       2. A proposed governance structure to oversee the

601-02525-26

2026480c1

2437 implementation and operations of the repository.

2438 3. An integration strategy to incorporate existing data  
2439 from relevant state agencies, including, but not limited to, the  
2440 Agency for Health Care Administration, the Department of  
2441 Children and Families, the Department of Juvenile Justice, the  
2442 Office of the State Courts Administrator, and the Department of  
2443 Corrections.

2444 4. Identification of relevant data and metrics to support  
2445 actionable information and ensure the efficient and responsible  
2446 use of taxpayer dollars within behavioral health systems of  
2447 care.

2448 5. Data security requirements for the repository.

2449 6. The structure and process that will be used to create an  
2450 annual analysis and report that gives state agencies and the  
2451 Legislature a better general understanding of trends and issues  
2452 in the state's behavioral health systems of care and the trends  
2453 and issues in behavioral health systems related to criminal  
2454 justice treatment, diversion, and incarceration.

2455 (c) Beginning December 1, 2026, and annually thereafter,  
2456 the Northwest Regional Data Center shall submit the developed  
2457 trends and issues report under subparagraph (b) 6. to the  
2458 Governor, the President of the Senate, and the Speaker of the  
2459 House of Representatives.

2460 (5) If such authority is terminated, the center has 1 year  
2461 to provide for the transition of its state agency customers to a  
2462 qualified alternative cloud-based data center that meets the  
2463 enterprise architecture standards established pursuant to this  
2464 chapter.

2465 Section 21. Subsection (4) of section 282.206, Florida

601-02525-26

2026480c1

2466 Statutes, is amended to read:

2467 282.206 Cloud-first policy in state agencies.—

2468 (4) Each state agency shall develop a strategic plan to be  
2469 updated annually to address its inventory of applications  
2470 located at the state data center. Each agency shall submit the  
2471 plan by October 15 of each year to DIGIT, the Office of Policy  
2472 and Budget in the Executive Office of the Governor, and the  
2473 chairs of the legislative appropriations committees, and the  
2474 Northwest Regional Data Center. For each application, the plan  
2475 must identify and document the feasibility, appropriateness,  
2476 readiness, appropriate strategy, and high-level timeline for  
2477 transition to a cloud-computing service based on the  
2478 application's quality, cost, and resource requirements. This  
2479 information must be used to assist the state data center in  
2480 making adjustments to its service offerings.

2481 Section 22. Section 1004.649, Florida Statutes, is amended  
2482 to read:

2483 1004.649 Northwest Regional Data Center.—There is created  
2484 at Florida State University the Northwest Regional Data Center.  
2485 The data center shall serve as the state data center as  
2486 designated in s. 282.201

2487 ~~(1) For the purpose of providing data center services to~~  
2488 ~~its state agency customers, the Northwest Regional Data Center~~  
2489 ~~is designated as a state data center for all state agencies and~~  
2490 ~~shall:~~

2491 ~~(a) Operate under a governance structure that represents~~  
2492 ~~its customers proportionally.~~

2493 ~~(b) Maintain an appropriate cost-allocation methodology~~  
2494 ~~that accurately bills state agency customers based solely on the~~

601-02525-26

2026480c1

2495 ~~actual direct and indirect costs of the services provided to~~  
2496 ~~state agency customers and ensures that, for any fiscal year,~~  
2497 ~~state agency customers are not subsidizing other customers of~~  
2498 ~~the data center. Such cost allocation methodology must comply~~  
2499 ~~with applicable state and federal regulations concerning the~~  
2500 ~~distribution and use of state and federal funds.~~

2501 ~~(e) Enter into a service-level agreement with each state~~  
2502 ~~agency customer to provide services as defined and approved by~~  
2503 ~~the governing board of the center. At a minimum, such service-~~  
2504 ~~level agreements must:~~

- 2505 ~~1. Identify the parties and their roles, duties, and~~  
2506 ~~responsibilities under the agreement;~~
- 2507 ~~2. State the duration of the agreement term, which may not~~  
2508 ~~exceed 3 years, and specify the conditions for up to two~~  
2509 ~~optional 1-year renewals of the agreement before execution of a~~  
2510 ~~new agreement;~~
- 2511 ~~3. Identify the scope of work;~~
- 2512 ~~4. Establish the services to be provided, the business~~  
2513 ~~standards that must be met for each service, the cost of each~~  
2514 ~~service, and the process by which the business standards for~~  
2515 ~~each service are to be objectively measured and reported;~~
- 2516 ~~5. Provide a timely billing methodology for recovering the~~  
2517 ~~cost of services provided pursuant to s. 215.422;~~
- 2518 ~~6. Provide a procedure for modifying the service-level~~  
2519 ~~agreement to address any changes in projected costs of service;~~
- 2520 ~~7. Include a right-to-audit clause to ensure that the~~  
2521 ~~parties to the agreement have access to records for audit~~  
2522 ~~purposes during the term of the service-level agreement;~~
- 2523 ~~8. Identify the products or services to be delivered with~~

601-02525-26

2026480c1

2524 sufficient specificity to permit an external financial or  
2525 performance audit;

2526 9. Provide that the service-level agreement may be  
2527 terminated by either party for cause only after giving the other  
2528 party notice in writing of the cause for termination and an  
2529 opportunity for the other party to resolve the identified cause  
2530 within a reasonable period; and

2531 10. Provide state agency customer entities with access to  
2532 applications, servers, network components, and other devices  
2533 necessary for entities to perform business activities and  
2534 functions and as defined and documented in a service-level  
2535 agreement.

2536 (d) In its procurement process, show preference for cloud-  
2537 computing solutions that minimize or do not require the  
2538 purchasing or financing of state data center infrastructure,  
2539 that meet the needs of state agency customer entities, that  
2540 reduce costs, and that meet or exceed the applicable state and  
2541 federal laws, regulations, and standards for cybersecurity.

2542 (e) Assist state agency customer entities in transitioning  
2543 from state data center services to other third party cloud-  
2544 computing services procured by a customer entity or by the  
2545 Northwest Regional Data Center on behalf of the customer entity.

2546 (f) Provide to the Board of Governors the total annual  
2547 budget by major expenditure category, including, but not limited  
2548 to, salaries, expenses, operating capital outlay, contracted  
2549 services, or other personnel services by July 30 each fiscal  
2550 year.

2551 (g) Provide to each state agency customer its projected  
2552 annual cost for providing the agreed-upon data center services

601-02525-26

2026480c1

2553 by September 1 each fiscal year.

2554 (h) Provide a plan for consideration by the Legislative  
2555 Budget Commission if the governing body of the center approves  
2556 the use of a billing rate schedule after the start of the fiscal  
2557 year that increases any state agency customer's costs for that  
2558 fiscal year.

2559 (i) Provide data center services that comply with  
2560 applicable state and federal laws, regulations, and policies,  
2561 including all applicable security, privacy, and auditing  
2562 requirements.

2563 (j) Maintain performance of the data center facilities by  
2564 ensuring proper data backup; data backup recovery; disaster  
2565 recovery; and appropriate security, power, cooling, fire  
2566 suppression, and capacity.

2567 (k) Prepare and submit state agency customer invoices to  
2568 the Department of Management Services for approval. Upon  
2569 approval or by default pursuant to s. 282.201(5), submit  
2570 invoices to state agency customers.

2571 (l) As funded in the General Appropriations Act, provide  
2572 data center services to state agencies from multiple facilities.

2573 (2) Unless exempt from the requirement to use the state  
2574 data center pursuant to s. 282.201(2) or as authorized by the  
2575 Legislature, a state agency may not do any of the following:

2576 (a) Terminate services with the Northwest Regional Data  
2577 Center without giving written notice of intent to terminate  
2578 services 180 days before such termination.

2579 (b) Procure third-party cloud computing services without  
2580 evaluating the cloud computing services provided by the  
2581 Northwest Regional Data Center.

601-02525-26

2026480c1

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

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

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

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

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

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

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

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

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

e. Enhance the collection and coordination of treatment and

601-02525-26

2026480c1

2611 ~~outcome information as an ongoing evidence base for research and~~  
2612 ~~education related to behavioral health.~~

2613 ~~2. Developing useful data analytics, economic metrics, and~~  
2614 ~~visual representations of such analytics and metrics to inform~~  
2615 ~~relevant state agencies and the Legislature of data and trends~~  
2616 ~~in behavioral health.~~

2617 ~~(b) The Northwest Regional Data Center shall develop, in~~  
2618 ~~collaboration with the Data Analysis Committee of the Commission~~  
2619 ~~on Mental Health and Substance Use Disorder created under s.~~  
2620 ~~394.9086 and with relevant stakeholders, a plan that includes~~  
2621 ~~all of the following:~~

2622 ~~1. A project plan that describes the technology,~~  
2623 ~~methodology, timeline, cost, and resources necessary to create a~~  
2624 ~~centralized, integrated, and coordinated data system.~~

2625 ~~2. A proposed governance structure to oversee the~~  
2626 ~~implementation and operations of the repository.~~

2627 ~~3. An integration strategy to incorporate existing data~~  
2628 ~~from relevant state agencies, including, but not limited to, the~~  
2629 ~~Agency for Health Care Administration, the Department of~~  
2630 ~~Children and Families, the Department of Juvenile Justice, the~~  
2631 ~~Office of the State Courts Administrator, and the Department of~~  
2632 ~~Corrections.~~

2633 ~~4. Identification of relevant data and metrics to support~~  
2634 ~~actionable information and ensure the efficient and responsible~~  
2635 ~~use of taxpayer dollars within behavioral health systems of~~  
2636 ~~care.~~

2637 ~~5. Data security requirements for the repository.~~

2638 ~~6. The structure and process that will be used to create an~~  
2639 ~~annual analysis and report that gives state agencies and the~~

601-02525-26

2026480c1

2640 Legislature a better general understanding of trends and issues  
2641 in the state's behavioral health systems of care and the trends  
2642 and issues in behavioral health systems related to criminal  
2643 justice treatment, diversion, and incarceration.

2644 (e) By December 1, 2025, the Northwest Regional Data  
2645 Center, in collaboration with the Data Analysis Committee of the  
2646 Commission on Mental Health and Substance Use Disorder, shall  
2647 submit the developed plan for implementation and ongoing  
2648 operation with a proposed budget to the Governor, the President  
2649 of the Senate, and the Speaker of the House of Representatives  
2650 for review.

2651 (d) Beginning December 1, 2026, and annually thereafter,  
2652 the Northwest Regional Data Center shall submit the developed  
2653 trends and issues report under subparagraph (b) 6. to the  
2654 Governor, the President of the Senate, and the Speaker of the  
2655 House of Representatives.

2656 (5) If such authority is terminated, the center has 1 year  
2657 to provide for the transition of its state agency customers to a  
2658 qualified alternative cloud-based data center that meets the  
2659 enterprise architecture standards established by the Florida  
2660 Digital Service.

2661 Section 23. Section 287.0583, Florida Statutes, is created  
2662 to read:

2663 287.0583 Contract requirements for information technology  
2664 commodities or services.—A contract for information technology  
2665 commodities or services involving the development,  
2666 customization, implementation, integration, support, or  
2667 maintenance of software systems, applications, platforms, or  
2668 related services must include provisions ensuring all of the

601-02525-26

2026480c1

2669 following:2670 (1) Any data created, processed, or maintained under the  
2671 contract is portable and can be extracted in a machine-readable  
2672 format upon request.2673 (2) The vendor will provide, upon request, comprehensive  
2674 operational documentation sufficient to allow continued  
2675 operation and maintenance by the agency or a new vendor.2676 (3) The vendor will provide, upon request, reasonable  
2677 assistance and support during a transition to the agency or to a  
2678 new vendor.2679 (4) All anticipated software license fees, license renewal  
2680 fees, and operation and maintenance costs are documented in  
2681 detail. If exact figures are not feasible, the vendor must  
2682 provide a reasonable cost range.2683 Section 24. Section 287.0591, Florida Statutes, is amended  
2684 to read:

2685 287.0591 Information technology; vendor disqualification.—

2686 (1) (a) Any competitive solicitation issued by the  
2687 department for a state term contract for information technology  
2688 commodities must include a term that does not exceed 48 months.2689 (b) (2) Any competitive solicitation issued by the  
2690 department for a state term contract for information technology  
2691 consultant services or information technology staff augmentation  
2692 contractual services must include a term that does not exceed 48  
2693 months.2694 (c) (3) The department may execute a state term contract for  
2695 information technology commodities, consultant services, or  
2696 staff augmentation contractual services that exceeds the 48-  
2697 month requirement if the Secretary of Management Services and

601-02525-26

2026480c1

2698 the state chief information officer certify in writing to the  
2699 Executive Office of the Governor that a longer contract term is  
2700 in the best interest of the state.

2701 (2)-(4) If the department issues a competitive solicitation  
2702 for information technology commodities, consultant services, or  
2703 staff augmentation contractual services, the department shall  
2704 coordinate with the Division of Integrated Government Innovation  
2705 and Technology within the Executive Office of the Governor  
2706 ~~Florida Digital Service within the department shall participate~~  
2707 in such solicitations. Such coordination must include reviewing  
2708 the solicitation specifications to verify compliance with  
2709 enterprise architecture and cybersecurity standards, evaluating  
2710 vendor responses under established criteria, answering vendor  
2711 questions, and providing any other technical expertise  
2712 necessary.

2713 (3) (a)-(5) If an agency issues a request for quote to  
2714 purchase information technology commodities, information  
2715 technology consultant services, or information technology staff  
2716 augmentation contractual services from the state term contract  
2717 which meets the CATEGORY TWO threshold amount, but is less than  
2718 the CATEGORY FOUR threshold amount:;

2719 1. For any contract with 25 approved vendors or fewer, the  
2720 agency must issue a request for quote to all vendors approved to  
2721 provide such commodity or service.

2722 2. For any contract with more than 25 approved vendors, the  
2723 agency must issue a request for quote to at least 25 of the  
2724 vendors approved to provide such commodity or contractual  
2725 service.

2726 (b) The agency shall maintain a copy of the request for

601-02525-26

2026480c1

2727 quote, the identity of the vendors that were sent the request  
2728 for quote, and any vendor response to the request for quote for  
2729 2 years after the date of issuance of the purchase order.

2730 (c) Use of a request for quote does not constitute a  
2731 decision or intended decision that is subject to protest under  
2732 s. 120.57(3).

2733 (4) (a) An agency issuing a request for quote to purchase  
2734 information technology commodities, information technology  
2735 consultant services, or information technology staff  
2736 augmentation contractual services from the state term contract  
2737 which exceeds the CATEGORY FOUR threshold amount is subject to  
2738 public records requirements pursuant to s. 287.057.

2739 Additionally, an agency shall publish:

2740 1. The request for quote for a minimum of 10 days before  
2741 executing the purchase order; and

2742 2. The name of the vendor awarded the purchase order.

2743 (b) The agency shall maintain a copy of the request for  
2744 quote, the identity of the vendors that were sent the request  
2745 for quote, and all vendor responses to the request for quote for  
2746 2 years after the date of issuance of the purchase order.

2747 (c) Use of a request for quote does not constitute a  
2748 decision or intended decision that is subject to protest under  
2749 s. 120.57(3).

2750 (5) A state agency may request the Division of Integrated  
2751 Government Innovation and Technology within the Executive Office  
2752 of the Governor for procurement advisory and review services  
2753 pursuant to s. 282.0061.

2754 (6) (a) Beginning October 1, 2021, and Each October 1  
2755 thereafter, the department shall prequalify firms and

601-02525-26

2026480c1

2756 individuals to provide information technology staff augmentation  
2757 contractual services and information technology commodities on  
2758 state term contract.

2759 (b) In order to prequalify a firm or individual for  
2760 participation on the state term contract, the department must  
2761 consider, at a minimum, the capability, experience, and past  
2762 performance record of the firm or individual.

2763 (c) A firm or individual removed from the source of supply  
2764 pursuant to s. 287.042(1)(b) or placed on a disqualified vendor  
2765 list pursuant to s. 287.133 or s. 287.134 is immediately  
2766 disqualified from state term contract eligibility.

2767 (d) Once a firm or individual has been prequalified to  
2768 provide information technology staff augmentation contractual  
2769 services or information technology commodities on state term  
2770 contract, the firm or individual may respond to requests for  
2771 quotes from an agency to provide such services.

2772 Section 25. Subsection (2) of section 20.22, Florida  
2773 Statutes, is amended to read:

2774 20.22 Department of Management Services.—There is created a  
2775 Department of Management Services.

2776 (2) The following divisions, programs, and services within  
2777 the Department of Management Services are established:

2778 (a) Facilities Program.

2779 (b) ~~The Florida Digital Service.~~

2780 (c) ~~(e)~~ Workforce Program.

2781 (c) ~~(d)~~ 1. Support Program.

2782 2. Federal Property Assistance Program.

2783 (d) ~~(e)~~ Administration Program.

2784 (e) ~~(f)~~ Division of Administrative Hearings.

601-02525-26

2026480c1

2785        (f) ~~(g)~~ Division of Retirement.

2786        (g) ~~(h)~~ Division of State Group Insurance.

2787        (h) ~~(i)~~ Division of Telecommunications.

2788        Section 26. Subsections (1), (5), (7), and (8) of section  
2789 282.802, Florida Statutes, are amended to read:

2790        282.802 Government Technology Modernization Council.—

2791        (1) The Government Technology Modernization Council, an  
2792 advisory council as defined in s. 20.03(7), is located ~~created~~  
2793 within DIGIT ~~the department~~. Except as otherwise provided in  
2794 this section, the advisory council shall operate in a manner  
2795 consistent with s. 20.052.

2796        (5) The state chief information officer ~~Secretary of~~  
2797 ~~Management Services~~, or his or her designee, shall serve as the  
2798 ex officio, nonvoting executive director of the council.

2799        (7) ~~(a)~~ The council shall meet at least quarterly to:

2800        (a)1. Recommend legislative and administrative actions that  
2801 the Legislature and state agencies as defined in s. 282.0041 ~~s.~~  
2802 ~~282.318(2)~~ may take to promote the development of data  
2803 modernization in this state.

2804        (b)2. Assess and provide guidance on necessary legislative  
2805 reforms and the creation of a state code of ethics for  
2806 artificial intelligence systems in state government.

2807        (c)3. Assess the effect of automated decision systems or  
2808 identity management on constitutional and other legal rights,  
2809 duties, and privileges of residents of this state.

2810        (d)4. Evaluate common standards for artificial intelligence  
2811 safety and security measures, including the benefits of  
2812 requiring disclosure of the digital provenance for all images  
2813 and audio created using generative artificial intelligence as a

601-02525-26

2026480c1

2814 means of revealing the origin and edit of the image or audio, as  
2815 well as the best methods for such disclosure.

2816 (e)5. Assess the manner in which governmental entities and  
2817 the private sector are using artificial intelligence with a  
2818 focus on opportunity areas for deployments in systems across  
2819 this state.

2820 (f)6. Determine the manner in which artificial intelligence  
2821 is being exploited by bad actors, including foreign countries of  
2822 concern as defined in s. 287.138(1).

2823 (g)7. Evaluate the need for curriculum to prepare school-  
2824 age audiences with the digital media and visual literacy skills  
2825 needed to navigate the digital information landscape.

2826 ~~(b) At least one quarterly meeting of the council must be a~~  
2827 ~~joint meeting with the Florida Cybersecurity Advisory Council.~~

2828 ~~(8) By December 31, 2024, and Each December 31 thereafter,~~  
2829 the council shall submit to the Governor, the President of the  
2830 Senate, and the Speaker of the House of Representatives any  
2831 legislative recommendations considered necessary by the council  
2832 to modernize government technology, including:

2833 (a) Recommendations for policies necessary to:

2834 1. Accelerate adoption of technologies that will increase  
2835 productivity of state enterprise information technology systems,  
2836 improve customer service levels of government, and reduce  
2837 administrative or operating costs.

2838 2. Promote the development and deployment of artificial  
2839 intelligence systems, financial technology, education  
2840 technology, or other enterprise management software in this  
2841 state.

2842 3. Protect Floridians from bad actors who use artificial

601-02525-26

2026480c1

2843 intelligence.

2844 (b) Any other information the council considers relevant.

2845 Section 27. Section 282.604, Florida Statutes, is amended  
2846 to read:2847 282.604 Adoption of rules.—~~DIGIT The Department of~~  
2848 ~~Management Services~~ shall, with input from stakeholders, adopt  
2849 rules pursuant to ss. 120.536(1) and 120.54 for the development,  
2850 procurement, maintenance, and use of accessible electronic  
2851 information technology by governmental units.2852 Section 28. Paragraph (b) of subsection (4) of section  
2853 443.1113, Florida Statutes, is amended to read:2854 443.1113 Reemployment Assistance Claims and Benefits  
2855 Information System.—

2856 (4)

2857 (b) The department shall seek input on recommended  
2858 enhancements from, at a minimum, the following entities:2859 1. The Division of Integrated Government Innovation and  
2860 Technology within the Executive Office of the Governor Florida  
2861 ~~Digital Service within the Department of Management Services.~~2862 2. The General Tax Administration Program Office within the  
2863 Department of Revenue.2864 3. The Division of Accounting and Auditing within the  
2865 Department of Financial Services.2866 Section 29. Subsection (5) of section 943.0415, Florida  
2867 Statutes, is amended to read:2868 943.0415 Cybercrime Office.—There is created within the  
2869 Department of Law Enforcement the Cybercrime Office. The office  
2870 may:2871 (5) Consult with the state chief information security

601-02525-26

2026480c1

2872 officer of the Division of Integrated Government Innovation and  
2873 Technology within the Executive Office of the Governor Florida  
2874 ~~Digital Service within the Department of Management Services in~~  
2875 the adoption of rules relating to the information technology  
2876 security provisions in s. 282.318.

2877 Section 30. Subsection (3) of section 1004.444, Florida  
2878 Statutes, is amended to read:

2879 1004.444 Florida Center for Cybersecurity.—

2880 (3) Upon receiving a request for assistance from a the  
2881 ~~Department of Management Services, the Florida Digital Service,~~  
2882 ~~or another state agency,~~ the center is authorized, but may not  
2883 be compelled by the agency, to conduct, consult on, or otherwise  
2884 assist any state-funded initiatives related to:

2885 (a) Cybersecurity training, professional development, and  
2886 education for state and local government employees, including  
2887 school districts and the judicial branch; and

2888 (b) Increasing the cybersecurity effectiveness of the  
2889 state's and local governments' technology platforms and  
2890 infrastructure, including school districts and the judicial  
2891 branch.

2892 Section 31. This act shall take effect January 5, 2027.